tions in this kind of combat employ their most sophisticated tools against each other. Thus, we really do not know who would win, nor what the results of such a cyber war would be. This book will lay out why the unpredictability associated with full-scale cyber war means that there is a credible possibility that such conflict may have the potential to change the world military balance and thereby fundamentally alter political and economic relations. And it will suggest ways to reduce that unpredictability.

Chapter Two

Cyber Warriors

In a television ad, a crew-cut young man in a jumpsuit walks around a darkened command center, chatting with subordinates who are illuminated by the greenish light from their computer screens. We hear his voice over the video: "control of power systems... water systems... that is the new battlefield... in the future this is going to be the premier war-fighting domain... this is going to be where the major battles are fought." He then looks right at the camera and says, "I am Captain Scott Hinck, and I am an Air Force Cyber Warrior." The screen fades to black, and then three words appear: "Air, Space, Cyberspace." Then, as the ad ends, we see a winged symbol and the name of the sponsor, "United States Air Force."

So now we know what one cyber warrior looks like. At least in
war meant and thought of it as "info ops," part of psychological warfare, or "psyops" (using propaganda to influence the outcome of wars). Others, particularly those in the intelligence branches, were seeing the ever-expanding Internet as a bonanza for electronic espionage. It started to become pretty obvious that once you had penetrated a network to collect information, a few more keystrokes could take that network down. As this realization grew among the electronic intelligence officers, they had a dilemma. The intelligence guys knew that if they told the "operators" (the fighting units) that the Internet was making a new kind of war possible, they would lose some control of cyberspace to the "warriors." On the other hand, the warriors would still have to rely on the intelligence geeks to do anything in cyberspace. Moreover, the opportunities cyberspace offered to relatively easily do significant damage to an enemy were too good to pass up. Slowly, the warriors realized that the geeks were on to something.

By the time George W. Bush was starting his second term, the importance of cyber war to the Pentagon became apparent, as the Air Force, Navy, and intelligence agencies engaged in a bitter struggle to see who would control this new area of warfare. Some advocated the creation of a Unified Command, bringing the units of all three services under one integrated structure. There were already Unified Commands for transportation, strategic nuclear war, and for each of the world's regions. When it appeared in the early 1980s that there would be a large role for the military in outer space, the Pentagon created a Unified Command for what it then thought of as a new domain for war-fighting, a domain that the United States had to control. U.S. Space Command lasted from 1985 to 2002, by which time it had become clear that neither the U.S. nor any other government had the money to do much in space. Space Command was folded into Strategic Command (STRATCOM), which operates the strategic nuclear forces. STRATCOM, headquartered at a
bomber base in Nebraska, was also given the centralized responsibility for cyber war in 2002. The Air Force, however, was set on running the actual war-fighting units. The creation of Air Force Cyber Command and the standing given to cyberspace in the Air Force recruitment ads jarred the other services and many in the Pentagon.

Some were concerned that the Air Force was talking too openly about something they believed should have been kept secret: the mere existence of cyber war capability. Yet there was the civilian Air Force Secretary (a vestigial post from the time before there was a strong civilian Defense Department) saying publicly, “Tell the nation the age of cyber war is here.” There were those damn ads, including one that said, ominously, that in the future a blackout “could be a cyber attack.” Another ad showed the Pentagon and claimed that it was “attacked” millions of times a day in cyberspace, but it was defended by the likes of an Air Force sergeant shown at his keyboard. There were persistent interviews and speeches by Air Force leaders who sounded very aggressive about their intentions. “Our mission is to control cyberspace, both for attacks and defense,” Lieutenant General Robert Elder had admitted. The Director of the Air Force Cyberspace Operations Task Force had been equally candid: “If you are defending in cyberspace, you’re already too late. If you do not dominate in cyberspace, you cannot dominate in other domains. If you are a developed country [and you are attacked in cyberspace], your life comes to a screeching halt.”

By 2008, those in the Pentagon not wearing blue uniforms had become persuaded about the importance of cyber war, but they were also convinced that it should not just be conducted by the Air Force. An integrated multiservice structure was agreed on in principle, but many were reluctant to “make the Space Command mistake again.” They did not want to create a Unified Command for what might prove to be a passing fad, as war fighting in space had been. The compromise was that a multiservice Cyber Command would be created, but it would remain subordinated to STRATCOM, at least on paper. The Air Force would have to stop calling its organization a command and would instead have to be satisfied with a “numbered air force,” their basic organizational unit, like Navy’s numbered fleets. The agreement in principle did not resolve all of the major issues standing in the way of a new command.

The intelligence community had a view. Under the post-9/11 reorganization, there was now a single person in charge of all eighteen U.S. intelligence agencies. In 2008, that man was Mike McConnell. He looked much the part of what he had recently been, a well-to-do businessman often seen in the halls of Wall Street financial institutions. He had come to the intelligence job from the global consulting giant Booz Allen Hamilton. Slightly hunched over and wearing thick glasses, the soft-spoken McConnell had not taken a traditional path to leadership at Booz. For most of his life, he had been in Navy intelligence, retiring as a three-star (or vice) admiral, the man in charge of the world’s premier electronic intelligence organization, the National Security Agency (NSA).

Hearing McConnell, or his successor, Air Force General Ken Minihan, talk about NSA even on an unclassified basis, you begin to understand why they believe re-creating some of its capabilities elsewhere is folly and perhaps impossible. They both speak with real reverence about the decades of experience and expertise NSA has in “doing the impossible” when it comes to electronic espionage. NSA’s involvement in the Internet grew out of its mission to listen to radio signals and telephone calls. The Internet was just another electronic medium. As Internet usage grew, so did intelligence agencies’ interest in it. Populated with Ph.D.s and electrical engineers, NSA quietly became the world’s leading center of cyberspace expertise.
Although not authorized to alter data or engage in disruption and damage, NSA thoroughly infiltrated the Internet infrastructure outside of the U.S. to spy on foreign entities.

