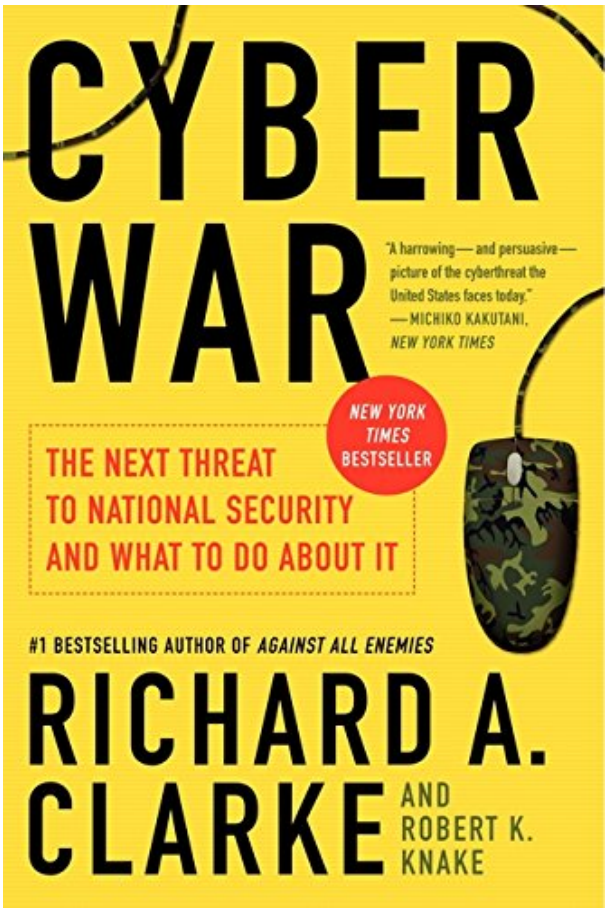
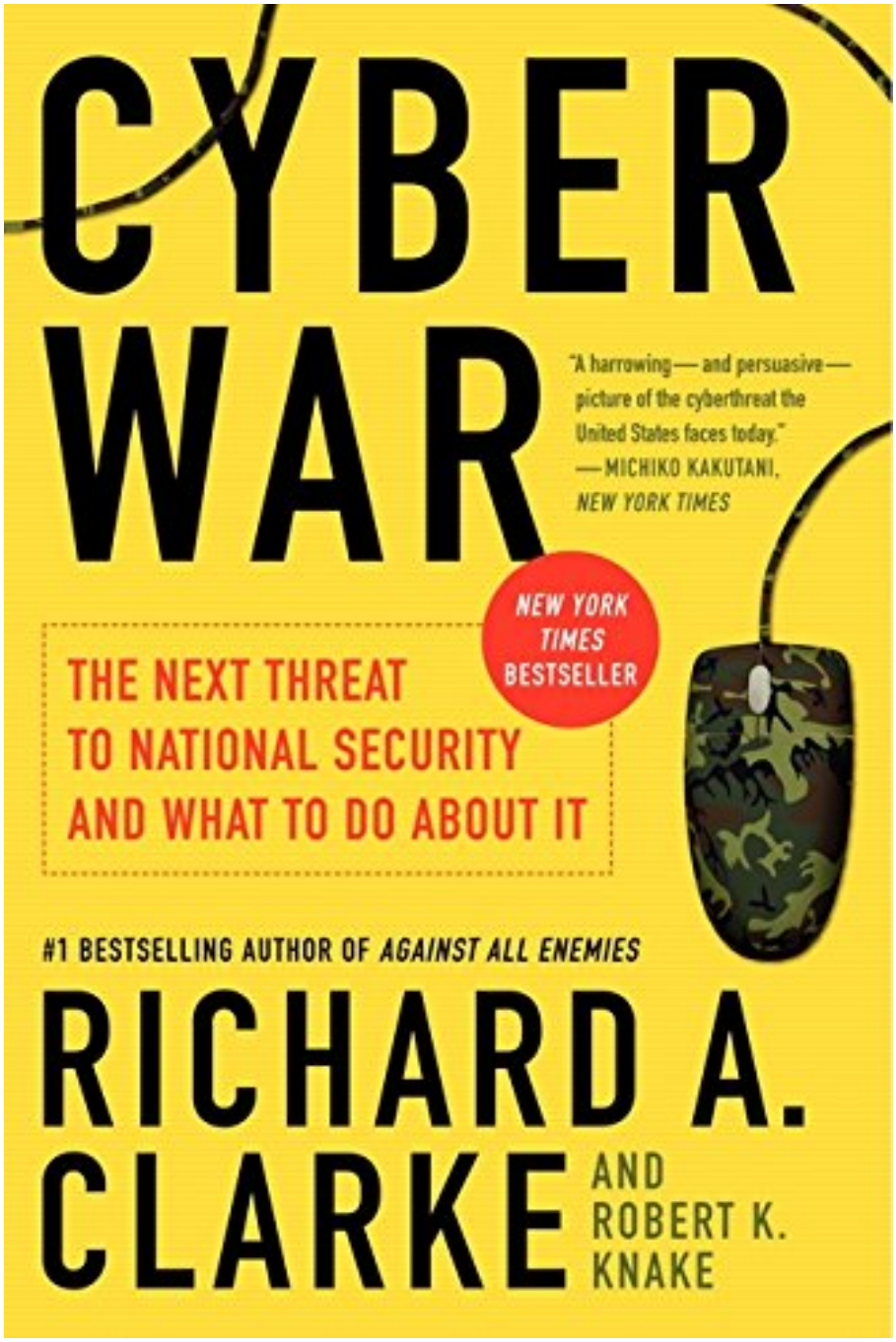
CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT BY RICHARD A. CLARKE, ROBERT KNAKE





CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT BY RICHARD A. CLARKE, ROBERT KNAKE PDF

What kind of book **Cyber War: The Next Threat To National Security And What To Do About It By Richard A. Clarke, Robert Knake** you will favor to? Now, you will not take the published publication. It is your time to get soft data book Cyber War: The Next Threat To National Security And What To Do About It By Richard A. Clarke, Robert Knake rather the published files. You can appreciate this soft file Cyber War: The Next Threat To National Security And What To Do About It By Richard A. Clarke, Robert Knake in whenever you anticipate. Even it remains in expected location as the various other do, you could read guide Cyber War: The Next Threat To National Security And What To Do About It By Richard A. Clarke, Robert Knake in your gadget. Or if you really want more, you can keep reading your computer system or laptop computer to get full display leading. Juts locate it right here by downloading the soft documents Cyber War: The Next Threat To National Security And What To Do About It By Richard A. Clarke, Robert Knake in link web page.

From Publishers Weekly

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.

From Booklist

International security experts—Clarke from the nuclear generation and Knake from the cyber generation—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 another’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 Korea’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

Review
“Chilling... [A] harrowing — and persuasive — picture of the cyberthreat the United States faces today.” (Michiko Kakutani, New York Times)

“Clarke and Knake are right to sound the alarm.” (Wall Street Journal)

“[CYBER WAR] may be the most important book about national-security policy in the last several years.” (Slate)

“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.” (Booklist)

“Will strengthen Clarke’s claims as one of the founding fathers of cybersecurocracy....It is worth buying this book if only for his pithy five-page vision of this coming apocalypse and a return to stone-age conditions within a week, all because of a few pesky hackers and viruses.” (Financial Times)

CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT BY RICHARD A. CLARKE, ROBERT KNAKE PDF

Find out the method of doing something from several sources. One of them is this publication qualify **Cyber War: The Next Threat To National Security And What To Do About It By Richard A. Clarke, Robert Knake** It is an extremely well known book Cyber War: The Next Threat To National Security And What To Do About It By Richard A. Clarke, Robert Knake that can be suggestion to check out now. This recommended book is one of the all great Cyber War: The Next Threat To National Security And What To Do About It By Richard A. Clarke, Robert Knake collections that remain in this website. You will certainly likewise discover various other title as well as motifs from different writers to browse here.

As we stated before, the technology helps us to constantly acknowledge that life will certainly be constantly simpler. Checking out book *Cyber War: The Next Threat To National Security And What To Do About It By Richard A. Clarke, Robert Knake* habit is additionally one of the advantages to obtain today. Why? Technology could be used to supply the publication Cyber War: The Next Threat To National Security And What To Do About It By Richard A. Clarke, Robert Knake in only soft documents system that could be opened up every time you want as well as everywhere you need without bringing this Cyber War: The Next Threat To National Security And What To Do About It By Richard A. Clarke, Robert Knake prints in your hand.

