

DARK TERRITORY

THE
SECRET HISTORY
OF
CYBER WAR

FRED KAPLAN

AUTHOR OF *THE INSURGENTS*

Thank you for downloading this Simon & Schuster eBook.

Join our mailing list and get updates on new releases, deals, bonus content and other great books from Simon & Schuster.

[CLICK HERE TO SIGN UP](#)

or visit us online to sign up at
eBookNews.SimonandSchuster.com

**THE SECRET
HISTORY OF
CYBER WAR**

DARK TERRITORY

FRED KAPLAN

SIMON & SCHUSTER

NEW YORK LONDON TORONTO SYDNEY NEW DELHI

CONTENTS

CHAPTER 1 “Could Something Like This Really Happen?”

CHAPTER 2 “It’s All About the Information”

CHAPTER 3 A Cyber Pearl Harbor

CHAPTER 4 Eligible Receiver

CHAPTER 5 Solar Sunrise, Moonlight Maze

CHAPTER 6 The Coordinator Meets Mudge

CHAPTER 7 Deny, Exploit, Corrupt, Destroy

CHAPTER 8 Tailored Access

CHAPTER 9 Cyber Wars

CHAPTER 10 Buckshot Yankee

CHAPTER 11 “The Whole Haystack”

CHAPTER 12 “Somebody Has Crossed the Rubicon”

CHAPTER 13 Shady RATs

CHAPTER 14 “The Five Guys Report”

CHAPTER 15 “We’re Wandering in Dark Territory”

Acknowledgments

About the Author

Notes

Index

“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 picked up 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 the 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 a little 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-14—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 war 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, electrical 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. Unlike 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, burglar 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, disable, even destroy them.

This damage was wreaked remotely; the attackers might be half a world away from the target. 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 and 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 at 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 mo-

economical, it would also let scientists around the country exchange data more freely and openly; 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 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

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 NORA 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 was 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 signal 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, 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 jamming 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 a 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 microwave beams emanating from the U.S. embassy's tenth floor, they started beaming their own 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

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, 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 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

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 System 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 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.

“IT’S ALL ABOUT THE INFORMATION”

ON August 2, 1990, Saddam Hussein, the president of Iraq, ordered his army to invade Kuwait, the small country to the south. Three days later, President George H. W. Bush declared that the aggression “will not stand.” On January 17, 1991, after a massive mobilization, U.S. helicopters and combat planes fired the first shots of a month-long air campaign over Iraq—followed, on February 24, by a hundred-hour ground assault, involving more than a half million American troops enveloping and crushing the Iraqi army, pushing its scattered survivors back across the border.

Known as Operation Desert Storm, it was the largest armored offensive the world had seen since the Second World War. It was also—though few were aware of this—the first campaign of “counter command-control warfare,” the harbinger of cyber wars to come.

The director of the NSA at the time was Rear Admiral William Studeman, who, like his mentor Bobby Ray Inman, had been director of naval intelligence before taking the helm at Fort Meade. When Studeman was appointed to run the NSA, he took with him, as his executive assistant, a veteran Navy cryptologist named Richard Wilhelm, who, a few years earlier, had been the number two at the agency’s large SIGINT site in Edsall, Scotland, running the test bed for Inman’s Bauded Signal Upgrade program, which aimed to decrypt Soviet communications.

As the planning for Desert Storm got under way, Studeman sent Wilhelm to the Pentagon as the NSA delegate to a hastily improvised group called the Joint Intelligence Center. The head of the center was Rear Admiral John “Mike” McConnell, who held the post of J-2, the intelligence officer for the chairman of the Joint Chiefs of Staff. Like most fast-rising officers in naval intelligence, Wilhelm and McConnell had known each other for years. In the new center, they created a multiservice apparatus that combined SIGINT, satellite imagery, and human spies on the ground into a single cell of intelligence-gathering and -analysis.