When McConnell left NSA in 1996 for Booz Allen Hamilton, he continued his focus on the Internet, working with leading U.S. companies on their cyber security plans for over a decade. Returning to the spook business in 2007, he tried, as the second-ever Director of National Intelligence, to assert authority over all of the U.S. intelligence agencies, including CIA. In doing so, his long-standing friendship with CIA Director Mike Hayden was damaged. Hayden had also once been Director of NSA, or as they say it in the intelligence community DIRNSA (pronounced “dern-sah”). Hayden remained an active-duty four-star Air Force General much of the time he ran CIA.

Because both Mikes (McConnell and Hayden) had the background of running NSA, they agreed on at least one thing: any new Cyber Command must not try to replicate the capabilities it had taken decades to develop at NSA. If anything were to be done, they and many of the other NSA alumni believed, NSA should just become the new Cyber Command. Their views mattered in the Pentagon, since they were, or had been, senior military officers, and they actually knew something about cyberspace. To counter the “NSA takeover” of Cyber Command, some in the military argued that NSA was really a civilian organization, an intelligence unit, and therefore could not legally fight wars. They talked about “Title 50 versus Title 10” authority, referring to the parts of the U.S. Code that give legal authority and limitations to various government departments and agencies. Such laws can, of course, be changed if they have outlived their utility. Nonetheless, the issue of who would run America’s cyber wars soon became a battle between military and civilian government lawyers.

In any other alignment of leaders, the outcome would likely have been decided in the military’s favor and some new organization would have been built from the ground up, replicating the hacking skills at which NSA was the past master. In 2006, however, the turf-grabbing Secretary of Defense, Donald Rumsfeld, had been replaced after devastating midterm election losses brought on in part by mismanagement of the Iraq War. Rumsfeld’s replacement was the president of Texas A&M University, Robert Gates. At the time of his nomination I had known Bob for the better part of three decades and expected that he would be an unusually good Secretary of Defense. He was not a Pentagon man, had not grown up there. Nor was he a national security novice from industry or academia, the type easily manipulated by experienced Pentagon hands. Bob had been a career CIA officer who worked his way up to CIA Director, stopping off in the White House National Security Council along the way. Gates saw the Cyber Command debate from an intelligence community perspective and, more important, from the unique perch one has at the White House. When you are working directly for whoever the President may be at the time, you suddenly realize that there is a national interest that surpasses the turf concerns of whatever bureaucracy you may have come from. Gates had that broader view, and he was a pragmatist.

What resulted was a compromise in which the Director of NSA would become a four-star general (up from three stars) and would also be the head of U.S. Cyber Command. The Pentagon calls having two jobs being “dual hatted.” For now, at least, Cyber Command would be a “sub-Unified Command” under STRATCOM. The assets of NSA would be available to support U.S. Cyber Command, thus obviating the need for reinventing many wheels. The Air Force, Navy, and Army would continue to have cyber war units, but they would be run by U.S. Cyber Command. Technically, it would be those war-fighting military units that would actually engage in cyber combat and not the partially civilian intelligence agency that
is NSA. While NSA has a lot of expertise in network penetration, under U.S. law (Title 10) the agency is restricted to collecting information and prohibited from war-fighting. Therefore it will have to be military personnel under Title 50 that enter the keystrokes to take down enemy systems. To assist Cyber Command in its defensive role of protecting Defense Department networks, the Pentagon would also co-locate its own Internet service provider at Fort Meade, Maryland, alongside NSA. The Pentagon's ISP is unlike any other, since it runs two of the largest networks in the world. Called the Defense Information Systems Agency (DISA), it is run by a three-star general. Thus, ninety-two years after it opened as an Army base, home to hundreds of horses, Fort Meade became the heart of America's defensive and offensive cyber war forces. Defense contractors are building offices nearby in the hopes of sharing in some of the billions of dollars that will be flowing to Fort Meade. Maryland-area universities are already recipients of large research grants from the nearby military campus, referred to throughout Washington simply as "The Fort."

As a result of the decision to create U.S. Cyber Command, what had been Air Force Cyber Command became the 24th Air Force, with headquarters at Lackland Air Force Base in Texas. This numbered air force won't have any aircraft. The mission of the 24th will be to provide "combat-ready forces trained and equipped to conduct sustained cyber operations, fully integrated within air and space operations." The 24th Air Force will have control of two existing "wings," the 688th Information Operations Wing, formerly the Air Force Information Operations Center, and the 67th Network Warfare Wing, as well as control of a new wing, the 689th Combat Communications Wing. The 688th IOW, as the Information Operations Wing is known, will act as the Air Force's "center of excellence" in cyber operations. The 688th will be a forward-looking element with the mission of finding new ways to create an advantage for the U.S. Air Force using cyber weapons. The 67th Wing will have the day-to-day responsibility for defending Air Force networks and for attacking enemy networks. All totaled, the 24th Air Force will comprise some 6,000 to 8,000 military and civilian cyber warriors.

In case the U.S. Air Force is ever given the order to do as one of its ads suggests ("A power blackout is just a blackout. But in the future, it could be a cyber attack."), the mission will likely fall to the Fighting 67th. Their motto, from pre-cybr days as an aerial reconnaissance outfit, is Lux Ex Tenebris (Light from Darkness). Perhaps they will soon modify it to Tenebra Ex Luce. Despite the demotion of their command, the Air Force lost little of their zeal for cyber war. In the summer of 2009, the head of the U.S. Air Force, General Norton Schwartz, wrote to his officers that "cyberspace is vital to today's fight and to the future U.S. military advantage [and] it is the intent of the United States Air Force to provide a full spectrum of cyberspace capabilities. Cyberspace is a contested domain, and the fight is on—today."

Not to be outdone, the U.S. Navy also reorganized. The Chief of Naval Operations, Admiral Gary Roughead (real), gave himself a new Deputy for Information Dominance. It's not just Roughead and his sailors who are into dominance; the U.S. military in general repeatedly characterizes cyberspace as something to be dominated. It is reminiscent of the Pentagon's way of speaking of nuclear war in the 1960s. The historian of nuclear strategy Lawrence Freedman noted that William Kaufmann, Henry Kissinger, and other strategists realized that there was a need then "to calm the spirit of offense, potent in Air Force circles . . . [whose] rhetoric encouraged a view of war that was out-moded and dangerous." That same sort of macho rhetoric is strong in Air Force cyber war circles today, and apparently in the Navy as well.