Those are a few of the perks to take when getting this Cyber War: The Next Threat To National Security And What To Do About It By Richard A. Clarke, Robert Knake by on-line. Yet, exactly how is the method to obtain the soft documents? It's extremely right for you to see this page due to the fact that you could obtain the web link web page to download and install guide Cyber War: The Next Threat To National Security And What To Do About It By Richard A. Clarke, Robert Knake Just click the link supplied in this short article and also goes downloading. It will not take significantly time to get this e-book Cyber War: The Next Threat To National Security And What To Do About It By Richard A. Clarke, Robert Knake, like when you need to go with e-book shop.

CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT BY RICHARD A. CLARKE, ROBERT KNAKE PDF

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 America’s vulnerability in a terrifying new international conflict—Cyber War! Every concerned American should read this startling and explosive book that offers an insider’s view of White House ‘Situation Room’ operations and carries the reader to the frontlines of our cyber defense. Cyber War exposes a virulent threat to our nation’s security. This is no X-Files fantasy or conspiracy theory madness—this is real.

- Sales Rank: #40104 in Books
- Brand: Brand: Ecco
- Published on: 2011-08-05
- Released on: 2012-04-10
- Original language: English
- Number of items: 1
- Dimensions: 8.00" h x .72" w x 5.31" l, .51 pounds
- Binding: Paperback
- 320 pages

Features

- Used Book in Good Condition

From Publishers Weekly
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.

From Booklist
International security experts—Clarke from the nuclear generation and Knake from the cyber

generation—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 another'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 Korea'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

Review
"Chilling... [A] harrowing — and persuasive — picture of the cyberthreat the United States faces today." (Michiko Kakutani, New York Times)

"Clarke and Knake are right to sound the alarm." (Wall Street Journal)

"[CYBER WAR] may be the most important book about national-security policy in the last several years." (Slate)

"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." (Booklist)

"Will strengthen Clarke's claims as one of the founding fathers of cybersecurocracy....It is worth buying this book if only for his pithy five-page vision of this coming apocalypse and a return to stone-age conditions within a week, all because of a few pesky hackers and viruses." (Financial Times)

Most helpful customer reviews

174 of 178 people found the following review helpful.
The best I've read on the topic
By Likes to eat Pi
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.

Only then does Clarke begin to go into the technical aspects of cyber attacks, but the technical stuff is very high level (the back cover description explicitly says that this book goes "beyond the geek talk"). He really is just trying to show the potential damage that can be done with cyber attacks. (In other words, this is the part of the book where he tries to scare you).

Clarke then discusses what he views as the primary reasons there has not been significant action in the area of defending against concerted cyber attacks. It is, in my opinion, a very realistic and fair analysis which avoids finger pointing. He then starts to lay out what he feels are reasonable defenses that the US must begin to take.

In the last part of the book he lays out a clear agenda for defending against cyber attacks which includes a mix of regulation (he admits it's a dirty word but thinks it's necessary), more technical controls at major network boundaries, and an expanded scope for DHS to protect the civilian infrastructure too. He also discusses international arms control treaties, and appears to be a big fan of some international cyber war treaties, which, like nuclear arms control treaties from a generation ago, could be used to create "rules of the game" for international war.

As I said, in the beginning, this is without a doubt the best piece on cyber war I've ever read. He really does an excellent job of covering everything from the history to the players to the regulations to the endless possibilities. The one place where I feel he misses the boat is in some of the technical aspects. He admits to not being a technical person, and does make a few technical errors, although they're all far too minor to be worth mentioning. My real issue is that in all his scenarios he starts with the assumption that every combatant (like, say, the USA and China) have successfully hacked into every network that the other side controls, and left backdoors to get back in. Further, none of these back doors have been discovered and removed. As someone who does this for a living, I can assure you it's not that simple. While I have no doubt that a government spending considerable resources could certainly gain access to many networks in a relatively short period of time, and if they left backdoors some might not be discovered, if someone left too many backdoors some would certainly be discovered. Breaking in is not as simple as just pushing a button like it is in the movies - in fact, recent studies have shown that the average security breach is the result of four separate mistakes. While mistakes are made all the time (which means that breaches occur all the time _somewhere_), it's much harder to cause breaches in every system you target all at once. In several places, Clarke's dire warnings fall into the trap of imitating movies more than real life. I will admit that as a technical person this is my bias showing, and I realize that this book is still largely intended to be a policy one, which is why I still give it a very positive rating. I would simply be remiss if I let this pass unmentioned.

92 of 102 people found the following review helpful.
Easy to Read..... and Scary!
By Amazon Customer
Richard Clarke's credentials are well established, having been a national security advisor to presidents of both parties, his viewpoints are his own, not politically-driven ideology.