Before the invasion, American intelligence officers knew little about Iraq or Saddam Hussein’s military machine. By the time the bombing began, they knew most of what there was to know. Months before the first shot was fired, McConnell’s analysts penetrated deep inside Saddam’s command-and-control network. A key discovery was that Saddam had run fiber-optic cable all the way from Baghdad down to Basra and, after his invasion, into Kuwait City. American intel officers contacted the Western firms that had installed the cable and learned from them the locations of the switching systems. When the bombing began in the wee hours of January 17, those switches were among the first targets hit. Saddam had to reroute communications to his backup network, built on microwave signals. Anticipating this move, the NSA had positioned a new top secret satellite directly over Iraq, one of three spy-in-the-sky systems that Wilhelm had managed before the war. This one sported a receiver that scooped up microwave signals.

At every step, then, the NSA, McConnell’s Joint Intelligence Center, and, through them, the American combat commanders knew exactly what Saddam and his generals were saying and where their soldiers were moving. As a result, the United States gained a huge edge in the fight: not only could its commanders swiftly counter the Iraqi army’s moves, they could also move their own forces around without fear of detection. The Iraqis had lots of anti-aircraft missiles, which they’d acquired over the years from the Soviets, and they were well trained to use them. They might have shot down more American combat planes, but McConnell’s center figured out how to disrupt Iraq’s command-and-control

systems and its air-defense radar.

Saddam's intelligence officers soon detected the breach, so he started to send orders to the front via couriers on motorbikes; but this was a slow process, the war by then was moving fast, and there was little he could do to avoid a rout.

This first experiment in counter-C2 warfare was a success, but it didn't go very far, not nearly as far as its partisans could have taken it, because the U.S. Army's senior officers weren't interested. General Norman Schwarzkopf, the swaggering commander of Desert Storm, was especially dismissive. "Stormin' Norman" was old-school: wars were won by killing the enemy and destroying his targets, and, in this regard, all wars were the same: big or small, conventional or guerrilla, on the rolling hills of Europe, in the jungles of Vietnam, or across the deserts of Mesopotamia.

Initially, Schwarzkopf wanted nothing to do with the feeds from McConnell's center. He'd brought with him only a handful of intelligence officers, figuring they'd be sufficient for the job. The entire intelligence community—the directors of the CIA, NSA, Defense Intelligence Agency, and others—raised a fuss. It took the intervention of the chairman of the Joint Chiefs of Staff, Colin Powell, an Army general with Washington grooming and a strategic outlook, to bring the center's intel analysts into a conversation with the war planners.

Even so, Schwarzkopf put up resistance. When he learned that Saddam was transmitting his orders through microwaves after the fiber-optic cables were destroyed, his first instinct was to blow up the microwave link. Some of his own intel analysts argued against him, pointing to the reams of valuable information they were getting from the intercept. Schwarzkopf dismissed these objections, insisting that destroying Saddam's communication links, rather than exploiting them for intelligence, would be the speedier path to victory.

It wasn't just Schwarzkopf who waved away the Joint Intelligence Center's schemes; the Pentagon's top civilians were also leery. This was all very new. Few politicians or senior officials were versed in the technology; neither President Bush nor his secretary of defense, Dick Cheney, had ever used a computer. At a crucial point in the war, as the American ground forces made their end run to attack the Iraqi army from the flanks and the rear, the NSA and the Joint Intelligence Center proposed disabling an Iraqi telecommunications tower by hacking into its electronics: the tower needed to be put out of action for just twenty-four hours; there was no need to blow it up (and probably kill some innocent people besides). Cheney was skeptical. He asked the analysts how confident they were that the plan would work; they were unable to quantify the odds. By contrast, a few bombs dropped from fighter planes would do the job with certainty. Cheney went with the bombs.



Those who were immersed in the secret counter-C2 side of the war came away feeling triumphant, but some were also perplexed and disturbed. Richard H. L. Marshall was a legal counselor for the NSA. Before the fighting started, he'd voiced some concerns about the battle plan. At one point, an Iraqi generator, which powered a military facility, was supposed to be disabled by electronic means. But Marshall saw that it also powered a nearby hospital. There was a chance that this attack—though it didn't involve bullets, missiles, or bombs—would nonetheless kill a lot of civilians, and the more helpless civilians at that.

