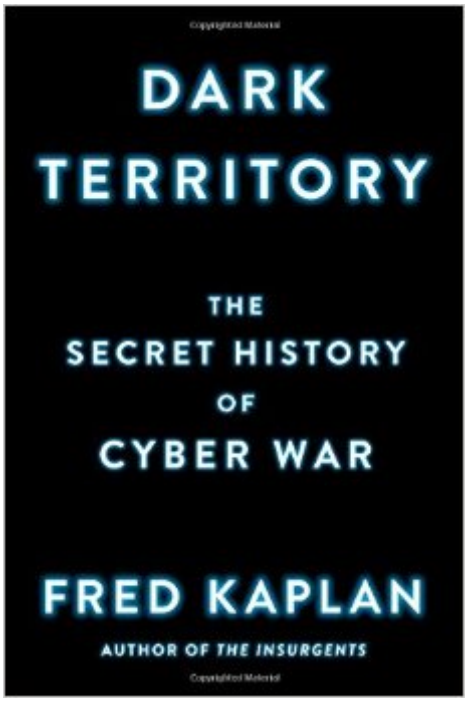
The book was found

Dark Territory: The Secret History Of Cyber War



PDF
Adobe
DOWNLOAD EBOOK

Synopsis

â œA consistently eye-opening history...not just a page-turner but consistently surprising.â • â ”The New York Times â œA book that grips, informs, and alarms, finely researched and lucidly related.â • â ”John le CarrÃ© As cyber-attacks dominate front-page news, as hackers join terrorists on the list of global threats, and as top generals warn of a coming cyber war, few books are more timely and enlightening than Dark Territory: The Secret History of Cyber War, by Slate columnist and Pulitzer Prizeâ “winning journalist Fred Kaplan.Kaplan probes the inner corridors of the National Security Agency, the beyond-top-secret cyber units in the Pentagon, the "information warfare" squads of the military services, and the national security debates in the White House, to tell this never-before-told story of the officers, policymakers, scientists, and spies who devised this new form of warfare and who have been planningâ ”and (more often than people know) fightingâ ”these wars for decades. From the 1991 Gulf War to conflicts in Haiti, Serbia, Syria, the former Soviet republics, Iraq, and Iran, where cyber warfare played a significant role, Dark Territory chronicles, in fascinating detail, a little-known past that shines an unsettling light on our future.

Book Information

Hardcover: 352 pages

Publisher: Simon & Schuster (March 1, 2016)

Language: English

ISBN-10: 1476763259

ISBN-13: 978-1476763255

Product Dimensions: 6 x 1 x 9 inches

Shipping Weight: 1.2 pounds (View shipping rates and policies)

Average Customer Review: 4.4 out of 5 starsÂ Â See all reviewsÂ (79 customer reviews)

Best Sellers Rank: #12,401 in Books (See Top 100 in Books) #4 inÂ Books > Textbooks > Social Sciences > Military Sciences #5 inÂ Books > Computers & Technology > Security & Encryption > Viruses #12 inÂ Books > Textbooks > Humanities > History > Military

Customer Reviews

I spent over two years producing a feature documentary for Alex Gibney called "Zero Days," about the use of cyber means in warfare. The day before our premiere at the Berlin Film Festival, the New York Times reported on one of our findings, the discovery of a classified program at U.S. Cyber Command and NSA, codeword Nitro Zeus, focused on waging a massive cyber war campaign against Iran.I say this simply so I can emphasize the following: I wish that we had had Fred Kaplan’s

"Dark Territory" when we began work on our film.The use of cyber attack by the military is a topic cloaked in secrecy, a topic that many at the very highest levels of government remain fearful to speak about even in scant outlines. It was only through years of painstaking journalistic work by a team of investigators that we could piece together the understanding of the cyber world that allowed us to make our film, including the crucial awareness of the deep history that led to operations like Olympic Games and Nitro Zeus. Kaplan has performed a tremendous service by making that history plain to the public here in this book.For those interested in the history of the subject, the books that are worth reading are few. Jay Healey's "A Fierce Domain" and Shane Harris's "@War" are excellent complements to Kaplan. I expect Thomas Rid's upcoming book will join that list.But start with Kaplan. He has details you won't find elsewhere, and tells the story with characteristic skill. Knowing how heavy that cloak of secrecy weighs on the people who have worked behind it, I am impressed by what Kaplan has achieved here, and I highly recommend the book.