Clarke takes the time to go over the basics of the cyber-universe for those that are not especially net-savvy, and then gets into the meat of the what, who, where and how (the "when" is the big question of course) of potential cyber attacks against the US. He gives a bit of history on attacks that have already happened, and a few that have failed.

I say the information is a bit scary because, even with a degree in Computer Science, I did not know the extent to which the Internet connects and controls so many aspects of our daily lives; in business as well as in our personal lives. More and more machines and appliances are being built with the capability to "talk" to the manufacturers who make them, a legitimate and smart way to diagnose problems and download fixes.... but the idea that the new copy machine in my home office might be hacked, and ordered to malfunction to the point that it catches on fire, is unsettling to say the least.

This is a good book, a page turner, and delivers information every 21st Century American should know.

84 of 94 people found the following review helpful.
worth reading, but with a big grain of salt
By Adam Thierer
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. And most ISPs take steps not just to guard against malware and other types of cyber attacks, but they also offer customers free (or cheap) security software as part of a growing suite of gratis services (anti-virus, parental controls, e-mail, etc).

Clarke and Knake would like to see government impose a fairly sweeping set of new rules on ISPs to better secure their networks against potential attacks. In true deputize-the-middleman fashion, they want ISPs to engage in a great deal more network monitoring (using deep-packet inspection techniques) under threat of legal sanction if things go wrong. They admit there are corresponding costs and privacy concerns, but largely dismiss them and essentially ask us to just get over those concerns in the name of a safer and more secure cyberspace. They do, however, say they would be willing to have a "Privacy and Civil Liberties Board" appointed "to ensure that neither the ISPs nor the government was illegal spying on us." I doubt that will soothe the fears of those who (like me) are fundamentally suspicious of government snooping.

Overall, Clarke and Knake have written a book that is worth reading, but suffers from hyperbolic rhetoric and a serious lack of documentation. Readers should also seek out other perspectives on cyber-security issues, which take a more reasoned approach to the issue.

See all 248 customer reviews...

CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT BY RICHARD A. CLARKE, ROBERT KNAKE PDF

This is likewise one of the factors by getting the soft documents of this Cyber War: The Next Threat To National Security And What To Do About It By Richard A. Clarke, Robert Knake by online. You may not need more times to invest to visit guide shop and look for them. Sometimes, you also do not locate the book Cyber War: The Next Threat To National Security And What To Do About It By Richard A. Clarke, Robert Knake that you are looking for. It will certainly squander the moment. However below, when you see this web page, it will be so easy to obtain and also download and install guide Cyber War: The Next Threat To National Security And What To Do About It By Richard A. Clarke, Robert Knake It will certainly not take often times as we explain before. You could do it while doing something else at residence or perhaps in your office. So simple! So, are you question? Simply exercise what we provide here and check out **Cyber War: The Next Threat To National Security And What To Do About It By Richard A. Clarke, Robert Knake** what you enjoy to check out!

From Publishers Weekly
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.

From Booklist
International security experts—Clarke from the nuclear generation and Knake from the cyber generation—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 another’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 Korea’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

Review
“Chilling... [A] harrowing — and persuasive — picture of the cyberthreat the United States faces today.” (Michiko Kakutani, New York Times)

“Clarke and Knake are right to sound the alarm.” (Wall Street Journal)

“[CYBER WAR] may be the most important book about national-security policy in the last several years.” (Slate)

“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.” (Booklist)

“Will strengthen Clarke’s claims as one of the founding fathers of cybersecurocracy....It is worth buying this book if only for his pithy five-page vision of this coming apocalypse and a return to stone-age conditions within a week, all because of a few pesky hackers and viruses.” (Financial Times)

What kind of book **Cyber War: The Next Threat To National Security And What To Do About It By Richard A. Clarke, Robert Knake** you will favor to? Now, you will not take the published publication. It is your time to get soft data book Cyber War: The Next Threat To National Security And What To Do About It By Richard A. Clarke, Robert Knake rather the published files. You can appreciate this soft file Cyber War: The Next Threat To National Security And What To Do About It By Richard A. Clarke, Robert Knake in whenever you anticipate. Even it remains in expected location as the various other do, you could read guide Cyber War: The Next Threat To National Security And What To Do About It By Richard A. Clarke, Robert Knake in your gadget. Or if you really want more, you can keep reading your computer system or laptop computer to get full display leading. Juts locate it right here by downloading the soft documents Cyber War: The Next Threat To National Security And What To Do About It By Richard A. Clarke, Robert Knake in link web page.