Marshall and other lawyers, in the NSA and the Pentagon, held a spirited discussion about the implications. Their concerns proved moot: Schwarzkopf and other commanders decided to drop bombs and missiles on the generator and almost every other urban target—power plants, water purification centers, communications towers, and various facilities having dual civil and military functions—and the "collateral damage" killed thousands of Iraqi civilians.

Still, from his vantage at NSA, Marshall could anticipate a growth spurt in this new sort of warfare—perhaps a time, in the not too distant future, when it matured to a dominant form of warfare. If a nation destroyed or disabled a piece of critical infrastructure, without launching a missile or dropping a bomb, would that constitute an act of war? Would its commanders and combatants be subject to the Law of Armed Conflict? Nobody knew; nobody with the authority to mull such matters had given

any thought.

Other NSA officers, more highly ranked and operationally oriented, had a different, more strategic concern. They were astonished by how easy it had been to take out Saddam's communications links. But some knew that, in a future war, especially against a foe more advanced than Iraq, it might not be so easy. The technology was changing: from analog to digital, from radio transmissions and microwaves to fiber optics, from discrete circuits of phone lines to data packets of what would come to be called cyberspace. Even Saddam Hussein had fiber-optic cable. Because European allies had installed it, American officials could learn where the switches were located and, therefore, where to drop the bombs. But one could imagine another hostile nation laying cable on its own. Or, if a war wasn't going on, if the NSA simply wanted to intercept signals whooshing through the cable, just as it had long been intercepting phone calls and radio transmissions, there would be no way to get inside. It might be technically possible to tap into the cable, but the NSA wasn't set up for the task.

The official most deeply worried about these trends was the NSA director, Bill Studeman.

In August 1988, a few days before Studeman took command at Fort Meade, Inman invited him and another old colleague, Richard Haver, to dinner. Seven years had passed since Inman had run the NSA, and he wasn't pleased with what his two successors—Lincoln Faurer and William Odom—had done with the place. Both were three-star generals, Faurer with the Air Force, Odom with the Army (the directorship usually rotated among the services), and to Inman, the career Navy man, that was part of the problem.

Of the military's three main services, the Navy was most attuned to shifts in surveillance technology. Its number-one mission was keeping track of the Soviet navy, especially Soviet submarines, and the U.S. Navy's most secretive branches conducted this hunt with many of the same tools and techniques that the NSA used. There was an esprit de corps among the coterie of Navy officers who rose through the ranks in these beyond-top-secret programs. In part, this was because they *were* highly classified; having the clearances to know the slightest details about them made them members of the military's most secret club. In part, it stemmed from the intensity of their mission: what they did 24/7, in peacetime—cracking Soviet codes, chasing Soviet submarines—was pretty much the same things they would do in wartime; the sense of urgency never let up.

Finally, this esprit had been the willed creation of Bobby Ray Inman. When he was director of naval intelligence in the mid-1970s, his top aides helped him identify the smartest people in the various branches of the Navy—attachés, officers on aircraft carriers, as well as black-ops submariners and cryptographers—and put them together in teams, to make sure that the most important intelligence got into the operators' hands and that the operators aligned their missions to the intel officers' needs.

