



Dark Territory: The Secret History of Cyber War

By Fred Kaplan

Download now

Read Online ➔

Dark Territory: The Secret History of Cyber War By Fred Kaplan

“A consistently eye-opening history...not just a page-turner but consistently surprising.” —*The New York Times*

“A book that grips, informs, and alarms, finely researched and lucidly related.” —John le Carré

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 Prize-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 planning—and (more often than people know) fighting—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.

↓ [Download Dark Territory: The Secret History of Cyber War ...pdf](#)

📖 [Read Online Dark Territory: The Secret History of Cyber War ...pdf](#)

Dark Territory: The Secret History of Cyber War

By Fred Kaplan

Dark Territory: The Secret History of Cyber War By Fred Kaplan

“A consistently eye-opening history...not just a page-turner but consistently surprising.” —*The New York Times*

“A book that grips, informs, and alarms, finely researched and lucidly related.” —John le Carré

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 Prize-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 planning—and (more often than people know) fighting—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.

Dark Territory: The Secret History of Cyber War By Fred Kaplan Bibliography

- Sales Rank: #37355 in Books
- Brand: Simon Schuster
- Published on: 2016-03-01
- Released on: 2016-03-01
- Original language: English
- Number of items: 1
- Dimensions: 9.00" h x 1.00" w x 6.00" l, .0 pounds
- Binding: Hardcover
- 352 pages



[Download Dark Territory: The Secret History of Cyber War ...pdf](#)



[Read Online Dark Territory: The Secret History of Cyber War ...pdf](#)

Editorial Review

Review

“A consistently eye-opening history of our government’s efforts to effectively manage our national security in the face of the largely open global communications network established by the World Wide Web. . . . The great strengths of *Dark Territory* . . . are the depth of its reporting and the breadth of its ambition. . . . The result is not just a page-turner but consistently surprising. . . . One of the most important themes that emerges from Mr. Kaplan’s nuanced narrative is the extent to which defense and offense are very much two sides of the same coin. . . . The biggest surprise of *Dark Territory* is the identity of the most prominent domestic heroes and villains in the “secret history.” . . . *Dark Territory* is the rare tome that leaves the reader feeling generally good about their civilian and military leadership.” (*The New York Times*)

“Comprehensively reported history . . . The book’s central question is how should we think about war, retaliation, and defense when our technologically advanced reliance on computers is also our greatest vulnerability?” (*The New Yorker*)

“A book that grips, informs and alarms, finely researched and lucidly related.” (John le Carré)

“*Dark Territory* captures the troubling but engrossing narrative of America’s struggle to both exploit the opportunities and defend against the risks of a new era of global cyber-insecurity. Assiduously and industriously reported. . . . Kaplan recapitulates one hack after another, building a portrait of bewildering systemic insecurity in the cyber domain. . . . One of the deep insights of *Dark Territory* is the historical understanding by both theorists and practitioners that cybersecurity is a dynamic game of offense and defense, each function oscillating in perpetual competition.” (*The Washington Post*)

“An important, disturbing, and gripping history arguing convincingly that, as of 2015, no defense exists against a resourceful cyberattack.” (*Kirkus Reviews, starred review*)

"*Dark Territory* offers thrilling insights into high-level politics, eccentric computer hackers and information warfare. In 15 chapters—some of them named after classified codenames and official (and unofficial) hacking exercises—Kaplan has encapsulated the past, present and future of cyber war." (*The Financial Express*)

“The best account to date of the history of cyber war...a human story: a history as revealed by the people involved in shaping it...full of detail, including information that will be new even to insiders.” (*The Times Literary Supplement*)

“Kaplan dives into a topic which could end up being just as transformational to national security affairs as the nuclear age was. The book opens fast and builds from there, providing insights from research that even professionals directly involved in cyber operations will not have gleaned. . . . You will love this book.” (Bob Gourley *CTOvision.com*)

“The best available history of the U.S. government’s secret use of both cyber spying, and efforts to use its computer prowess for more aggressive attacks. . . . Contains a number of fascinating, little-known stories about the National Security Agency and other secret units of the U.S. military and intelligence community. . . . An especially valuable addition to the debate.” (John Sipher *Lawfare*)

“Fascinating . . . To understand how deeply we have drifted into legally and politically uncharted waters, read Kaplan’s new book, *Dark Territory: The Secret History of Cyber War*.” (George F. Will *The Washington Post*)

“Deeply sourced. Luckily, he’s not slavishly loyal to his sources.” (*Pittsburgh Post-Gazette*)

EDITORS' CHOICE (*New York Times Book Review*)

"Fred Kaplan’s *Dark Territory* may become a classic reference for scholars and students seeking to understand the complicated people who ushered the United States into the cyber-conflict era and the tough decisions they made." (Rear Admiral Grace Hopper, Director, Center for Cyber Conflict, US Naval War College *Proceedings of the U.S. Naval Institute*)

“Chilling . . . Kaplan is one of America’s leading writers on national security, and his accounts of cyberattacks are gripping . . . assiduously researched.” (Edward Lucas *The Times (London)*)

“Peppered with many fascinating behind-the-scenes anecdotes . . . A readable and informative history.” (P.W. Singer *The New York Times Book Review*)

A “Hot Type” Book Pick for March 2016 (*Vanity Fair*)

A “Hot Tech Book of 2016” (*Tech Republic*)

“Worthy of any spy thriller. . . a strong narrative flow . . . impressively detailed . . . deeply relevant . . . vital.” (*The National (UAE)*)

