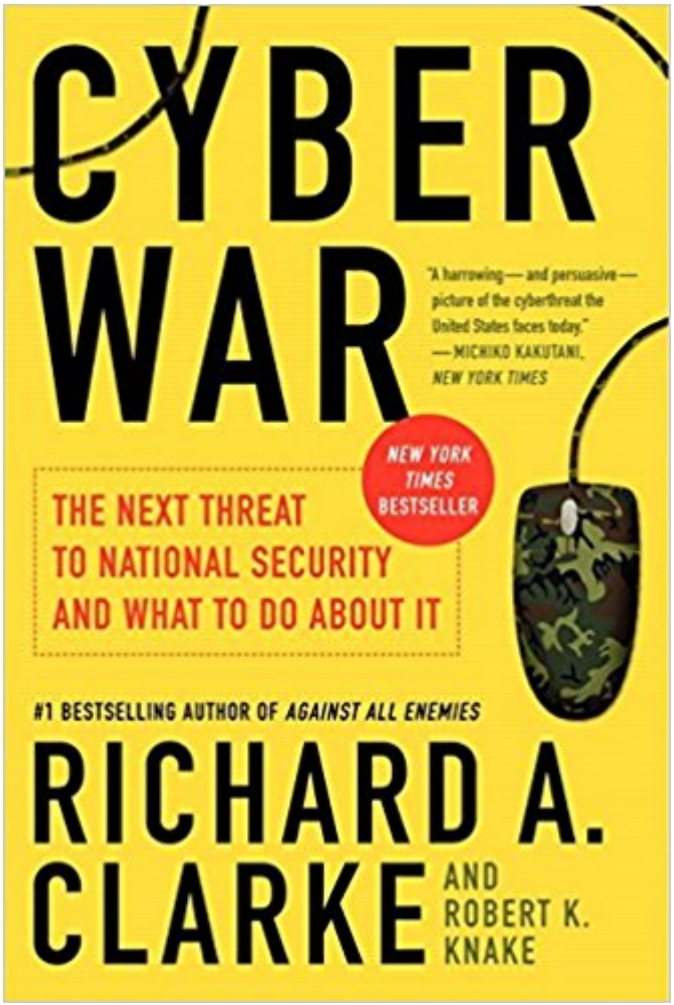
Cyber War: The Next Threat To National Security And What To Do About It



Synopsis

Author of the #1 New York Times bestseller Against All Enemies, former presidential advisor and counter-terrorism expert Richard A. Clarke sounds a timely and chilling warning about Americaâ ™s vulnerability in a terrifying new international conflictâ ”Cyber War! Every concerned American should read this startling and explosive book that offers an insiderâ ™s view of White House â ˆSituation Roomâ ™ operations and carries the reader to the frontlines of our cyber defense. Cyber War exposes a virulent threat to our nationâ ™s security. This is no X-Files fantasy or conspiracy theory madnessâ ”this is real.

Book Information

Paperback: 320 pages

Publisher: Ecco; Reprint edition (August 5, 2011)

Language: English

ISBN-10: 9780061962240

ISBN-13: 978-0061962240

ASIN: 0061962244

Product Dimensions: 5.3 x 0.7 x 8 inches

Shipping Weight: 8.8 ounces (View shipping rates and policies)

Average Customer Review: 4.6 out of 5 stars 1,002 customer reviews

Best Sellers Rank: #40,359 in Books (See Top 100 in Books) #62 inÂ Books > Politics & Social Sciences > Politics & Government > International & World Politics > Security #77 inÂ Books > Politics & Social Sciences > Politics & Government > Elections & Political Process > General #86 inÂ Books > Politics & Social Sciences > Politics & Government > Specific Topics > Intelligence & Espionage

Customer Reviews

On today’s battlefields computers play a major role, controlling targeting systems, relaying critical intelligence information, and managing logistics. And, like their civilian counter-parts, defense computers are susceptible to hacking. In September 2007, Israeli cyber warriors "blinded" Syrian anti-aircraft installations, allowing Israeli planes to bomb a suspected nuclear weapons manufacturing facility (Syrian computers were hacked and reprogrammed to display an empty sky). One of the first known cyber attacks against an independent nation was a Russian DDOS (Deliberate Denial of Service) on Estonia. Since it can rarely be traced directly back to the source, the DDOS has become a common form of attack, with Russia, China, North Korea, the U.S., and

virtually every other country in possession of a formidable military having launched low-level DDOS assaults. Analysts across the globe are well aware that any future large-scale conflict will include cyber warfare as part of a combined arms effort. Clarke and Knake argue that today's leaders, though more computer savvy than ever, may still be ignorant of the cyber threats facing their national security. Copyright Â© Reed Business Information, a division of Reed Elsevier Inc. All rights reserved. --This text refers to the Hardcover edition.