Admiral Roughead created not just a Dominance office on the
Navy Staff, but a new "war-fighting" command. The 5th Fleet sails the Arab Gulf, the 6th Fleet the Mediterranean, and the 7th the China Sea. To fight cyber war, the U.S. Navy has reactivated its 10th Fleet. Originally, a small organization during World War II that coordinated antisubmarine warfare in the Atlantic, the 10th Fleet was disbanded shortly after victory over Germany in 1945. Then as now, the 10th Fleet was a "paper" or "phantom" fleet that had no ships. It was a land-based organization that filled a necessary coordinating role. Mustest in scope and scale, the 10th Fleet in World War II served its limited purpose well with no more than fifty intelligence officers. This time, the Navy has much more ambitious plans for the 10th Fleet. The existing Naval Network Warfare Command, known as NETWARCOM, will continue its operational responsibilities subordinated to the 10th Fleet. Although the Navy has not done the sort of public self-promotion of its cyber warriors that the Air Force has, they insist that they have as much tech savvy as "the fly boys." Perhaps to prove that point, one Naval officer told me, "You know, the 10th Fleet took a pretty bad licking from the Cardassians in 2374," thus proving that the current U.S. Navy at least has Trekkies, if perhaps not as many geeks as the Air Force.

For its part, the Army's cyber warriors are mostly contained in the Network Enterprise Technology Command, the 9th Signal Command at Fort Huachuca, Arizona. Members of this unit are assigned to the signal commands in each geographic region of the world. Network warfare units, what the Army calls NetWar units, under the Army's Intelligence and Security Command, are also forward-deployed to support combat operations alongside traditional intelligence units. They work closely with NSA to deliver intelligence to war fighters on the ground in Iraq and Afghanistan. The Army Global Network Operations and Security Center, known by the awkward acronym A-GNOSC, manages LandWarNet, which is what the Army calls its portion of the Department of Defense's networks. In July 2008, the Army stood up its first NetWar Battalion. If the Army sounds like the least organized of the services to fight cyber war, that is because it is. After the decision to create Cyber Command was made, the Secretary of Defense mandated the creation of an Army task force to review the Army's cyber mission and organization to support that mission.

While most people who followed the fight over cyber war in the Pentagon thought NSA won it, former NSA Director Ken Minihan was not satisfied, and that gave me pause. Ken is a friend whom I have known since, as an Air Force three-star general, he took over NSA in 1996. He believes that NSA and the U.S. military's approach to cyber operations needs to be rethought. The Navy, he thinks, is focused only on other navies. The Air Force is focused on air defense. The Army is hopelessly lost, and the NSA remains at heart an intelligence collection agency. "Not one of these entities is sufficiently focused on foreign counterintelligence in cyberspace, or on gaining hold of foreign critical infrastructure that the U.S. may want to take down without dropping a bomb in the next conflict." He believes that cyber war planning today lacks a "requirements process," a national-level planning system to get NSA and other organizations working on the same page. "Right now, they are all focused on doing what they want to do, not what a President may need them to be able to do."

Minihan and McConnell are both concerned that U.S. Cyber Command cannot defend the United States. "All the offensive cyber capability the U.S. can muster won't matter if no one is defending the nation from cyber attack," said McConnell. Cyber Command's mission is to defend DoD and maybe some other government agencies, but there are no plans or capabilities for it to defend the civilian infrastructure. Both former NSA Directors believe that mission should be handled by the Department of Homeland Security, as in the existing plans; but both men contend that Homeland has no
current ability to defend the corporate cyberspace that makes most of the country work. Neither does the Pentagon. As Minihan put it, "Though it is called the 'Defense' Department, if called on to defend the U.S. homeland from a cyber attack carried out by a foreign power, your half-trillion-dollar-a-year Defense Department would be useless."

THE SECRET ATTEMPT AT A STRATEGY

The perception that cyberspace is a "domain" where fighting takes place, a domain that the U.S. must "dominate," pervades American military thinking on the subject of cyber war. The secret-level National Military Strategy for Cyber Operations (partially declassified as a result of a Freedom of Information Act request) reveals the military's attitude toward cyber war, in part because it was written as a document that we, the citizens, were never supposed to see. It is how they talk about it behind the closed doors of the Pentagon. What is striking in the document is not only the acknowledgment that cyber war is real, but the almost reverential way in which it is discussed as the keystone holding up the edifice of modern war-fighting capability. Because there are so few opportunities to hear from the U.S. military on cyber war strategy, it is worth reading closely the secret-level attempt at a cyber war strategy.

The document, signed out under a cover letter from the Secretary of Defense, declares that the goal is "to ensure the US military [has] strategic superiority in cyberspace." Such superiority is needed to guarantee "freedom of action" for the American military and to "deny the same to our adversaries." To obtain superiority, the U.S. must attack, the strategy declares. "Offensive capabilities in cyberspace [are needed] to gain and maintain the initiative." At first read, the strategy sounds like a mission statement with a bit of zealotry thrown in. On closer examination, however, the strategy reflects an understanding of some of the key problems created by cyber war. Speaking to the geography of cyberspace, the strategy implicitly acknowledges the sovereignty issue ("the lack of geopolitical boundaries . . . allows cyberspace operations to occur nearly anywhere") as well as the presence of civilian targets ("cyberspace reaches across geopolitical boundaries . . . and is tightly integrated into the operations of critical infrastructure and the conduct of commerce"). It does not, however, suggest that such civilian targets should be off-limits from U.S. attacks. When it comes to defending U.S. civilian targets, the strategy passes the buck to the Department of Homeland Security.

The need to take the initiative, to go first, is dictated in part by the fact that actions taken in cyberspace move at a pace never before experienced in war ("cyberspace allows high rates of operational maneuver . . . at speeds that approach the speed of light. . . . [It] affords commanders opportunities to deliver effects at speeds that were previously incomprehensible"). Moreover, the strategy notes that if you do not act quickly, you may not be able to do so because "a previously vulnerable target may be replaced or provided with new defenses with no warning, rendering cyberspace operations less effective." In short, if you wait for the other side to attack you in cyberspace, you may find that the opponent has, simultaneously with their attack, removed your logic bombs or disconnected the targets from the network paths you expected to use to access them. The strategy does not discuss the problems associated with going first or the pressure to do so.