“Jarring . . . a rich, behind-the-headlines history of our government’s efforts to make policy for the jaw-dropping vulnerabilities of our ever-increasing dependence on computers. . . . Kaplan renders a vivid account of the long struggle waged by presidents, bureaucrats, generals, private-sector CEOs, and privacy advocates . . . Kaplan enjoys considerable credibility in defense circles, but he guides us through the dark territory of cyber conflict with an omniscient-narrator voice reminiscent of Bob Woodward’s behind-the-scenes books. . . . Today, Kaplan argues, it is precisely U.S. pre-eminence in the network connectivity that makes us the most vulnerable target in the world to cyber sabotage.” (*Washington Independent Review of Books*)

“Pulitzer-prizewinning journalist Fred Kaplan’s taut, urgent history traces the dual trajectory of digital surveillance and intervention, and high-level US policy from the 1980s on.” (*NATURE*)

“*Dark Territory* is a remarkable piece of reporting. Fred Kaplan has illuminated not merely the profound vulnerabilities of our nation to cyber warfare, but why it has taken so long for our policy-makers to translate indifference into concern and concern into action. This is a vitally important book by a meticulous journalist.” (Ted Koppel, author of *Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath*)

“A fascinating account of the people and organizations leading the way towards a cyber war future.” (Dorothy E. Denning, author of *Information Warfare and Security*, 1st Inductee, National Cyber Security Hall of Fame)

“Everyone has heard the term 'cyber warfare.' Very few people could explain exactly what it means and why it matters. *Dark Territory* solves that problem with an account that is both fascinating and authoritative. Fred

Kaplan has put the people, the technologies, the dramatic turning points, and the strategic and economic stakes together in a way no author has done before.” (James Fallows, national correspondent, *The Atlantic*)

“Revealing. . . . On a vital current-events topic, the well-connected Kaplan’s well-sourced history gives readers much to ponder.” (*Booklist*)

“Chilling” (*Haaretz*)

“A very in-depth work... its content is enlightening and intelligent and the secrets it uncovers are astounding.” (*The News Hub*)

Praise for *The Insurgents*:

“Thrilling reading . . . A fascinating history . . . *The Insurgents* proceeds like a whodunit . . . An authoritative, gripping and somewhat terrifying account of how the American military approached two major wars in the combustible Islamic world . . . There is no one better equipped to tell the story than Fred Kaplan, a rare combination of defense intellectual and pugnacious reporter . . . He brings genuine expertise to his fine storytelling.” (*NYT Book Review*)

“One of the very best books ever written about the American military in the era of small wars . . . Fred Kaplan brings a formidable talent for writing intellectual history.” (*The New York Review of Books*)

“Excellent . . . An intellectual thriller.” (*Time*)

“Excellent . . . Poignant and timely . . . A good read, rich in texture and never less than wise.” (*Foreign Policy*)

Praise for *Daydream Believers*:

“Illuminating . . . incisive.” (*The New York Times*)

“Excellent and devastating . . . Go, please, and buy Kaplan’s book. His great work deserves attention and reward.” (*Time*)

“Fred Kaplan has long been one of our most incisive thinkers about strategic issues. In this provocative book, he challenges many of our assumptions about the post-9/11 world and offers a dose of realism about the way the world actually works after the end of the Cold War. It’s a bracing read.” (Walter Isaacson)

Praise for *The Wizards of Armageddon*:

“Fascinating . . . It contains much that is not only new but stunning about the nation’s official thinking and planning for nuclear war.” (*Washington Post Book World*)

“An absorbing work . . . The story of the remarkable civilians who developed the novel field of nuclear strategy—men such as Bernard Brodie, William Kaufmann, Albert Wohlstetter, and Herman Kahn—is told admirably well. Even those who are familiar with this story will find fascinating details here.” (*Foreign Affairs*)

“[The] definitive intellectual history of early nuclear deterrence.” (Steve Coll, author of *Ghost Wars*)

About the Author

Fred Kaplan is the national-security columnist for *Slate* and the author of five books, including *Dark Territory: The Secret History of Cyber War*; *The Wizards of Armageddon*; *1959*; *Daydream Believers*; and *The Insurgents: David Petraeus and the Plot to Change the American Way of War*, which was a *New York Times* bestseller and Pulitzer Prize finalist. A former Pulitzer Prize–winning reporter for *The Boston Globe*, he graduated from Oberlin College, earned a PhD from MIT, and lives in Brooklyn with his wife, Brooke Gladstone.

Excerpt. © Reprinted by permission. All rights reserved.

Dark Territory

CHAPTER 1

“COULD SOMETHING LIKE THIS REALLY HAPPEN?”

IT was Saturday, June 4, 1983, and President Ronald Reagan spent the day at Camp David, relaxing, reading some papers, then, after dinner, settling in, as he often did, to watch a movie. That night’s feature was *WarGames*, starring Matthew Broderick as a tech-whiz teenager who unwittingly hacks into the main computer at NORAD, the North American Aerospace Defense Command, and, thinking that he’s playing a new computer game, nearly triggers World War III.