Inman was a ruthless player of bureaucratic politics; Bill Studeman and Rich Haver liked to say that Machiavelli was an angel by comparison. As NSA director in the late 1970s and early 1980s, Inman was engaged in protracted power struggles over which agency, NSA or CIA, would win control of the new technologies. When Ronald Reagan was elected president, he asked Inman, whose term as NSA director had nearly expired, to move over to Langley and become deputy director of the CIA. The Senate confirmed his nomination to the new job on February 12, 1981, but he remained director of the NSA until March 30. In that five-week period of dual powers, Inman sent several memos to himself—NSA director to CIA deputy director, and vice versa—and thereby settled many of the scores between the two agencies. (Inman's boss at the CIA, the director, William Casey, was focused more on secret wars against communists in Central America and Afghanistan, so didn't concern himself with internal matters.) In the end, the NSA was given sole control of computerbased intelligence. (This set the stage, three years later, for Reagan's NSDD-145, which, until Congress overrode it, gave the NSA the power to establish security standards for all telecommunications and computers; Inman's self-addressed memos had established the precedents for this authority.) In a few other disputes, Inman split the responsibilities, creating joint CIA-NSA teams. With the roles and missions secure, Inman also boosted both agencies' budgets for expensive hardware that he'd desired back at Fort Meade—including supercomputers and miniaturized chips that enhanced the collection powers of sensors on satellites, spy planes, and submarines.

Inman stayed at the CIA for less than two years, then retired from government, moved back to his native Texas, and made a fortune in start-up software and commercial-encryption companies. From that vantage, he saw how quickly the digital revolution was spreading worldwide—and how radical the NSA would have to change to keep pace. He remained active on government advisory boards, occasionally checked in with former underlings at Fort Meade, and grew frustrated that Linc Faure and then Bill Odom, weren't paying attention to the sharp turns ahead.

Now, in the final year of Reagan's presidency, Bill Studeman—not only a Navy man with experience in classified projects, but also a fellow Texan and one of Inman's top protégés—was about to become the director of NSA. Rich Haver, who joined the two for dinner that summer night, was then deputy director of naval intelligence.

When Inman had been director of naval intelligence, Studeman and Haver had worked on his staff. Studeman had worked on the advances in surveillance and computer processing, including the Baudot Signals Upgrade, that gave America a leg up on Russia at the beginning of Reagan's presidency. Haver, a persuasive figure with a slide show and a pointer, was the one who briefed the president and his top aides on the advances' implications. The three of them—Inman, Studeman, and Haver—had degrees in history, not physics or engineering. The world was changing; the Cold War was entering a new phase; and they saw themselves as frontline players in a realm of the struggle that almost no one else knew existed.

Inman called together his two former underlings that night to tell them—really, to lecture them through the entirety of a three-hour dinner—that they had to push the intelligence community, especially the NSA, out in front of the technological changes. They had to alter the way the agency did business, promoted their personnel, and focused their energies.

Among the first things that Studeman did when he assumed the helm at Fort Meade a few days later, was to commission two papers. One, called the "Global Access Study," projected how quickly the world would shift from analog to digital. It concluded that the change wouldn't take place all at once, but uniformly; that the NSA would have to innovate in order to meet the demands (and intercept the communications) of the new world, while still monitoring the present landscape of telephone, radio, and microwave signals.

Studeman's second paper, an analysis of NSA personnel and their skill sets, concluded that the balance was wrong: there were too many Kremlinologists, not enough computer scientists. When Inman was director, he'd taken a few small steps to bring the technicians into the same room as the SIGINT operators and analysts, but the effort had since stalled. Most of the agency's computer experts worked in IT or maintenance. No one in SIGINT was tapping their expertise for advice on vulnerabilities in new hardware and software. In short, no one was preparing for the new era.

Studeman's studies—the very fact that he commissioned them—sparked resistance, anger, and fear from the rank and file. Over the years, the NSA's managers had invested, and were still spending colossal sums on analog technology, and they chose to ignore or dismiss warnings that they'd made a bad bet. The old guard took Studeman's second study—the one on the looming mismatch between the agency's skill sets and its mission—as a particularly ominous threat: if the new director acted on his study's conclusions, thousands of veteran analysts and spies would soon be out of a job.

There was only so much Studeman could do during his three years in charge. For one thing, the world was changing more quickly than anyone could have imagined. By the time Studeman left Fort Meade in April 1992, the Cold War—the struggle that had animated the NSA since its birth—was over and won. Even if the need for NSA reform had been widely accepted (and it wasn't), it suddenly seemed less urgent.