After recently reading Robert Gates: Passion for Leadership book, I was enthralled with this Fred Kaplan tome, Ã¢Â ÂœDark TerritoryÃ¢Â Â•, especially since Robert Gates (Former Defense Secretary and Director of the CIA) referred to the online cyber world as the Dark Territory. Its aptly named and has long been a personal belief of mine since before the world wide web existed, when the internet was a vast majority of random servers and bulletin board systems. Even at that point, it was filled to the brim with persons and groups of individuals hacking and forging their way through the original emptiness of what we have come to know as todayÃ¢Â Â™s internet.Since the dawn of that existence, both sides have been at war, a cyberwar between good and evil, dark and light, knowledge and secrecy. It has always been an avid interest of mine to go deeper into this realm and now Kaplan, a Pulitzer prize winning author brings us into the climax of it.I say highlights because Kaplan starts off by bringing us into how President Reagan initially jumped on board while viewing the movie War Games with Matthew Broderick and wondering if this could actually happen and the answer was a resounding Ã¢Â Âœyes.Ã¢Â Â•I say highlights because Kaplan traverses this ground and jumps throughout the internetÃ¢Â Â™s history recalling many stories, interviews with anonymous hackers and although he has a great depth to his reporting, in my view, he is just scratching the surface in relation to many issues and histories of the battleground that is cyberspace.For those that are unfamiliar with a lot of the history, events and inner workings of what takes place, he does a fantastic job, spotlighting some pivotal moments to help these readers be aware of what goes on in Ã¢Â ÂœDark TerritoryÃ¢Â Â• Since before the world web existed, our government has largely tapped into a venerable resource for both offensive attacks and defensive

efforts to protect our national security. Even though the internet has opened a global stage for other countries trying to accomplish the same goals, it is an extensively daunting battle uphill. This totality of cyber wars has outrun our conventional wars and will continue to be on the upstroke.Even so, Kaplan kept me interested with tidbits of information from Reagan and Ã¢Â ÂœWar Games" to Ã¢Â ÂœSneakersÃ¢Â Â• and the NSA, showing the screenwriters for both and how they were intimately tied in with the RAND corporation and how they took cues from one of the original programmers for the North American Aerospace Defense Command computer, and never knew that he was also on an advisory board to the National Security Agency.These tidbits, highlights and coincidences form a lot of the interweaving of the book, even though Kaplan jumps back and forth through different eras to show us this. He touches on various Presidents and how they viewed cybersecurity and their reasoning for and/or against, throughout history. He brings us on varying accounts of how our government averts disaster, as well as how they have mounted attacks. He talks about Edward Snowden and President ObamaÃ¢Â Â™s reactions to the same. Corporate securities, attacks on various corporations (eBay, Sony, Target and many others), banks and generally anything in between. He brings to light, the theme of protecting our nation while balancing our civil liberties, as we are currently seeing now with the Apple quagmire of recent weeks. The book is filled with complexities and is well told and researched by Kaplan.I believe as I said before, that this just brings to light, a surface view of what is really transpiring daily, on the world wide web. There are so many factors to counter in, with cyber attacks and cyber sabotage, both inward and outward, in between corporations, individuals and government. There is the Ã¢Â ÂœDeep WebÃ¢Â Â• running its underground drug trade, credit card fraud trades, human trafficking and much more throughout the world on anonymous TOR servers. The new currency of the criminal world, as Bitcoin has shown us and since most of the credit card fraud trade is Russian and Chinese based, it effectually is bringing about a new world war throughout cyberspace that we have to consistently be aware of, reminiscent of our intelligence operations in the Cold War.There are simply too many factors to this Ã¢Â ÂœDark TerritoryÃ¢Â Â• to cover effectively in one book, but I really enjoyed that Kaplan has directed our attention to a taste of it for us. Especially for those reading the book, that do not have this knowledge beforehand, it is an eye opening tour for most readers.