The importance of cyberspace and cyber war to the U.S. military is revealed in the strategy's declaration that "DOD will conduct kinetic missions to preserve freedom of action and strategic
advantage in cyberspace." Translated from Pentagonese, that statement means that rather than cyber attacks being just some support mechanism of a shooting war, the Defense Department envisions the need to bomb things in the physical world to defend against cyber attack, or to drive an enemy into networks that American cyber warriors control.

The strategic concept of deterrence is discussed in the strategy only insofar as it envisions a desired end state where "adversaries are deterred from establishing or employing offensive capabilities against US interests in cyberspace." Since twenty or thirty nations have already established offensive cyber units, we apparently did not deter them from "establishing." The way to stop those nations from using that capability against us, however, is discussed as "inducing adversary restraint based on demonstrated capabilities." However, the secrecy surrounding U.S. offensive cyber war weapons means that we have no demonstrated capabilities. By the logic of the U.S. military's strategy, we therefore cannot induce adversary restraint. The strategy does not suggest a way around this conundrum, let alone recognize it. Thus, what is called a military strategic for cyber operations raises some of the key issues that would need to be addressed in a strategy, but it does not provide answers. It is not really a strategy, but more of an appreciation. To the extent that it provides guidance, it seems to argue for initiating combat in cyberspace before the other side does, and for doing all that may be needed to dominate in cyberspace, because to do otherwise would put other kinds of American dominance at risk.

Buried in the document is, however, a realistic assessment of the problems facing the U.S. in cyber war: "threat actors can take advantage of [our] dependence" on cyberspace; and, "absent significant effort, the US will not continue to possess an advantage in cyberspace" and the U.S. will "risk parity with adversaries." Put another way, the strategy does note the fact that other nations may be able to inflict cyber war damage on us equal to our ability to inflict it on them. It may actually be worse, because we have a greater dependence on cyberspace, which can play to the advantage of an attacker.

If the U.S. is so vulnerable, to whom is it vulnerable? Who are the other cyber warriors?

WAKE-UP CALL FROM KUWAIT

It may have been the first Gulf War that convinced the generals of China's People's Liberation Army (PLA) that they needed a special advantage, an asymmetrical technical capability against the United States.

It was the first real war the U.S. had fought since Vietnam. In the decades before the 1990-91 Gulf War, the U.S. military had been relatively constrained abroad, by the continued presence of the Soviet Union and its nuclear arsenal. The invasions of Grenada by President Reagan and Panama by the first President Bush had been small engagements in our own backyard, and yet they had not gone terribly well. In those conflicts, U.S. military operations still showed the kind of dysfunction and poor coordination that marked the failed Desert One Mission in Iran in 1980 and helped to end the presidency of Jimmy Carter. Then came Desert Storm. President George H. W. Bush and his cabinet assembled the largest coalition since World War II. More than thirty nations coalesced against Saddam Hussein, bringing together more than 4,000 aircraft, 12,000 tanks, and nearly 2 million military personnel, all paid for by donations from Japan, Germany, Kuwait, and Saudi Arabia. The war was to mark a new era in international relations, what General Brent Scowcroft, President Bush's National Security Advisor, went so far as to call a "new world order." In it, the sovereignty of all nations would be respected and the mission of the United Nations would finally be
fulfilled, now that the Soviet Union was no longer in a position to check such actions. Desert Storm was also the dawn of a new kind of warfare, dominated by the computer and other high technology to manage logistics and provide near-realtime intelligence. The Armed Forces Communications and Electronics Association, an American industry group, publicly documented just how dramatically the use of computer networks changed that war in its 1992 book, *The First Information War*.

While General Norman Schwarzkopf and the other military brass may not have been ready to use cyber weapons to take down the Iraqi air defense network, they were ready to embrace computer networks to target the enemy. The war fighters also loved the new breed of “smart weapons” that information systems technology made possible. Designed to replace traditional bombs that required many missions and many tons of munitions dropped to destroy a target, “smart bombs” were designed to put one bomb, and one bomb only, precisely on each target every time. They would greatly reduce the number of missions that needed to be flown and promised to nearly eliminate civilian collateral-damage casualties.

Of course, these “smart weapons” of 1991 were not so smart, and there were not too many of them. In the 1996 movie *Wag the Dog*, a fictional political operative named Conrad “Connie” Brean, played by Robert De Niro, claims that the famous missile down a chimney was done in a studio in Hollywood. “What’s the thing people remember about the Gulf War?” Brean asks. “A bomb falling down a chimney. Let me tell you something: I was in the building where we filmed that with a ten-inch model made out of Legos.” What De Niro’s character claimed wasn’t true, but the smart bombs of 1991 were overhyped. While the video was real, the tightly controlled media did not seem to realize that most of the bombs dropped were not precision munitions guided by lasers and satellites but “dumb” bombs, dropped in the thousands by B-52s. The smart bombs then were unreliable and in short supply, but they showed the direction that warfare was moving in, and they showed the Chinese that they were decades behind.

As Desert Storm unfolded, Americans sat glued to their TVs, watching those grainy videos of bombs being dropped down smokestacks. They cheered the renewed prowess of the once-again formidable American military. Saddam Hussein’s army was the fourth-largest in the world. His weapons, largely of Soviet make and design, the same as China’s arsenal, were mostly destroyed from the air before they could ever be used. The U.S. ground war lasted one hundred hours, following thirty-eight days of air strikes. Among those watching on television were the leaders of the Chinese military. The former Director of National Intelligence, Admiral Mike McConnell, believes that “the Chinese received a big shock when watching the action of Desert Storm.” Later they probably read *The First Information War* and other accounts and realized how far behind they really were. They soon began referring to the Gulf War as *zhengda bianjue*, “the great transformation.”