Studeman's successor was Rear Admiral Mike McConnell, who had run the Joint Intelligence Center during Operation Desert Storm. McConnell had remained General Powell's intelligence officer in the year and a half since the war. In the mid-1980s, he'd spent a year-long tour at NSA headquarters attached to the unit tracking Soviet naval forces. But returning to Fort Meade as NSA director, at

moment of such stark transition, McConnell didn't quite know what he and this enormous agency were supposed to do.

There were two distinct branches of the agency's SIGINT Directorate: the "A Group," which monitored the Soviet Union and its satellites; and the "B Group," which monitored the rest of the world. As its title suggested, the A Group was the elite branch, and everyone in the building knew it. Its denizens imbibed a rarefied air: *they* were the ones protecting the nation from the rival superpower. They had learned the imponderably specialized skills, and had immersed themselves so deeply into the Soviet mindset, that they could take a stream of seemingly random data and extract patterns and shifts of patterns that, pieced together, gave them (at least in theory) a picture of the Kremlin's intentions and the outlook for war and peace. Now that the Cold War was over, what good were those skills? Should the Kremlin-watchers still be called the A Group?

A still larger uncertainty was how the NSA, as a whole, would continue to do its watching—and listening. Weeks into his tenure as director, McConnell learned that some of the radio receivers and antennas, which the NSA had set up around the globe, were no longer picking up signals. Studeman's "Global Access Study"—which predicted the rate at which the world would switch to digital—was coming true.

Around the same time, one of McConnell's aides came into his office with two maps. The first was a standard map of the world, with arrows marking the routes that the major shipping powers navigated across the oceans—the "sea lines of communication," or SLOCs, as a Navy man like McConnell would have called them. The second map showed the lines and densities of fiber-optic cable around the world.

This is the map that you should study, the aide said, pointing to the second one. Fiber-optic lines were the new SLOCs, but they were to SLOCs what wormholes were to the galaxies: they whooshed you from one point to any other point instantaneously.

McConnell got the parallel, and the hint of transformation, but he didn't quite grasp its implications for his agency's future.

Shortly after that briefing, he saw a new movie called *Sneakers*. It was a slick production, a comedy-thriller with an all-star cast. The only reason McConnell bothered to see the film was that someone had told him it was about the NSA. The plot was dopey: a small company that does white-hat hacking and high-tech sleuthing is hired to steal a black box sitting on a foreign scientist's desk; the clients say that they're with the NSA and that the scientist is a spy; as it turns out, the clients are spies, the scientist is an agency contractor, the black box is a top secret device that can decode all encrypted data, and the NSA wants it back; the sleuths are on the case.

Toward the end of the film, there was a scene where the evil genius (played by Ben Kingsley), a former computer-hacking prankster who turns out to have ordered the theft of the black box, confronts the head sleuth (played by Robert Redford), an old friend and erstwhile comrade from the mischievous college days, and uncorks a dark soliloquy, explaining why he stole the box:

"The world isn't run by weapons anymore, or energy, or money," the Kingsley character says at a frenzied clip. "It's run by ones and zeroes, little bits of data. It's all just electrons. . . . There's a war out there, old friend, a world war. And it's not about who's got the most bullets. It's about who controls the information: what we see and hear, how we work, what we think. It's all about the information."

McConnell sat up as he watched this scene. Here, in the unlikely form of a Hollywood movie, was the NSA mission statement that he'd been seeking: *The world is run by ones and zeroes . . . There's a war out there . . . It's about who controls the information.*

Back at Fort Meade, McConnell spread the word about *Sneakers*, encouraged every employee he ran into to go see it. He even obtained a copy of the final reel and screened it for the agency's top officials, telling them that this was the vision of the future that they should keep foremost in their minds.

He didn't know it at the time, but the screenplay for *Sneakers* was cowritten by Larry Lasker and Walter Parkes—the same pair that, a decade earlier, had written *WarGames*. And, though not quite to the same degree, *Sneakers*, too, would have an impact on national policy.