The following Wednesday morning, back in the White House, Reagan met with the secretaries of state, defense, and treasury, his national security staff, the chairman of the Joint Chiefs of Staff, and sixteen prominent members of Congress, to discuss a new type of nuclear missile and the prospect of arms talks with the Russians. But he couldn’t get that movie out of his mind. At one point, he put down his index cards and asked if anyone else had seen it. Nobody had (it had just opened in theaters the previous Friday), so he launched into a detailed summary of its plot. Some of the legislators looked around the room with suppressed smiles or arched eyebrows. Not quite three months earlier, Reagan had delivered his “Star Wars” speech, calling on scientists to develop laser weapons that, in the event of war, could shoot down Soviet nuclear missiles as they darted toward America. The idea was widely dismissed as nutty. What was the old man up to now?

After finishing his synopsis, Reagan turned to General John Vessey, the chairman of the Joint Chiefs, the U.S. military’s top officer, and asked, “Could something like this really happen?” Could someone break into our most sensitive computers?

Vessey, who’d grown accustomed to such queries, said he would look into it.

One week later, the general came back to the White House with his answer. *WarGames*, it turned out, wasn’t at all far-fetched. “Mr. President,” he said, “the problem is much worse than you think.”

Reagan’s question set off a string of interagency memos, working groups, studies, and meetings, which culminated, fifteen months later, in a confidential national security decision directive, NSDD-145, signed September 17, 1984, titled “National Policy on Telecommunications and Automated Information Systems Security.”

It was a prescient document. The first laptop computers had barely hit the market, the first public Internet providers wouldn’t come online for another few years. Yet the authors of NSDD-145 noted that these new

devices—which government agencies and high-tech industries had started buying at a rapid clip—were “highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation.” Hostile foreign intelligence agencies were “extensively” hacking into these services already, and “terrorist groups and criminal elements” had the ability to do so as well.

This sequence of events—Reagan’s oddball question to General Vessey, followed by a pathbreaking policy document—marked the first time that an American president, or a White House directive, discussed what would come to be called “cyber warfare.”

The commotion, for now, was short-lived. NSDD-145 placed the National Security Agency in charge of securing all computer servers and networks in the United States, and, for many, that went too far. The NSA was America’s largest and most secretive intelligence agency. (Insiders joked that the initials stood for “No Such Agency.”) Established in 1952 to intercept foreign communications, it was expressly forbidden from spying on Americans. Civil liberties advocates in Congress were not about to let a presidential decree blur this distinction.

And so the issue vanished, at least in the realm of high-level politics. When it reemerged a dozen years later, after a spate of actual cyber intrusions during Bill Clinton’s presidency, enough time had passed that the senior officials of the day—who didn’t remember, if they’d ever known of, NSDD-145—were shocked by the nation’s seemingly sudden vulnerability to this seemingly brand-new threat.

When the White House again changed hands (and political parties) with the election of George W. Bush, the issue receded once more, at least to the public eye, especially after the terrorist attacks of September 11, 2001, which killed three thousand Americans. Few cared about hypothetical cyber wars when the nation was charging into real ones with bullets and bombs.

But behind closed doors, the Bush administration was weaving cyber war techniques with conventional war plans, and so were the military establishments of several other nations, friendly and otherwise, as the Internet spread to the globe’s far-flung corners. Cyber war emerged as a mutual threat and opportunity, a tool of espionage and a weapon of war, that foes could use to hurt America and that America could use to hurt its foes.

During Barack Obama’s presidency, cyber warfare took off, emerging as one of the few sectors of the defense budget that soared while others stayed stagnant or declined. In 2009, Obama’s first secretary of defense, Robert Gates, a holdover from the Bush years, created a dedicated Cyber Command. In its first three years, the command’s annual budget tripled, from \$2.7 billion to \$7 billion (plus another \$7 billion for cyber activities in the military services, all told), while the ranks of its cyber attack teams swelled from 900 personnel to 4,000, with 14,000 foreseen by the end of the decade.

The cyber field swelled worldwide. By the midpoint of Obama’s presidency, more than twenty nations had formed cyber warfare units in their militaries. Each day brought new reports of cyber attacks, mounted by China, Russia, Iran, Syria, North Korea, and others, against the computer networks of not just the Pentagon and defense contractors but also banks, retailers, factories, electric power grids, waterworks—everything connected to a computer network, and, by the early twenty-first century, that included nearly everything. And, though much less publicized, the United States and a few other Western powers were mounting cyber attacks on other nations’ computer networks, too.

In one sense, these intrusions were nothing new. As far back as Roman times, armies intercepted enemy communications. In the American Civil War, Union and Confederate generals used the new telegraph

machines to send false orders to the enemy. During World War II, British and American cryptographers broke German and Japanese codes, a crucial ingredient (kept secret for many years after) in the Allied victory. In the first few decades of the Cold War, American and Russian spies routinely intercepted each other's radio signals, microwave transmissions, and telephone calls, not just to gather intelligence about intentions and capabilities but, still more, to gain an advantage in the titanic war to come.

In other ways, though, information warfare took on a whole new dimension in the cyber age. Until the new era, the crews gathering SIGINT—signals intelligence—tapped phone lines and swept the skies for stray electrons, but that's all they could do: listen to conversations, retrieve the signals. In the cyber age, once they hacked a computer, they could prowl the entire network connected to it; and, once inside the network, they could not only read or download scads of information; they could change its content—disrupt, corrupt, or erase it—and mislead or disorient the officials who relied on it.

Once the workings of almost everything in life were controlled by or through computers—the guidance systems of smart bombs, the centrifuges in a uranium-enrichment lab, the control valves of a dam, the financial transactions of banks, even the internal mechanics of cars, thermostats, burglary alarms, toasters—hacking into a network gave a spy or cyber warrior the power to control those centrifuges, dams, and transactions: to switch their settings, slow them down, speed them up, or disable, even destroy them.