For a period of several years in the mid-1990s the Chinese talked very openly, for a Communist police state, about what they had learned from the Gulf War. They noted that their strategy had been to defeat the U.S. by overwhelming numbers if a war ever happened. Now they concluded that that strategy would not work. They began to downsize their military and invest in new technologies. One of those technologies was *wangluohua*, “networkization,” to deal with the “new battlefield of computers.” What they talked about publicly then sounds strikingly similar to what the U.S. Air Force generals were saying. Writing in his military’s daily paper, one Chinese expert explained that “the enemy country can receive a paralyzing blow through the Internet.” A senior colonel, perhaps thinking of the U.S. and China, wrote that “a superior force that loses information dominance will be beaten, while an inferior one that seizes
information dominance will be able to win.” Major General Wang Pufeng, head of strategy at the military academy, wrote openly of the goal of zhixinxiguan, “information dominance.” Major General Dai Qingmin of the General Staff stated that such dominance could only be achieved by preemptive cyber attack. These strategists created “Integrated Network Electronic Warfare,” something similar to the Netcentric Warfare fad that was sweeping the Pentagon.

By the end of the 1990s, China’s strategists had converged on the idea that cyber warfare could be used by China to make up for its qualitative military deficiencies when compared to the United States. Admiral McConnell believes that “the Chinese concluded from the Desert Storm experience that their counter-strategy had to be to challenge America’s control of the battle space by building capabilities to knock out our satellites and invade our cyber networks. In the name of the defense of China in this new world, the Chinese feel they have to remove that advantage of the U.S. in the event of a war.”

A recurring word in these Chinese statements was “asymmetry”; likewise, the phrase “asymmetric warfare.” Much of what we know about China’s asymmetric warfare doctrine is contained in a slim volume translated as Unrestricted Warfare. The book, written by two high-ranking Chinese army colonels, was first published in 1999. It provides a blueprint for how weaker countries can outmaneuver status quo powers using weapons and tactics that fall outside the traditional military spectrum. The publishers of the most widely available English translation view the book as “China’s master plan to destroy America,” a subtitle the Americans added to the front cover of the U.S. edition. And in case the reader misses the point, the cover shows the World Trade Center engulfed in flames. A quote on the back, from a right-wing lunatic, claims that the book “is evidence linking China to 9-11.” Despite the right-wing rhetoric surrounding the U.S. edition, the book is one of the best windows through which we can understand Chinese military thinking on cyber war.

The book advocates tactics that have become known as shushoujian, the “assassin’s mace,” meant to take advantage of weaknesses created by an adversary’s seemingly superior conventional capabilities. The goal of the strategy is “fighting the fight that fits one’s weapons” and “making the weapons fit the fight.” It proposes a strategy of ignoring the traditional rules of conflict, including, at its extreme, the prohibition on targeting civilians. It also advocates manipulating foreign media, flooding enemy countries with drugs, controlling the markets for natural resources, and joining international legal bodies in order to bend them to one’s will. For a book written a decade ago, it also places a heavy emphasis on cyber war.

This possible use of cyber war against a superior force does not mean that China is in fact intent on fighting the U.S., just that its military planners recognize that war with the U.S. is a contingency for which they must plan. The Chinese government has adopted the phrase “peacefully rising” to describe the country’s projected emergence as a (if not the) global superpower in the twenty-first century. Yet Admiral Mike McConnell believes that “the Chinese are exploiting our systems for information advantage, looking for the characteristics of a weapons system or academic research on plasma physics.” China’s rapid economic growth and dependence upon global resources, as well as its disputes with its neighbors (Taiwan, Vietnam), probably suggest to its military, however, that they have to be ready for possible conflict someday. And they are getting ready.

To the head of the U.S. military, Admiral Mike Mullen (Chairman of the Joint Chiefs of Staff), it all looks like it is aimed squarely at the United States. “[China is] developing capabilities that are very maritime focused, maritime and air focused, and in many ways, very much focused on us,” he said in a speech at the Navy League in May of 2009. “They seem very focused on the United States Navy
and our bases that are in that part of the world," he continued. The 2009 update of the annual report from the Office of the Secretary of Defense on the "Military Power of the People's Republic of China" supports these claims. The Chinese have developed long-range radar that can see past our air base on Guam. They have developed anti-ship missiles that close so fast that none of our defense systems could intercept them. China has purchased one Russian Kuznetsov-class aircraft carrier and is currently in the process of refurbishing it at Dalian shipyard. They will soon have the capability to start constructing new carriers and have put in place a training program so that pilots will be qualified for carrier operations. They have strung over 2,000 missiles along the coast facing Taiwan and are adding more at the rate of 100 per year. They are close to deploying a missile with a 5,000-mile range that could give them a sea-based nuclear strike capability.

It all sounds a bit scary, but look closer and you will see evidence that the modernization alone is insufficient to counter U.S. conventional force superiority. China's military budget is just a fraction of America's. Allegedly only $70 billion, it is less than one-eighth of the Pentagon's budget before adding in the costs of the wars in Afghanistan and Iraq. A U.S. carrier strike group is one of the most powerful conventional forces ever assembled. Consisting of up to a dozen ships, including guided-missile cruisers, destroyers, frigates, submarines, and supply ships, a carrier strike group can cover over 700 nautical miles in a single day, which allows it to go anywhere there is ocean within two weeks. The U.S. Navy boasts eleven carrier battle groups. To keep that force modern, the Navy is in the process of constructing three next-generation Ford-class carriers, with the first carrier set to be launched in 2015.

The Pentagon's annual assessment, Military Power of the People's Republic of China, for 2009 estimates that the former Russian aircraft carrier will not be operational before 2015. The consensus view in the U.S. intelligence community is that China is at least a decade away from being able to marshal a modern fighting force that is capable of convincingly defeating even a moderate-sized enemy like Vietnam. Not until 2015 will China be able to project significant power off of its shores, and only then in limited cases against an opponent less capable than the U.S. is now. Unless...