Soon after his film-inspired epiphany, McConnell called Rich Wilhelm, who'd been the NS

representative—in effect, his right-hand man—on the Joint Intelligence Center during Desert Storm. After the war, Wilhelm and Rich Haver had written a report, summarizing the center's activities and listing the lessons learned for future SIGINT operations. As a reward, Wilhelm was swiftly promoted to take command of the NSA listening station at Misawa Air Base in Japan, one of the agency's largest foreign sites. In the order of NSA field officers, Wilhelm was king of the hill.

But now, McConnell was asking Wilhelm to come back to Fort Meade and take on a new job that he was creating just for him. Its title would be Director of Information Warfare. (*There's a war out there . . . It's about who controls the information.*)

The concept, and the nomenclature, spread. The following March, General Colin Powell, chairman of the Joint Chiefs of Staff, issued a policy memorandum on “information warfare,” which he defined as operations to “decapitate the enemy's command structure from its body of combat forces.” The military services responded almost at once, establishing the Air Force Information Warfare Center, the Naval Information Warfare Activity, and the Army Land Information Warfare Activity. (These entities already existed, but under different names.)

By the time McConnell watched *Sneakers*, he'd been fully briefed on the Navy and NSA programs in counter-C2 warfare, and he was intrigued with the possibilities of applying the concept to the new era. In its modern incarnation (“information warfare” was basically counter-C2 warfare plus digital technology), he could turn SIGINT on its ear, not just intercepting a signal but penetrating its source—and, once inside the mother ship, the enemy's command-control system, he could feed it false information, altering, disrupting, or destroying the machine, disorienting the commanders: *controlling the information to keep the peace and win the war.*

None of this came as news to Wilhelm; he'd been skirmishing on the information war's front lines for years. But six weeks into the new job, he came to McConnell's office and said, “Mike, we're kind of fucked here.”

Wilhelm had been delving into the details of what information *war*—a *two-way* war, in which both sides use the same weapons—might look like, and the sight wasn't pretty. The revolution in digital signals and microelectronics was permeating the American military and American society. In the name of efficiency, generals and CEOs alike were hooking up *everything* to computer networks. The United States was growing more dependent on these networks than any country on earth. About 90 percent of government files, including intelligence files, were flowing alongside commercial traffic. Banks, power grids, pipelines, the 911 emergency call system—all of these enterprises were controlled through networks, and all of them were vulnerable, most of them to very simple hacking.

When you think about attacking someone else's networks, Wilhelm told McConnell, keep in mind that *they* can do the same things to *us*. Information warfare wasn't just about gaining an advantage in combat; it also had to be about protecting the nation from other countries' efforts to gain the same advantage.

It was a rediscovery of Willis Ware's warning from a quarter century earlier.

McConnell instantly grasped the importance of Wilhelm's message. The Computer Security Center, which Bobby Ray Inman created a decade earlier, had since lured little in the way of funding or attention. The Information Security (now called Information Assurance) Directorate was still—literally—a sideshow, located a twenty-minute drive from headquarters.

Meanwhile, the legacy of Reagan's presidential directive on computer security, NSDD-145, lay in tatters. Congressman Jack Brooks's overhaul of the directive, laid out in the Computer Security Act of 1987, gave NSA control over the security of *military* computers and *classified* networks, but directed the National Bureau of Standards, under the Department of Commerce, to handle the rest. The formula was doomed from the start: the NBS lacked technical competence, while the NSA lacked institutional desire. When someone at the agency's Information Assurance Directorate or Computer Security Center discovered a flaw in a software program that another country might also be using, the real powers at NSA—the analysts in the SIGINT Directorate—wanted to exploit it, not fix it; they saw it as a new way to penetrate a foreign nation's network and to intercept its communications.

In other words, it wasn't so much that the problem went ignored; rather, no one in power saw it as

problem.

McConnell set out to change that. He elevated the Information Assurance Directorate, gave it more money at a time when the overall budget—not just for the NSA but for the entire Defense Department—was getting slashed, and started moving personnel back and forth, between the SIGINT and Information Assurance directorates, just for short-term tasks, but the idea was to expose the two cultures to one another.