This damage was wreaked remotely; the attackers might be half a world away from the target. And unlike the atomic bomb or the intercontinental ballistic missile, which had long ago erased the immunity of distance, a cyber weapon didn't require a large-scale industrial project or a campus of brilliant scientists; all it took to build one was a roomful of computers and a small corps of people trained to use them.

There was another shift: the World Wide Web, as it came to be called, was just that—a network stretched across the globe. Many classified programs ran on this same network; the difference was that their contents were encrypted, but this only meant that, with enough time and effort, they could be decrypted or otherwise penetrated, too. In the old days, if spies wanted to tap a phone, they put a device on a single circuit. In the cyber era, Internet traffic moved at lightning speed, in digital packets, often interspersed with packets containing other people's traffic, so a terrorist's emails or cell phone chatter couldn't be extracted so delicately; everyone's chatter and traffic got tossed in the dragnet, placed, potentially, under the ever-watchful eye.

The expectation arose that wars of the future were bound to be, at least in part, cyber wars; cyberspace was officially labeled a "domain" of warfare, like air, land, sea, and outer space. And because of the seamless worldwide network, the packets, and the Internet of Things, cyber war would involve not just soldiers, sailors, and pilots but, inexorably, the rest of us. When cyberspace is everywhere, cyber war can seep through every digital pore.

During the transitions between presidents, the ideas of cyber warfare were dismissed, ignored, or forgotten, but they never disappeared. All along, and even before Ronald Reagan watched WarGames, esoteric enclaves of the national-security bureaucracy toiled away on fixing—and, still more, exploiting—the flaws in computer software.

General Jack Vessey could answer Reagan's question so quickly—within a week of the meeting on June 8, 1983, where the president asked if someone could really hack the military's computers, like the kid in that movie—because he took the question to a man named Donald Latham. Latham was the assistant secretary of defense for command, control, communications, and intelligence—ASD(C3I), for short—and, as such, the Pentagon's liaison with the National Security Agency, which itself was an extremely secret part of the

Department of Defense. Spread out among a vast complex of shuttered buildings in Fort Meade, Maryland, surrounded by armed guards and high gates, the NSA was much larger, better funded, and more densely populated than the more famous Central Intelligence Agency in Langley, Virginia. Like many past (and future) officials in his position, Latham had once worked at the NSA, still had contacts there, and knew the ins and outs of signals intelligence and how to break into communications systems here and abroad.

There were also top secret communications-intelligence bureaus of the individual armed services: the Air Intelligence Agency (later called the Air Force Information Warfare Center) at Kelly Air Force Base in San Antonio, Texas; the 609th Information Warfare Squadron at Shaw Air Force Base in Sumter, South Carolina; scattered cryptology labs in the Navy; the CIA's Critical Defense Technologies Division; the Special Technological Operations Division of J-39, a little known office in the Pentagon's Joint Staff (entry required dialing the combination locks on two metal doors). They all fed to and from the same centers of beyond-top-secret wizardry, some of it homegrown, some manufactured by ESL, Inc. and other specialized private contractors. And they all interacted, in one way or another, with the NSA.

When Reagan asked Vessey if someone could really hack into the military's computers, it was far from the first time the question had been asked. To those who would write NSDD-145, the question was already very old, as old as the Internet itself.

In the late 1960s, long before Ronald Reagan watched WarGames, the Defense Department undertook a program called the ARPANET. Its direct sponsor, ARPA (which stood for Advanced Research Projects Agency), was in charge of developing futuristic weapons for the U.S. military. The idea behind ARPANET was to let the agency's contractors—scientists at labs and universities across the country—share data, papers, and discoveries on the same network. Since more and more researchers were using computers, the idea made sense. As things stood, the director of ARPA had to have as many computer consoles in his office as there were contractors out in the field, each hooked up to a separate telephone modem—one to communicate with UCLA, another with the Stanford Research Institute, another with the University of Utah, and so forth. A single network, linking them all, would not only be more economical, it would also let scientists around the country exchange data more freely and openly; it would be a boon to scientific research.

In April 1967, shortly before ARPANET's rollout, an engineer named Willis Ware wrote a paper called "Security and Privacy in Computer Systems" and delivered it at the semiannual Joint Computer Conference in New York City. Ware was a pioneer in the field of computers, dating back to the late 1940s, when there barely was such a field. At Princeton's Institute for Advanced Studies, he'd been a protégé of John von Neumann, helping design one of the first electrical computers. For years now, he headed the computer science department at the RAND Corporation, an Air Force-funded think tank in Santa Monica, California. He well understood the point of ARPANET, lauded its goals, admired its ambition; but he was worried about some implications that its managers had overlooked.

In his paper, Ware laid out the risks of what he called "resource-sharing" and "on-line" computer networks. As long as computers stood in isolated chambers, security wouldn't be a problem. But once multiple users could access data from unprotected locations, anyone with certain skills could hack into the network—and after hacking into one part of the network, he could roam at will.

Ware was particularly concerned about this problem because he knew that defense contractors had been asking the Pentagon for permission to store classified and unclassified files on a single computer. Again, on one level, the idea made sense: computers were expensive; commingling all the data would save lots of money. But in the impending age of ARPANET, this practice could prove disastrous. A spy who hacked into unclassified networks, which were entirely unprotected, could find "back doors" leading to the classified

sections. In other words, the very existence of a network created sensitive vulnerabilities; it would no longer be possible to keep secrets.

