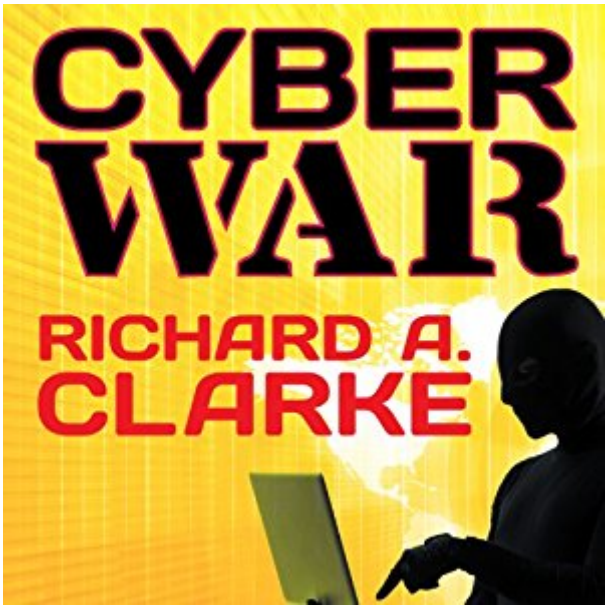
Cyber War: The Next Threat To National Security And What To Do About It



Synopsis

Richard A. Clarke warned America once before about the havoc terrorism would wreak on our national security-and he was right. Now he warns us of another threat, silent but equally dangerous. Cyber War is a powerful book about technology, government, and military strategy; about criminals, spies, soldiers, and hackers. This is the first book about the war of the future - cyber war - and a convincing argument that we may already be in peril of losing it.Cyber War goes behind the "geek talk" of hackers and computer scientists to explain clearly and convincingly what cyber war is, how cyber weapons work, and how vulnerable we are as a nation and as individuals to the vast and looming web of cyber criminals. From the first cyber crisis meeting in the White House a decade ago to the boardrooms of Silicon Valley and the electrical tunnels under Manhattan, Clarke and coauthor Robert K. Knake trace the rise of the cyber age and profile the unlikely characters and places at the epicenter of the battlefield. They recount the foreign cyber spies who hacked into the office of the Secretary of Defense, the control systems for U.S. electric power grids, and the plans to protect America’s latest fighter aircraft. Economically and militarily, Clarke and Knake argue, what we’ve already lost in the new millennium’s cyber battles is tantamount to the Soviet and Chinese theft of our nuclear bomb secrets in the 1940s and 1950s. The possibilities of what we stand to lose in an all-out cyber war-our individual and national security among them-are just as chilling. Powerful and convincing, Cyber War begins the critical debate about the next great threat to national security.

Book Information

Audible Audio Edition
Listening Length: 10 hoursÂ andÂ 6 minutes
Program Type: Audiobook
Version: Unabridged
Publisher: Tantor Audio
Audible.com Release Date: March 5, 2014
Whispersync for Voice: Ready
Language: English
ASIN: B00IK3IV3M
Best Sellers Rank: #31 inÂ Books > Politics & Social Sciences > Politics & Government > Elections & Political Process > General #42 inÂ Books > Audible Audiobooks > Nonfiction > Computers #54 inÂ Books > Audible Audiobooks > Politics & Current Events > Freedom & Security

Customer Reviews

I've been in the information security field just about my entire professional life, both in and out of government, and I've been hearing people sound the alarms about "cyber warfare" for at least the last 15 years. Most of the time their grasp of the technical aspects is limited, they don't have a clear idea about what they're talking about, their scenarios read like movie plots, and they're usually trying to win government contracts. Although this book does have some serious shortcomings, Clarke's book is without a doubt the clearest and best work I've seen on cyber warfare. I'll lay out his book and his thesis first, then I'll tell you where I thought he fell short and what I thought of it.Clarke first gives an overview of all the instances to date where cyber attacks have been used by state actors. In all cases but one (The Estonia attacks in 2007), the cyber attack was used to enhance a conventional attack. This is actually the best such overview I've seen, included some examples I hadn't heard of before, and Clarke's analysis is spot on. The only thing he didn't include was the very recent "operation aurora" (Google it if you want details), which probably occurred after he finished writing the book.The book then has a detailed discussion of American policy on cyber warfare, and Clarke details all the developments to date. Since Clarke worked for presidents Clinton, Bush, and Obama on national security issues, this book provides a front row seat to the ins and outs of the way our policies have developed. Clarke also details what is known about the cyber war capabilities of other countries, including China, Russia, and North Korea.