It was a start, but not much more than that. McConnell had a lot on his plate: the budget cuts, the accelerating shift from analog circuits to digital packets, the drastic decline in radio signals, and the resulting need to find new ways to intercept communications. (Not long after McConnell became director, he found himself having to shut down one of the NSA antennas in Asia; it was picking up radio signals; *all* the traffic that it had once monitored, in massive volume at its peak, had moved to underground cables or cyberspace.)

In the fall of 1994, McConnell saw a demonstration, in his office, of the Netscape Matrix—one of the first commercial computer network browsers. He thought, “This is going to change the world. *Everyone* was going to have access to the Net—not just allied and rival governments, but individuals, including terrorists. (The first World Trade Center bombing had taken place the year before; terrorism, once seen as a nuisance during the nuclear arms race and the Cold War, was emerging as a major threat.) With the rise of the Internet came commercial encryption, to keep network communications at least somewhat secure. Code-making was no longer the exclusive province of the NSA and its counterparts; everyone was doing it, including private firms in Silicon Valley and along Route 128 near Boston, which were approaching the agency’s technical prowess. McConnell feared that the NSA would lose its unique luster—its ability to tap into communications affecting national security.

He was also coming to realize that the agency was ill equipped to seize the coming changes. A young man named Christopher Mellon, on the Senate Intelligence Committee’s staff, kept coming around asking questions. Mellon had heard the briefings on Fort Meade’s adaptations to the new digital world, but when he came to headquarters and examined the books, he discovered that, of the agency’s \$3 billion budget, just \$2 million was earmarked for programs to penetrate communications on the Internet. Mellon asked to see the personnel assigned to this program; he was taken to a remote corner of the main floor, where a couple dozen techies—out of a workforce numbered in the tens of thousands—were fiddling with computers.

McConnell hadn’t known just how skimpy these efforts were, and he assured the Senate committee that he would beef up the programs as a top priority. But he was diverted by what he saw as a more urgent problem—the rise of commercial *voice* encryption, which would soon make it very difficult for the NSA (and the FBI) to tap phone conversations. McConnell’s staff devised what they saw as a solution to the problem—the Clipper Chip, an encryption key that they billed as perfectly secure. The idea was to install the chip in every telecommunications device. The government could tap in and listen to a phone conversation, only if it followed an elaborate, two-key procedure. An agent would have to go to the National Institute of Standards and Technology, as the National Bureau of Standards was now called, to get one of the crypto-keys, stored on a floppy disk; another agent would go to the Treasury Department to get the other key; then the two agents would go to the Marine base at Quantico, Virginia, to insert both disks into a computer, which would unlock the encryption.

McConnell pushed hard for the Clipper Chip—he made it his top priority—but it was doomed from the start. First, it was expensive: a phone with a Clipper Chip installed would cost more than a thousand dollars. Second, the two-key procedure was baroque. (Dorothy Denning, one of the country’s top cryptologists, took part in a simulated exercise. She obtained the key from Treasury, but after driving out to Quantico, learned that the person from NIST had picked up the wrong key. They couldn’t unlock the encryption.) Finally, there was the biggest obstacle: very few people trusted the Clipper Chip, because very few people trusted the intelligence agencies. The revelations of CIA and NSA domestic surveillance, unleashed by Senator Frank Church’s committee in the mid-1970s, were still a fresh memory. Nearly everyone—even those who weren’t inclined to distrust spy agencies—suspected that the NSA had programmed the Clipper Chip with a *secret* back door that its agents could

open, then listen to phone conversations, without going through Treasury, NIST, or any legal process

~~The Clipper Chip ended with a whimper. It was McConnell's well-intentioned, but misguided~~
effort to forge a compromise between personal privacy and national security—and to do so openly,
the public eye. The next time the NSA created or discovered back doors into data, it would do so, as
had always done, under the cloak of secrecy.