Stephen Lukasik, ARPA's deputy director and the supervisor of the ARPANET program, took the paper to Lawrence Roberts, the project's chief scientist. Two years earlier, Roberts had designed a communications link, over a 1200-baud phone line, between a computer at MIT's Lincoln Lab, where he was working at the time, and a colleague's computer in Santa Monica. It was the first time anyone had pulled off the feat: he was, in effect, the Alexander Graham Bell of the computer age. Yet Roberts hadn't thought about the security of this hookup. In fact, Ware's paper annoyed him. He begged Lukasik not to saddle his team with a security requirement: it would be like telling the Wright brothers that their first airplane at Kitty Hawk had to fly fifty miles while carrying twenty passengers. Let's do this step by step, Roberts said. It had been hard enough to get the system to work; the Russians wouldn't be able to build something like this for decades.

He was right; it would take the Russians (and the Chinese and others) decades—about three decades—to develop their versions of the ARPANET and the technology to hack into America's. Meanwhile, vast systems and networks would sprout up throughout the United States and much of the world, without any provisions for security.

Over the next forty years, Ware would serve as a consultant on government boards and commissions dealing with computer security and privacy. In 1980, Lawrence Lasker and Walter Parkes, former Yale classmates in their late twenties, were writing the screenplay for the film that would come to be called *WarGames*. They were uncertain about some of the plotline's plausibility. A hacker friend had told them about "demon-dialing" (also called "war-dialing"), in which a telephone modem searched for other nearby modems by automatically dialing each phone number in a local area code and letting it ring twice before moving on to the next number. If a modem answered, it would squawk; the demon-dialing software would record that number, and the hacker would call it back later. (This was the way that early computer geeks found one another: a pre-Internet form of web trolling.) In the screenplay, this was how their whiz-kid hero breaks into the NORAD computer. But Lasker and Parkes wondered whether this was possible: wouldn't a military computer be closed off to public phone lines?

Lasker lived in Santa Monica, a few blocks from RAND. Figuring that someone there might be helpful, he called the public affairs officer, who put him in touch with Ware, who invited the pair to his office.

They'd found the right man. Not only had Ware long known about the myriad vulnerabilities of computer networks, he'd helped design the software program at NORAD. And for someone so steeped in the world of big secrets, Ware was remarkably open, even friendly. He looked like Jiminy Cricket from the Disney cartoon film of *Pinocchio*, and he acted a bit like him, too: excitable, quick-witted, quick to laugh.

Listening to the pair's questions, Ware waved off their worries. Yes, he told them, the NORAD computer was supposed to be closed, but some officers wanted to work from home on the weekend, so they'd leave a port open. Anyone could get in, if the right number was dialed. Ware was letting the fledgling screenwriters in on a secret that few of his colleagues knew. The only computer that's completely secure, he told them with a mischievous smile, is a computer that no one can use.

Ware gave Lasker and Parkes the confidence to move forward with their project. They weren't interested in writing sheer fantasy; they wanted to imbue even the unlikeliest of plot twists with a grain of authenticity, and Ware gave them that. It was fitting that the scenario of *WarGames*, which aroused Ronald Reagan's curiosity and led to the first national policy on reducing the vulnerability of computers, was in good part the creation of the man who'd first warned that they were vulnerable.

Ware couldn't say so, but besides working for RAND, he also served on the Scientific Advisory Board of the National Security Agency. He knew the many ways in which the NSA's signals intelligence crews were piercing the shields—penetrating the radio and telephone communications—of the Russian and Chinese military establishments. Neither of those countries had computers at the time, but ARPANET was wired through dial-up modems—through phone lines. Ware knew that Russia or China could hack into America's phone lines, and thus into ARPANET, with the same bag of tricks that America was using to hack into their phone lines.

In other words, what the United States was doing to its enemies, its enemies could also do to the United States—maybe not right now, but someday soon.

The National Security Agency had its roots in the First World War. In August 1917, shortly after joining the fight, the United States government created Military Intelligence Branch 8, or MI-8, devoted to deciphering German telegraph signals. The unit stayed open even after the war, under the dual auspices of the war and state departments, inside an inconspicuous building in New York City that its denizens called the Black Chamber. The unit, whose cover name was the Code Compilation Company, monitored communications of suspected subversives; its biggest coup was persuading Western Union to provide access to all the telegrams coming over its wires. The Black Chamber was finally shut down in 1929, after Secretary of State Henry Stimson proclaimed, "Gentlemen don't read each other's mail." But the practice was revived, with the outbreak of World War II, as the Signal Security Agency, which, along with British counterparts, broke the codes of German and Japanese communications—a feat that helped the Allies win the war. Afterward, it morphed into the Army Security Agency, then the multiservice Armed Forces Security Agency, then in 1952—when President Harry Truman realized the services weren't cooperating with one another—a unified code-breaking organization called the National Security Agency.

Throughout the Cold War, the NSA set up bases around the world—huge antennas, dishes, and listening stations in the United Kingdom, Canada, Japan, Germany, Australia, and New Zealand—to intercept, translate, and analyze all manner of communications inside the Soviet Union. The CIA and the Air Force flew electronic-intelligence airplanes along, and sometimes across, the Soviet border, picking up signals as well. In still riskier operations, the Navy sent submarines, equipped with antennas and cables, into Soviet harbors.