Unless... they can even things up by using cyber war against such things as U.S. carriers. The Chinese were always impressed by U.S. carriers, but their attention was heightened in 1996, when President Bill Clinton sent two U.S. carrier battle groups to protect Taiwan during one particularly nasty exchange of tough rhetoric between Beijing and Taipei. So the Chinese military followed its new strategy and developed a "virtual roadmap" for how to take down an aircraft carrier battle group in a paper titled "Tactical Data Links in Information Warfare." This unclassified paper, written by two Chinese Air Force officers, relies on open source material, most of which can be pulled off the web, to illustrate how the information systems that the U.S. military relies on can be jammed or disrupted using relatively low-tech means.

These are the kinds of tactics that Unrestricted Warfare's strategy articulates. The book recommends a program to steal a potential enemy's technology, find flaws in it to exploit, and develop one's own version as part of a program to create a modernized and smaller force. Not lost on Chinese military strategists, however, is the ability of cyber weapons to skip the battlefield altogether. China has prepared for the event of war to inflict damage on the enemy's home front, not with conventional weapons, but asymmetrically, through cyber attack. The two paths of improvement only make sense together.

Even with the significant modernization of equipment, China will not be the equal of the U.S. military for many decades. However, if China can use asymmetrical tactics like cyber war, it believes the new, modern Chinese forces would be sufficiently advanced to take
on U.S. forces that will have been crippled by Chinese cyber attack. Recently, Pentagon planners have had a scare put into them by an article in *Orbis* titled “How the United States Lost the Naval War of 2015.” In it, James Kraska paints a vivid picture of how in the near future China could take on the United States Navy and win.

**THE EAST IS GEEK**

From what we know of China’s cyber warfare capabilities and the espionage campaigns the Chinese have carried out, that two-pronged approach is exactly what the Chinese have undertaken. Since the late 1990s, China has systematically done all the things a nation would do if it contemplated having an offensive cyber war capability and also thought that it might itself be targeted by cyber war; it has

- created citizen hacker groups,
- engaged in extensive cyber espionage, including of U.S. computer software and hardware,
- taken several steps to defend its own cyberspace,
- established cyber war military units, and
- laced U.S. infrastructure with logic bombs.

While developing cyber strategy, China also made use of private hackers closely aligned with the state’s interests. The U.S.-China Economic and Security Review Commission estimates that there are up to 250 groups of hackers in China that are sophisticated enough to pose a threat to U.S. interests in cyberspace. We saw something of their early capabilities in 1999, when the United States led a NATO air campaign to stop the slaughter in Kosovo by Serbian forces. The U.S. had all but perfected its smart weapons and used them to eliminate the Serbians’ Soviet-era military apparatus without losing a single American life (one U.S. warplane went down due to mechanical failure). Unfortunately, smart weapons can’t make up for bad intelligence. Six bombs dropped from U.S. aircraft hit the precise coordinates provided to the mission planners by the CIA. The target was supposed to be the Yugoslav Federal Directorate for Supply and Procurement, a planning agency of the Serbian military. The coordinates, however, were about 900 feet off from the Directorate and exactly on top of the Chinese embassy.

The Chinese held protests outside U.S. embassies and consulates, issued condemnatory statements within the UN and other bodies, and demanded compensation for the victims and their families. After the embassy bombing, U.S. and NATO websites were targeted with denial of service attacks. Government agencies had their inboxes stuffed with spam messages protesting the bombing. Some NATO webpages were forced down, while others were defaced. The attacks did little damage to U.S. military or government operations. The effort amounted to little more than what we call “hacktivism” today, a fairly mild form of online protest. It was, however, a first use of cyberspace by China to protest. Chinese hacktivists did it again in 2001, when a U.S. “spy plane” allegedly entered Chinese airspace and was forced by Chinese fighter jets to land in China. However, while these Chinese citizen hackers were launching their primitive denial of service and spam attacks, China’s intelligence-industry partnership was also busy.

The Chinese government went after two underpinnings of the U.S. computer industry’s dominance of networking technology, Microsoft and Cisco. By threatening to ban Chinese government procurement from Microsoft, Beijing persuaded Bill Gates to provide China with a copy of its secret operating system code. Microsoft had refused to show that code to its largest U.S. commercial customers. Then China copied the Cisco network router found on almost all U.S. networks and at most Internet service providers.
Cisco had a manufacturing plant for the routers in China. Chinese companies then sold counterfeit Cisco routers at cut-rate discounts around the world. The buyers allegedly included the Pentagon and other federal government entities. Counterfeit routers started showing up on the market in 2004. Three years later, the FBI and the Justice Department indicted two brothers who owned a company called Syren Technology for selling the counterfeit routers to a customer list that included the Marine Corps, the Air Force, and multiple defense contractors. A fifty-page report authored by the FBI and circulated within the technology industry concluded that the routers could be used by foreign intelligence agencies to take down networks and “weaken cryptographic systems.” Meanwhile, another Chinese company, Huawei, was selling similar routers throughout Europe and Asia. The major difference was that, unlike the counterfeits, these routers did not say Cisco on the front. Their label said Huawei.

With intimate knowledge of the flaws in Microsoft and Cisco software and hardware, China’s hackers could stop most networks from operating. But wouldn’t the Chinese be vulnerable, too? They would be, if they used the same Microsoft and Cisco products we do. As part of the deal with Microsoft, the Chinese modified the version sold in their country to introduce a secure component using their own encryption. Hedging their bets, they also developed their own operating system, called Kylin, modeled on the stable open source system known as FreeBSD. Kylin was approved by the People’s Liberation Army for use on their systems. China allegedly also developed its own secure microprocessor for use on servers and Huawei routers. The Chinese government is trying to install “Green Dam Youth Escort” software on all of its computers, allegedly to screen for child pornography and other prohibited material. If they get it to work, and proliferate it on all their systems, Green Dam could also scan for malware installed by other states.

In addition to Green Dam, there is the system that U.S. wags call the Great Firewall of China. Not really a firewall, the government-run system screens traffic on ISPs for subversive material, such as the Universal Declaration of Human Rights. The system engages in something called “Domain Name System hijacking,” sending you to a Chinese government clone of a real site when you are in China and try to go, for example, to the webpage of a Christian evangelical organization. It also has the ability to disconnect all Chinese networks from the rest of the global Internet, something that would be handy to have if you thought the U.S. was about to launch a cyber war attack on you. James Mulvenon, one of the leading American experts on China’s cyber war capabilities, says that taken together, Green Dam, the Great Firewall, and other systems represent “a substantial investment by Chinese authorities in enhanced blocking, filtering, and monitoring of their own cyberspace.