Occasionally, I come across a book on an important topic thatÃ¢Â Â™s crammed with information I was able to find nowhere else Ã¢Â Â” but is a chore to read. Even though it is not an academic study but clearly intended for a general audience, Fred KaplanÃ¢Â Â™s recent history of cyber war,

Dark Territory, is one such book.A story stretching over five decadesUnlike previous treatments that IÃ¢Â Â™ve read about the topic, which zero in on the vulnerability of the American economy to attacks through cyberspace, Dark Territory traces the history of our governmentÃ¢Â Â™s slowly growing awareness of the threat, beginning nearly half a century ago. Then, a prescient Pentagon scientist wrote a paper warning about the dangers inherent in computer networks. Apparently, though, no one in a position to do anything about it paid much attention to him.Kaplan identifies an incident fully fifteen years later in 1984 when President Ronald Reagan Ã¢Â Â" a movie fan, of course Ã¢Â Â" saw the film War Games. He queried the chairman of the Joint Chiefs of Staff at a top-level White House meeting whether it was possible for a teenager like the one portrayed in the film by Matthew Broderick to hack into sensitive Pentagon computers. When the chairman, General John Vessey, reported some time later that the feat was in fact possible, Reagan called for and later signed the governmentÃ¢Â Â™s first policy directive on the topic of cyber war. But that, too, led to no significant change at the Pentagon or anywhere else in the federal government.Dark Territory is filled with revealing anecdotes like this, based on what surely was top-secret information not long ago. Kaplan reveals many little-known details about the Russian cyber war on Estonia and Ukraine, the Chinese ArmyÃ¢Â Â™s prodigious hacking of American corporations and the Pentagon, the massive North Korean assault on Sony, IranÃ¢Â Â™s disabling of 20,000 computers in Sheldon AdelsonÃ¢Â Â™s casino empire, and the successful US-Israeli attack on IranÃ¢Â Â™s nuclear infrastructure. Kaplan also reveals the reason why US complaints about ChinaÃ¢Â Â™s cyber attacks have fallen on deaf ears: it turns out that the National Security Agency is attacking the Chinese government in much the same way. As The Guardian revealed in 2013, Ã¢Â Âœthe NSA had launched more than 61,000 cyber operation, including attacks on hundreds of computers in Hong Kong and mainland China.Ã¢Â Â•The book casts a particularly harsh light on the Administration of George W. Bush. Bush, Cheney, Rumsfeld, and other senior officials in the early 2000s cavalierly dismissed urgent reports from national security and intelligence officials that the threat of cyber war, and the vulnerability of the US economy, were growing at an alarming rate. Only under BushÃ¢Â Â™s successor did reality strongly take hold. As Kaplan writes, Ã¢Â ÂœDuring Barack ObamaÃ¢Â Â™s presidency, cyber warfare took off, emerging as one of the few sectors in the defense budget that soared while others stayed stagnant or declined.Ã¢Â Â•ItÃ¢Â Â™s difficult to understand how anyone who was awake could have failed to grasp the problem. For example, a war game conducted in 1997 was intended to test the vulnerability of the PentagonÃ¢Â Â™s computer systems within two weeks. Ã¢Â ÂœBut the game was over Ã¢Â Â" the entire defense establishmentÃ¢Â Â™s network was penetrated Ã¢Â Â" in four days. The National Military