A CYBER PEARL HARBOR

ON April 19, 1995, a small gang of militant anarchists, led by Timothy McVeigh, blew up a federal office building in Oklahoma City, killing 168 people, injuring 600 more, and destroying or damaging 325 buildings across a sixteen-block radius, causing more than \$600 million in damage. The shocking thing that emerged from the subsequent investigation was just how easily McVeigh and his associates had pulled off the bombing. It took little more than a truck and a few dozen bags of ammonium nitrate, a common chemical in fertilizers, obtainable in many supply stores. Security around the building was practically nonexistent.

The obvious question, in and out of the government, was what sorts of targets would get blown up next: a dam, a major port, the Federal Reserve, a nuclear power plant? The damage from any of those hits would be more than simply tragic; it could reverberate through the entire economy. So how vulnerable were they, and what could be done to protect them?

On June 21, Bill Clinton signed a Presidential Decision Directive, PDD-39, titled “U.S. Policy on Counterterrorism,” which, among other things, put Attorney General Janet Reno in charge of a “cabinet committee” to review—and suggest ways to reduce—the vulnerability of “government facilities” and “critical national infrastructure.”

Reno turned the task over to her deputy, Jamie Gorelick, who set up a Critical Infrastructure Working Group, consisting of other deputies from the Pentagon, CIA, FBI, and the White House. After a few weeks of meetings, the group recommended that the president appoint a commission, which in turn held hearings and wrote a report, which culminated in the drafting of another presidential directive.

Several White House aides, who figured the commission would come up with new ways to secure important physical structures, were startled when more than half of its report and recommendations dealt with the vulnerability of computer networks and the urgent need for what it called “cyber security.”

The surprise twist came about because key members of the Critical Infrastructure Working Group and the subsequent presidential commission had come from the NSA or the Navy’s super-secret black programs and were thus well aware of this new aspect of the world.

Rich Wilhelm, the NSA director of information warfare, was among the most influential members of the working group. A few months before the Oklahoma City bombing, President Clinton had put Vice President Al Gore in charge of overseeing the Clipper Chip; Mike McConnell sent Wilhelm to the White House as the NSA liaison on the project. The chip soon died, but Gore held on to Wilhelm and made him his intelligence adviser, with a spot on the National Security Council staff. Early on his new job, Wilhelm told some of his fellow staffers about the discoveries he’d made at Fort Mead, especially those highlighting the vulnerability of America’s increasingly networked society. He wrote a memo on the subject for Clinton’s national security adviser, Anthony Lake, who signed it with his own name and passed it on to the president.

When Jamie Gorelick put together her working group, it was natural that Wilhelm would be on it. One of its first tasks was to define its title, to figure out which infrastructures were *critical*—which sectors were vital to the functioning of a modern society. The group came up with a list of eight: telecommunications, electrical power, gas and oil, banking and finance, transportation, water supply,

- [download online Tara Duncan and the Spellbinders pdf, azw \(kindle\), epub](#)
- [read Empires Apart: A History of American and Russian Imperialism online](#)
- [read Spectrometric Identification of Organic Compounds \(7th Edition\)](#)
- [download online The Way of Shadows \(Night Angel, Book 1\)](#)
- [click Toys pdf, azw \(kindle\), epub](#)
- [God on the Rocks online](#)

- <http://www.experienceolvera.co.uk/library/Toute-Allure--Falling-in-Love-in-Rural-France.pdf>
- <http://transtrade.cz/?ebooks/Empires-Apart--A-History-of-American-and-Russian-Imperialism.pdf>
- <http://weddingcellist.com/lib/The-Architecture-of-Happiness.pdf>
- <http://www.netc-bd.com/ebooks/Linear-Quadratic-Controls-in-Risk-Averse-Decision-Making--Performance-Measure-Statistics-and-Control-Decision-Op>
- <http://musor.ruspb.info/?library/Toys.pdf>
- <http://growingsomeroots.com/ebooks/Nothing-To-Lose.pdf>