By 2003, China had announced the creation of cyber warfare units. Housed at the naval base on Hainan Island are the Third Technical Department of the PLA and the Lingshui Signals Intelligence Facility. According to the Pentagon, these units are responsible for offense and defense in cyberspace, and have designed cyber weapons that have never been seen before and that no defenses have been designed to stop. In one publication, the Chinese listed ten examples of such weapons and techniques:

- planting information mines
- conducting information reconnaissance
- changing network data
- releasing information bombs
- dumping information garbage
- disseminating propaganda
- applying information deception
- releasing clone (sic) information
• organizing information defense
• establishing network spy stations

China did establish two "network spy stations," not far from the U.S., in Cuba. With the permission of the Castro government, the Chinese military created a facility to monitor U.S. Internet traffic and another to monitor DoD communications. At about the same time China announced the creation of its cyber warfare units, the U.S. experienced one of the worst episodes of cyber espionage to date. Known as Titan Rain, the U.S. code name given to the case, the incident involved the extraction of between 10 and 20 terabytes of data off the Pentagon's unclassified network. The hackers also targeted the defense contractor Lockheed Martin, other military sites, and, for reasons that remain hard to fathom, the World Bank. Vulnerabilities in Pentagon and other targeted networks were systematically identified and then exploited to extract information through servers in South Korea and Hong Kong. Investigators were able to trace the flow from these intermediate servers back to a final server in Guangdong, China. U.S. Air Force Major General William Lord directly and publicly attributed the attacks not to Chinese hacks- tivists, but to the Chinese government.

By 2007, the Chinese government seemed to be involved in a widespread series of penetrations of U.S. and European networks, successfully copying and exporting huge volumes of data. The Director of the British domestic intelligence service MI5, Jonathan Evans, wrote letters to 300 leading companies in the U.K., advising them that their networks had probably been penetrated by the Chinese government. Evans's counterpart in Germany, Hans Remberg, also accused the Beijing government, this time of hacking into the computer of Angela Merkel, the German Chancellor.

The computer espionage also went after a high-ranking American, hacking into the computer of Secretary of Defense Robert Gates. Later, Chinese operatives copied information off of U.S. Secretary of Commerce Carlos Gutierrez's laptop when he visited Beijing, then attempted to use that information to gain access to Commerce Department computers. Commenting on the Chinese, Gates's Deputy Undersecretary, Robert Lawless, admitted that they have "a very sophisticated capability to attack and degrade our computer systems... to shut down our critical systems. They see it as a major component of their asymmetrical warfare capability."

In 2009, Canadian researchers uncovered a highly sophisticated computer program they dubbed GhostNet. It had taken over an estimated 1,300 computers at several countries' embassies around the world. The program had the capability to remotely turn on a computer's camera and microphone without alerting the user and to export the images and sound silently back to servers in China. A top target of the program were offices related to nongovernmental organizations working on Tibetan issues. The operation ran for twenty-two months until discovered. The same year, U.S. intelligence leaked to the media that Chinese hackers had penetrated the U.S. power grid and left behind tools that could be used to bring the grid down.

The extent of Chinese government hacking against U.S., European, and Japanese industries and research facilities is without precedent in the history of espionage. Exabytes of data have been copied from universities, industrial labs, and government facilities. The secrets behind everything from pharmaceutical formulas to bioengineering designs, to nanotechnology, to weapons systems, to everyday industrial products have been taken by the People's Liberation Army and by private hacking groups and given to China, Inc.

In the latest incident to become public, Google revealed its discovery of a highly sophisticated campaign targeting both the company's intellectual property and the e-mail accounts of leaders in the Chinese dissident movement.
The hackers used advance “spear-phishing” techniques to dupe senior Google executives into visiting websites where malware would automatically be downloaded onto their computers to give the hackers root access. While most phishing scams cast a wide net and try to catch a few people who are gullible enough to fall for Nigerian scammer e-mails, spear-phishing specifically targets an individual, figures out who their acquaintances are on Facebook or LinkedIn, and then tailors a message to look like it is from someone they would trust. If you were a senior research scientist at Google, you might have received an e-mail containing a link to a website that looked like it was from a colleague. The message might have said, “Hey, Chuck, I think this story will interest you…” and then provided a link to a fairly innocuous site. When the target clicked on the link and visited the site, the hackers used a zero-day flaw in Internet Explorer, one that was not publicly known and had yet to be patched, to download the malware silently and in such a fashion that no antivirus software or other measures would detect it. The malware created a back door to the computer so the hackers could maintain their access and used the first compromised computer to work their way across the corporate network until they reached the servers containing the source code, the crown jewel of a software company.

When Google’s scientists figured out what was going on in mid-December, they traced back the hacking to a server in Taiwan, where they found copies of their proprietary information and those of at least twenty other companies, including Adobe, Dow Chemical, and the defense contractor Northrop Grumman. From there, they traced the attacks back to Mainland China, and then went to the FBI, making their public announcement of the hacking and plans to exit the Chinese market in mid-January.

Some will suggest that war with China is, in any event, unlikely. China’s dependence on U.S. markets for its manufactured goods and the trillions the country has invested in U.S. Treasury bills mean that China would have a lot to lose in a war. One Pentagon official who spoke on the condition of anonymity isn’t so sure. He points out that the economic meltdown in the U.S. has had a secondary effect in China that has put millions of Chinese factory workers out on the streets. The Chinese government has not shown the kind of concern that we expect in the West and is not apparently worried about any weakening of its grip on the Chinese people. The lesson the Pentagon official takes away is that China can take economic lumps and may well do so if the gains from warfare are perceived as high enough.