Command Center Ã¢Â Â” the facility that would transmit orders from the president of the United States in wartime Ã¢Â Â” was hacked on the first day. And most of the officers manning those servers didnÃ¢Â Â™t even know theyÃ¢Â Â™d been hacked.Ã¢Â Â• Not long afterwards, the Pentagon was hacked in a similar way by two 16-year-old boys in San Francisco. And when national security officials widened the scope of their attention to encompass the countryÃ¢Â Â™s critical civilian infrastructure, such as the electricity grid, they were shocked to discover that the situation was far worse. The Pentagon eventually bowed to the warnings and implemented needed security measures. But private corporations blatantly refused to do so because they didnÃ¢Â Â™t want to spend the money Ã¢Â Â” and Congress declined to allow the federal government to make security measures obligatory.Unfortunately, KaplanÃ¢Â Â™s book is poorly organized. ItÃ¢Â Â™s roughly structured along chronological lines but jumps back and forth through time with such regularity as to be dizzying. And itÃ¢Â Â™s crammed so full of the names of sometimes obscure government officials and military officers that it becomes even more difficult to follow the thread of the story.However, these challenges aside, a picture clearly emerges from Dark Territory: For decades the American public has been at the mercy of incompetent and pigheaded people in sensitive positions in the government, the military, and private industry Ã¢Â Â” and we still are. Bureaucratic games proliferate. Politics intrude. Inter-service rivalries abound. Personal grudges get in the way. Repeatedly, some of those who are entrusted with the security of the American people make what even at the time could easily be seen as stupid decisions.Other takes on cyber warLast year I read and reviewed a book titled Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It, by Marc Goodman. I described it as Ã¢Â Âœthe scariest book IÃ¢Â Â™ve read in years.Ã¢Â Â•Five years earlier, I read Cyber War: The Next Threat to National Security and What to Do About It, by Richard A. Clarke and Robert K. Knake. From the early 1970s until George W. BushÃ¢Â Â™s invasion of Iraq, Clarke filled high-level national security positions under seven Presidents, so he knows whereof he writes. (He resigned in protest over the invasion of Iraq, which he thought distracted the government from the real threats facing the country.) Not long afterward, I read and reviewed Worm: The First Digital World War, by Mark Bowden, a much more focused treatment of the topic Ã¢Â Â” a case study, really Ã¢Â Â” but equally unsettling.Though less current, all three of these books are better organized and more readable than Dark Territory. Admittedly, though, KaplanÃ¢Â Â™s book reveals the history that is only hinted at in the others.About the authorFred Kaplan wrote five previous books about the nuclear arms race and other topics bearing on US national security. He was on a team at the Boston Globe in 1983 that won a Pulitzer Prize for a series about the nuclear arms race.

Download to continue reading...

Dark Territory: The Secret History of Cyber War Cyber-Safe Kids, Cyber-Savvy Teens: Helping Young People Learn To Use the Internet Safely and Responsibly Top Secret Files: The Civil War: Spies, Secret Missions, and Hidden Facts from the Civil War (Top Secret Files of History) Cyber War: The Next Threat to National Security and What to Do About It ManSpace: A Primal Guide to Marking Your Territory Our Indian Summer in the Far West: An Autumn Tour of Fifteen Thousand Miles in Kansas, Texas, New Mexico, Colorado, and the Indian Territory (The ... on Art and Photography of the American West) The Map and the Territory: Risk, Human Nature, and the Future of Forecasting Canoeing the Mountains: Christian Leadership in Uncharted Territory Virgin Territory: Exploring the World of Olive Oil Urban Survival Handbook: The Beginners Guide to Securing Your Territory, Food and Weapons (How to Survive Your First Disaster) Chaos, Territory, Art: Deleuze and the Framing of the Earth (The Wellek Library Lectures) Virgin Territory The Map and the Territory 2.0: Risk, Human Nature, and the Future of Forecasting But He Doesn't Know the Territory The Indians of Cape Flattery: At the Entrance to the Strait of Fuca, Washington Territory Cyber Design: Illustration: The Best Computer Generated Design Cyber Bullying No More: Parenting A High Tech Generation (Growing with Love) Cyber Commerce Reframing CCFP Certified Cyber Forensics Professional All-in-One Exam Guide Cyber bullying (Introducing Issues with Opposing Viewpoints)

Dmca