In the early years of the Cold War, they were all listening mainly to radio signals, which bounced off the ionosphere all around the globe; a powerful antenna or large dish could pick up signals from just about anyplace. Then, in the 1970s, the Russians started switching to microwave transmissions, which beamed across much shorter distances; receivers had to be in the beam's line of sight to intercept it. So the NSA created joint programs, sending spies from the CIA or other agencies across enemy lines, mainly in the Warsaw Pact nations of Eastern Europe, to erect listening posts that looked like highway markers, telephone poles, or other mundane objects.

Inside Moscow, on the tenth floor of the American embassy, the NSA installed a vast array of electronic intelligence gear. In a city of few skyscrapers, the tenth floor offered a panoramic view. Microwave receivers scooped up phone conversations between top Soviet officials—including Chairman Leonid Brezhnev himself—as they rode around the city in their limousines.

The KGB suspected something peculiar was going on up there. On January 20, 1978, Bobby Ray Inman, the NSA director, was awakened by a phone call from Warren Christopher, the deputy secretary of state. A fire had erupted in the Moscow embassy, and the local fire chief was saying he wouldn't put it out unless he was given access to the tenth floor. Christopher asked Inman what he should do.

Inman replied, “Let it burn.” (The firefighters eventually put it out anyway. It was one of several fires that mysteriously broke out in the embassy during that era.)

By 1980, the last full year of Jimmy Carter’s presidency, the American spy agencies had penetrated the Soviet military machine so deeply, from so many angles, that analysts were able to piece together a near-complete picture of its operations, patterns, strengths, and weaknesses. And they realized that, despite its enormous buildup in troops and tanks and missiles, the Soviet military was extremely vulnerable.

The fatal gaps lay in the communications links of its command-control systems—the means by which radar operators tracked incoming planes and missiles, general officers sent out orders, and Kremlin higher-ups decided whether to go to war. And once American SIGINT crews were inside Soviet command-control, they could not only learn what the Russians were up to, which was valuable enough; they could also insert false information, disrupt the command signals, even shut them off. These disruptions might not win a war by themselves, but they could tip the balance, sowing confusion among Soviet officers, making them distrust the intelligence they were seeing and the orders they were receiving—which, in the best of scenarios, might stop them from launching a war in the first place.

The Russians, by now, had learned to encrypt their most vital command-control channels, but the NSA figured out how to break the codes, at least some of them. When cryptologists of whatever nationality coded a signal, they usually made a mistake here and there, leaving some passages in plain text. One way to break the code was to find the mistake, work backward to see how that passage—say, an often-used greeting or routine military jargon—had been encrypted in previous communiqués, then unravel the code from there.

Bobby Ray Inman had been director of naval intelligence before he took over the NSA in 1977, at the start of President Carter’s term. Even back then, he and his aides had fiddled with encryption puzzles. Now with the NSA’s vast secret budget at his disposal, Inman went at the task with full steam. In order to compare encrypted passages with mistakes in the clear, he needed machines that could store a lot of data and process it at high speed. For many years, the NSA had been building computers—vast corridors were filled with them—but this new task exceeded their capacity. So, early on in his term as director, Inman started a program called the Bauded Signals Upgrade, which involved the first “supercomputer.” The machine cost more than a billion dollars, and its usefulness was short-lived: once the Soviets caught on that their codes had been broken, they would devise new ones, and the NSA code breakers would have to start over. But for a brief period of Russian obliviousness, the BSU helped break enough high-level codes that, combined with knowledge gained from other penetrations, the United States acquired an edge—potentially a decisive edge—in the deadliest dimension of the Cold War competition.

Inman had a strong ally in the Pentagon’s top scientist, William Perry. For a quarter century, Perry had immersed himself in precisely this way of thinking. After his Army service at the end of World War II, Perry earned advanced degrees in mathematics and took a job at Sylvania Labs, one of the many high-tech defense contractors sprouting up in Northern California, the area that would later be called Silicon Valley. While many of these firms were designing radar and weapons systems, Sylvania specialized in electronic countermeasures—devices that jammed, diffracted, or disabled those systems. One of Perry’s earliest projects involved intercepting the radio signals guiding a Soviet nuclear warhead as it plunged toward its target, then altering its trajectory, so the warhead swerved off course. Perry figured out a way to do this, but he told his bosses it wouldn’t be of much use, since Soviet nuclear warheads were so powerful—several megatons of blast, to say nothing of thermal heat and radioactive fallout—that millions of Americans would die anyway. (This experience led Perry, years later, to become an outspoken advocate of nuclear arms-reduction treaties.)

Still, Perry grasped a key point that most other weapons scientists of the day did not: that getting inside the enemy's communications could drastically alter the effect of a weapon—and maybe the outcome of a battle or a war.

Perry rose through the ranks of Sylvania, taking over as director in 1954, then ten years later he left to form his own company, Electromagnetic Systems Laboratory, or ESL, which did contract work almost exclusively for the NSA and CIA. By the time he joined the Pentagon in 1977, he was as familiar as anyone with the spy agencies' advances in signals intelligence; his company, after all, had built the hardware that made most of those advances possible.

It was Perry who placed these scattershot advances under a single rubric: "counter-C2 warfare," the "C2" standing for "command and control." The phrase derived from his longtime preoccupation with electronic countermeasures, for instance jamming an enemy jet's radar receiver. But while jammers gave jets a tactical edge, counter-C2 warfare was a strategic concept; its goal was to degrade an enemy commander's ability to wage war. The concept regarded communications links—and the technology to intercept, disrupt, or sever them—not merely as a conveyor belt of warfare but as a decisive weapon in its own right.