Clarke and Knake's book is important if for no other reason than, as they note, "there are few books on cyber war." Thus, their treatment of the issue will likely remain the most relevant text in the field for some time to come. They define cyber war as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" and they argue that such actions are on the rise. And they also claim that the U.S. has the most to lose if and when a major cyber war breaks out, since we are now so utterly dependent upon digital technologies and networks.At their best, Clarke and Knake walk the reader through the mechanics of cyber war, who some of the key players and countries are who could engage in it, and identify what the costs of such of war would entail. Other times, however, the book suffers from a somewhat hysterical tone, as the authors are out here not just to describe cyber war, but to also issue a clarion call for regulatory action to combat it. A bigger problem with the book is the complete lack of reference material, footnotes, or even an index. If you're going to go around sounding like a couple of cyber-Jeremiahs, you really should include some reference material to back up your gloomy assertions of impending doom.The authors go after ISPs and many other comapnies for supposedly

not caring about cyber-security. In reality, those companies have powerful incentives to make sure their networks are relatively safe and secure to avoid costly attacks and retain customers who demand their online information and activities be trouble-free.

The jacket for "Cyber War" (CW) says "This is the first book about the war of the future -- cyber war." That's not true, but I would blame the publisher for those words and not the authors. A look back to 1998 reveals books like James Adams' "The Next World War: Computers Are the Weapons & the Front Line Is Everywhere," a book whose title is probably cooler than its contents. (I read it back then but did not review it.) So what's the value of CW? I recommend reading the book if you'd like a Beltway insider's view of government and military information warfare history, combined with a few recommendations that could make a difference. CW is strongest when drawing on the authors' experience with arms control but weakest when trying to advocate technical "solutions."Early in the book I liked the "modern history" of cyber war. I especially enjoyed comparisons with the US military's experiences creating Space Command. I lived through some of that period but was unaware how Space Command's history affected creation of Cyber Command. Later, the book is almost derailed by the over-the-top cyber-geddon described at the end of chapter 3. It's just not necessary to include several pages where everything fails simultaneously, and I bet it erodes the confidence some readers have in the story. I'd remove the doom-and-gloom in future editions because I think people can imagine disasters fairly easily. Push through to chapter 4 and the book is once again on a sensible path, at least with respect to policy and history. For example, I loved reading Microsoft's lobbying goals: don't regulate, keep the military as a customer, and don't critique China! These rang true for me.Shortly thereafter we encounter the weakest part of CW: technical advice.

Appraisal of American National Security Policy during the Cold War The Fifty-Year Mission: The Next 25 Years: From The Next Generation to J. J. Abrams: The Complete, Uncensored, and Unauthorized Oral History of Star Trek National Geographic Yellowstone and Grand Teton National Parks Road Guide: The Essential Guide for Motorists (National Park Road Guide) Thinking Security: Stopping Next Year's Hackers (Addison-Wesley Professional Computing Series) Paria Canyon, Kanab [Vermillion Cliffs National Monument, Grand Staircase-Escalante National Monument] (National Geographic Trails Illustrated Map) Banksy. You are an Acceptable Level of Threat and If You Were Not You Would Know About it Rise of the Robots: Technology and the Threat of a Jobless Future Dark Pools: High-Speed Traders, A.I. Bandits, and the Threat to the Global Financial System Overconnected: The Promise and Threat of the Internet The Euro: And its Threat to the Future of Europe How the Other Half Banks: Exclusion, Exploitation, and the Threat to Democracy Threat Warning