International security expertsâ ”Clarke from the nuclear generation and Knake from the cyber generationâ ”ponder the irony that although the U.S. pioneered the technology behind cyber warfare, outdated thinking, policies, and strategies make us vulnerable to losing any cyber contest with a hostile nation. Cyber war refers to hostile attempts by one nation to penetrate anotherâ ™s computers or networks. Among recent examples: suspicion that in 2007 Israel executed a cyber assault on a Syrian nuclear weapons plant being built by North Korea, the 2008 cyber attack on Georgia by Russia to knock out its government computers before an actual attack on that nation, and North Koreaâ ™s actions in 2009 after a nuclear missile test to launch botnets to disrupt government computer systems in the U.S. and South Korea. Cyber warriors often use programs to crash Web sites and computers to cover other, more aggressive actions in the real world. In this chilling and eye-opening book, Clarke and Knake provide a highly detailed yet accessible look at how cyber warfare is being waged and the need to rethink our national security to face this new threat. --Vanessa Bush --This text refers to the Hardcover edition.

I'm a retired Army officer and Viet Nam vet. The book was engaging from its beginning citing (then) LTC Cavoli's (whom I know personally) leadership and experiences thru to events in 2012. I learned a great deal. However, I found the (to me) over emphasis on the tactical detracted from an overall story of a lack a national strategic purpose, rationale and approach (then and still). Half of the tactical accounts would have been equally convincing and credible. That there were nearly as many strategic approaches as there were major commanders and Sec Defs was also a compelling argument. It was interesting and true that all too often presidential and secretarial pronouncements and orders were impossible to implement at the brigade level and below. I liked the idea of a viable career path for military advisors. Finally, I also believe that at any level leaving the nation building to the State Department is an absolute non-starter, a guaranteed local and national failure waiting to happen. There is not a word in the book to convince me otherwise.

Richard Clarke’s experience in cybersecurity is virtually unmatched in the recent era. He has no end of experience (and stories) to tell in both commercial and government arenas protecting networks and high visibility systems from attack.Whether you are in the IT industry, or just someone who wants to know about the threats our country faces, Cyber War is a brilliant introduction to the surface layer of what that conflict looks like in the last couple years. As the threat landscape continues to get broader with the introduction of cyber capabilities by more countries - some better controlled and more tightly defined than others - it pays dividends to understand the threat and think about how your life can be impacted.This book offers a series of stories, of descriptions, and a discussion of the evolution of the cyber attack as a tool in the arsenal of criminal enterprise, and - lately - nation states. It is, for the most part, well written and requires basic knowledge of what computers are and how they work to get the most out of the text, but stays at a high enough level that you really do not have to be a "techie" to "get it".One side note, those who are immersed in this world daily will find snatches of Richard Clarke’s experience interesting, but overall will find little new in the text if you are indeed in this arena day to day. (It is, after all, an unclassified published discussion "looking back" as it were.) Still worth the buy in my opinion, if only as something to read through and then keep on the virtual shelf for when something is rattling around in your brain and you want to look back through.

Great book. An interesting look at the combat experience and indirectly, a look at US policy in Afghanistan. (No criticsm inferred or implied.) With Junger’s book, TRIBES, it does much to explain PTSD and the continuing problems we see around us today, in the "civilized" world.The documentary RESTREPO is the foundation for this book.

Recently I published an article, "Seven Books Every Presidential Candidate Should Read." After reading this frightening book about the vulnerability of our military and economy, from the power grid to the financial structure, to cyber war, I will update the article. Clarke is a recognized expert, and is not a partisan hack. he has served as an adviser to Reagan, the Bushes, Clinton and Obama on these topics. Though this was published in 2010, I’ve seen nothing to suggest we are less vulnerable today, and some articles suggesting we are more so. Worth reading, and not just by computer geeks.Robert A. HallAuthor: TheComing Collapse of the American republic

Those interested in cyber security, international diplomacy or governmentreview This is one of those books you should read for its message, especially if you think that we’re safe from cyber attack.

Unfortunately the truth is far different, and it will likely stay that way indefinitely. Stated simply, if you're not afraid yet, you should be, and reading Richard Clarke's Cyber War should do just fine to repopulate your anxiety closet if it's been emptying out lately.Clarke is in a position to know what the real story is due to his recent government experience in the upper echelons of cyber defense. He presents his case for stronger defenses clearly, and without too much jargon. He also outlines not only current weaknesses of concern, but also the administrative and bureaucratic flaws that can lead as surely to vulnerabilities as technical gaps.A highlight for those interested in the nuts and bolts of cyber warfare are his readable details on how actual attacks (such as the US/Israeli - Stuxnet attack launched against Iran) were conducted, and how U.S. enemies could exploit similar weaknesses in our own defenses.Any book in an area as fast-moving as cyber security is itself vulnerable to becoming out of date quickly, but this one should hold up well for a number of years more, due to the fact that it focuses on fundamental weaknesses rather than the details of how individual exploits have been conducted

World War III Series: Book IV Dark Territory: The Secret History of Cyber War Cyber War Will Not Take Place World War 1: Soldier Stories: The Untold Soldier Stories on the Battlefields of WWI (World War I, WWI, World War One, Great War, First World War, Soldier Stories) Civil War: American Civil War in 50 Events: From the Very Beginning to the Fall of the Confederate States (War Books, Civil War History, Civil War Books) (History in 50 Events Series Book 13) World War 1: World War I in 50 Events: From the Very Beginning to the Fall of the Central Powers (War Books, World War 1 Books, War History) (History in 50 Events Series)