When Jimmy Carter was briefed on these strategic breakthroughs, he seemed fascinated by the technology. When his successor, the Cold War hawk Ronald Reagan, heard the same briefing a year later, he evinced little interest in the technical details, but was riveted to the big picture: it meant that if war broke out between the superpowers, as many believed likely, the United States could win, maybe quickly and decisively.

In his second term as president, especially after the reformer Mikhail Gorbachev took over the Kremlin, Reagan rethought the implications of American superiority: he realized that his military's aggressive tactics and his own brazen rhetoric were making the Russians jumpy and the world more dangerous; so he softened his rhetoric, reached out to Gorbachev, and the two wound up signing a string of historic arms-reduction treaties that nearly brought the Soviet Union—the "evil empire," as Reagan had once described it—into the international order. But during his first term, Reagan pushed hard on his advantage, encouraging the NSA and other agencies to keep up the counter-C2 campaign.

Amid this pressure, the Russians didn't sit passive. When they found out about the microwaves emanating from the U.S. embassy's tenth floor, they started beaming its windows with their own microwave generators, hoping to listen in on the American spies' conversations.

The Russians grew clever at the spy-counterspy game. At one point, officials learned that the KGB was somehow stealing secrets from the Moscow embassy. The NSA sent over an analyst named Charles Gandy to solve the mystery. Gandy had a knack for finding trapdoors and vulnerabilities in any piece of hardware. He soon found a device called the Gunman inside sixteen IBM Selectric typewriters, which were used by the secretaries of high-level embassy officials. The Gunman recorded every one of their keystrokes and transmitted the data to a receiver in a church across the street. (Subsequent probes revealed that an attractive Russian spy had lured an embassy guard to let her in.)

It soon became clear that the Russians were setting up microwave beams and listening stations all over Washington, D.C., and New York City. Senior Pentagon officials—those whose windows faced high buildings across the Potomac River—took to playing Muzak in their offices while at work, so that if a Russian spy was shooting microwaves at those windows, it would clutter the ambient sound, drowning out their conversations.

Bobby Ray Inman had his aides assess the damage of this new form of spying. President Carter, a technically

sophisticated engineer (he loved to examine the blueprints of the military's latest spy satellites), had been assured that his phone conversations, as well as those of the secretaries of state and defense, were carried on secure landlines. But NSA technicians traced those lines and discovered that, once the signal reached Maryland, it was shunted to microwave transmitters, which were vulnerable to interception. There was no evidence the Soviets were listening in, but there was no reason to think they weren't; they certainly could be, with little difficulty.

It took a while, but as more of these vulnerabilities were discovered, and as more evidence emerged that Soviet spies were exploiting them, a disturbing thought smacked a few analysts inside NSA: Anything we're doing to them, they can do to us.

This anxiety deepened as a growing number of corporations, public utilities, and government contractors started storing data and running operations on automated computers—especially since some of them were commingling classified and unclassified data on the same machines, even the same software. Willis Ware's warnings of a dozen years earlier were proving alarmingly prophetic.

Not everyone in the NSA was troubled. There was widespread complacency about the Soviet Union: doubt, even derision at the idea, that a country so technologically backward could do the remarkable things that America's SIGINT crews were doing. More than that, to the extent computer hardware and software had security holes, the NSA's managers were reluctant to patch them. Much of this hardware and software was used (or copied) in countries worldwide, including the targets of NSA surveillance; if it could easily be hacked, so much the better for surveillance.

The NSA had two main directorates: Signals Intelligence and Information Security (later called Information Assurance). SIGINT was the active, glamorous side of the puzzle palace: engineers, cryptologists, and old-school spies, scooping up radio transmissions, tapping into circuits and cables, all aimed at intercepting and analyzing communications that affected national security. Information Security, or INFOSEC, tested the reliability and security of the hardware and software that the SIGINT teams used. But for much of the agency's history, the two sides had no direct contact. They weren't even housed in the same building. Most of the NSA, including the SIGINT Directorate, worked in the massive complex at Fort Meade, Maryland. INFOSEC was a twenty-minute drive away, in a drab brown brick building called FANEX, an annex to Friendship Airport, which later became known as BWI Marshall Airport. (Until 1968, INFOSEC had been still more remote, in a tucked-away building—which, many years later, became the Department of Homeland Security headquarters—on Nebraska Avenue, in Northwest Washington.) INFOSEC technicians had a maintenance function; they weren't integrated into operations at all. And the SIGINT teams did nothing but operations; they didn't share their talents or insights to help repair the flaws in the equipment they were monitoring.

These two entities began to join forces, just a little, toward the end of Carter's presidency. Pentagon officials, increasingly aware that the Soviets were penetrating their communications links, wanted INFOSEC to start testing hardware and software used not only by the NSA but by the Defense Department broadly. Inman set up a new organization, called the Computer Security Center, and asked his science and technology chief, George Cotter, to direct it. Cotter was one of the nation's top cryptologists; he'd been doing signals intelligence since the end of World War II and had worked for the NSA from its inception. Inman wanted the new center to start bringing together the SIGINT operators and the INFOSEC technicians on joint projects. The cultures would remain distinct for years to come, but the walls began to give.

The order to create the Computer Security Center came from the ASD(C3I), the assistant secretary of defense for command, control, communications, and intelligence—the Pentagon's liaison with the NSA.

When Reagan became president, his defense secretary, Caspar Weinberger, appointed Donald Latham to the position. Latham had worked SIGINT projects with George Cotter in the early to mid-1970s on the front lines of the Cold War: Latham as chief scientist of U.S. European Command, Cotter as deputy chief of NSA-Europe. They knew, as intimately as anyone, just how deeply both sides—the Soviets and the Americans (and some of their European allies, too)—were getting inside each other’s communications channels. After leaving NSA, Latham was named deputy chief of the Pentagon’s Office of Microwave, Space and Mobile Systems—and, from there, went on to work in senior engineering posts at Martin Marietta and RCA, where he remained immersed in these issues.

When General Jack Vessey came back from that White House meeting after Ronald Reagan had watched WarGames and asked his aides to find out whether someone could hack into the military’s most sensitive computers, it was only natural that his staff would forward the question to Don Latham. It didn’t take long for Latham to send back a response, the same response that Vessey would deliver to the president: Yes, the problem is much worse than you think.

Latham was put in charge of working up, and eventually drafting, the presidential directive called NSDD-145. He knew the various ways that the NSA—and, among all federal agencies, only the NSA—could not only hack but also secure telecommunications and computers. So in his draft, he put the NSA in charge of all their security.

The directive called for the creation of a National Telecommunications and Information Systems Security Committee “to consider technical matters” and “develop operating policies” for implementing the new policy. The committee’s chairman would be the ASD(C3I)—that is to say, the chairman would be Don Latham.

The directive also stated that residing within this committee would be a “permanent secretariat composed of personnel of the National Security Agency,” which “shall provide facilities and support as required.” There would also be a “National Manager for Telecommunications and Automated Information Systems Security,” who would “review and approve all standards, techniques, systems, and equipments.” The directive specified that this National Manager would be the NSA director.

It was an ambitious agenda, too ambitious for some. Congressman Jack Brooks, a Texas Democrat and Capitol Hill’s leading civil-liberties advocate, wasn’t about to let the NSA—which was limited, by charter, to surveillance of foreigners—play any role in the daily lives of Americans. He wrote, and his fellow lawmakers passed, a bill that revised the president’s directive and denied the agency any such power. Had Don Latham’s language been left standing, the security standards and compliance of every computer in America—government, business, and personal—would have been placed under the tireless gaze of the NSA.

It wouldn’t be the last time that the agency tried to assert this power—or that someone else pushed back.

Users Review

From reader reviews:

Michelle Bachman:

The book Dark Territory: The Secret History of Cyber War give you a sense of feeling enjoy for your spare time. You may use to make your capable far more increase. Book can to be your best friend when you getting tension or having big problem with your subject. If you can make reading through a book Dark Territory: The Secret History of Cyber War to be your habit, you can get considerably more advantages, like

add your own capable, increase your knowledge about a few or all subjects. You may know everything if you like start and read a e-book Dark Territory: The Secret History of Cyber War. Kinds of book are several. It means that, science guide or encyclopedia or others. So , how do you think about this reserve?

Jerry Lyon:

What do you ponder on book? It is just for students since they're still students or this for all people in the world, the particular best subject for that? Just you can be answered for that concern above. Every person has various personality and hobby for each and every other. Don't to be pressured someone or something that they don't desire do that. You must know how great in addition to important the book Dark Territory: The Secret History of Cyber War. All type of book are you able to see on many resources. You can look for the internet methods or other social media.

Trina Durham:

The feeling that you get from Dark Territory: The Secret History of Cyber War is the more deep you looking the information that hide inside words the more you get considering reading it. It doesn't mean that this book is hard to comprehend but Dark Territory: The Secret History of Cyber War giving you thrill feeling of reading. The article writer conveys their point in a number of way that can be understood by simply anyone who read the item because the author of this book is well-known enough. This book also makes your personal vocabulary increase well. Therefore it is easy to understand then can go together with you, both in printed or e-book style are available. We recommend you for having this Dark Territory: The Secret History of Cyber War instantly.

Dwight Hancock:

Your reading 6th sense will not betray an individual, why because this Dark Territory: The Secret History of Cyber War reserve written by well-known writer whose to say well how to make book that could be understand by anyone who else read the book. Written in good manner for you, still dripping wet every ideas and producing skill only for eliminate your personal hunger then you still doubt Dark Territory: The Secret History of Cyber War as good book but not only by the cover but also from the content. This is one publication that can break don't judge book by its deal with, so do you still needing an additional sixth sense to pick that!? Oh come on your reading sixth sense already alerted you so why you have to listening to one more sixth sense.

Download and Read Online Dark Territory: The Secret History of Cyber War By Fred Kaplan #KPCA12RI7HE

Read Dark Territory: The Secret History of Cyber War By Fred Kaplan for online ebook

Dark Territory: The Secret History of Cyber War By Fred Kaplan Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Dark Territory: The Secret History of Cyber War By Fred Kaplan books to read online.

Online Dark Territory: The Secret History of Cyber War By Fred Kaplan ebook PDF download

Dark Territory: The Secret History of Cyber War By Fred Kaplan Doc

Dark Territory: The Secret History of Cyber War By Fred Kaplan Mobipocket

Dark Territory: The Secret History of Cyber War By Fred Kaplan EPub

KPCA12RI7HE: Dark Territory: The Secret History of Cyber War By Fred Kaplan