What might such gains be? The trite answer one often hears is that China may find itself forced to stop Taiwan from implementing a declaration of independence. When serious analysts weigh the prospects of open conflict with China, however, they see it playing out over the open waters of the South China Sea. The Spratly Islands are not exactly a tourist destination. They are not exactly islands. If all were piled up together, the reefs, sandbars, and rocks in the South China Sea would amount to less than two square miles of land. That two square miles of land is spread out over more than 150,000 square miles of ocean. It’s not the islands that China, Vietnam, Taiwan, Malaysia, the Philippines, and Brunei are feuding over, but what is under them and around them. The reefs have some of the largest remaining stocks of fish in the world, a resource not to be discounted among the growing and hungry nations that lay claim to the waters. The islands also skirt the critical trade route that links the Indian Ocean to the Pacific nations through which a large majority of the world’s oil flows out of the Middle East. Then there are the Spratlys’ oil and gas. Undeveloped fields estimated to hold more natural gas than are Kuwait, currently home to the
fourth-largest reserves in the world, could fuel the economies of any of the countries for decades to come. Oil fields in the islands are already well developed, often with platforms established by several nations drawing out of the same reservoir.

If China decides to flex its newly developed military muscle, it may very well be in an attempt to wrest these islands from its neighbors, a scenario explored as a tabletop exercise later in the book. If China does seize the islands, the U.S. could, though reluctantly, be drawn into a response. The U.S. has established security guarantees with both the Philippines and Taiwan. Chevron has helped Vietnam develop the offshore oil fields that that nation claims.

Alternatively, we might be deterred from intervening against China in the Pacific Rim if the costs of doing so would be significant damage or disruption at home. According to Defense Secretary Robert Gates, cyber attacks “could threaten the United States’ primary means to project its power and help its allies in the Pacific.” Is that enough to deter the U.S. from a confrontation with China? If the possibility of China crippling our force projection capability is not enough to deter us, maybe the realization of our domestic vulnerabilities to cyber attack would be. The alleged emplacement of logic bombs in our electric grid may have been done in such a way that we would notice. One former government official told us that he suspects the Chinese wanted us to know that if we intervened in a Chinese conflict with Taiwan, the U.S. power grid would likely collapse. “They want to deter the United States from getting involved militarily within their sphere of influence.”

The problem is, however, that deterrence only works if the other side is listening. U.S. leaders may not have heard, or fully understood, what Beijing was trying to say. The U.S. has done little or nothing to fix the vulnerabilities in its power grid or in other civilian networks.

I focused on China because its cyber war development has been, oddly, somewhat transparent. U.S. intelligence officials do not, however, rate China as the biggest threat to the U.S. in cyberspace. “The Russians are definitely better, almost as good as we are,” said one. There seems to be a consensus that China gets more attention because, intentionally or otherwise, it has often left a trail of bread crumbs that can be followed back to Tiananmen Square.

The Russian nongovernmental hackers, including large cyber criminal enterprises, are a real force in cyberspace, as was demonstrated in the attacks on Estonia and Georgia discussed in chapter 1. The hacktivists and criminals are generally thought to be sanctioned by what used to be called the Sixteenth Directorate, a part of the infamous Soviet intelligence apparatus known as the KGB. Later it was called FAPSI. Few American intelligence officers could ever remember what FAPSI stood for (it’s the Russian acronym for: Federal Commission for Government Communications and Information), they just knew it was “Moscow’s NSA.”

Like America’s NSA, FAPSI started out doing code making and breaking, radio intercept, bugging, and wiretapping. As soon as the Internet appeared, however, FAPSI was on to it, taking over the largest ISP in Russia, later requiring all Russian ISPs to install monitoring systems that only FAPSI could access. Of course, during the rise of the Internet, the Soviet Union ended, and so, theoretically, did the KGB and FAPSI. In fact, the organizations merely put up their headquarters with new names. After several changes, in 2003 FAPSI became the Service of Special Communications and Information. Not all of their placarded buildings are in Moscow. In the southern city of Voronezh, FAPSI, as many Russians still call it, runs what might be the largest (and certainly one of the best) hacker schools in
the world. By now, of course, they are probably calling themselves cyber warriors.

Other nations known to have skilled cyber war units are Israel and France. U.S. intelligence officials have suggested that there are twenty to thirty nihilaries with respectable cyber war capability, including those of Taiwan, Iran, Australia, South Korea, India, Pakistan, and several NATO states. "The vast majority of the industrialized countries in the world today have cyber-attack capabilities," said former Director of National Intelligence Admiral Mike McConnell.

WHEN CYBER WARRIORS ATTACK

You may by now believe that there are cyber warriors, but in addition to jamming Internet sites what can they do, really? Obviously, we have not had a full-scale cyber war yet, but we have a good idea what it would look like if we were on the receiving end. Imagine a day in the near future. You are the Assistant to the President for Homeland Security and you get a call from the White House Situation Room as you are packing up to leave the office for the day, at eight p.m. NSA has issued a "CRITIC" message, a rare alert that something important has just happened. The one-line message says only: "large scale movement of several different zero-day malware programs moving on Internet in the US, affecting critical infrastructure." The Situation Room's Senior Duty Officer suggests that you come down and help him figure out what is going on.

By the time you get to the Situation Room, the Director of the Defense Information Systems Agency is waiting on the secure phone for you. He has just briefed the Secretary of Defense, who suggested he call you. The unclassified Department of Defense network known as the NIPRNET is collapsing. Large-scale routers throughout the network are failing, and constantly rebooting. Network traffic is essentially halted. As he is telling you this, you can hear someone in the background trying to get his attention. When the general comes back on the line, he says softly and without emotion, "Now it's happening on the SIPRNET and JWICS, too." He means that DoD's classified networks are grinding to a halt.

Unaware of what is happening across the river at the Pentagon, the Undersecretary of Homeland Security has called the White House, urgently needing to speak to you. FEMA, the Federal Emergency Management Agency, has told him that two of its regional offices, in Philadelphia and in Denton, Texas, have reported large refinery fires and explosions in Philadelphia and Houston, as well as lethal clouds of chlorine gas being released from several chemical plants in New Jersey and Delaware. He adds that the U.S. Computer Emergency Response Team in Pittsburgh is being deluged with reports of systems failing, but he hasn't had time to get the details yet.

Before you can ask the Senior Duty Officer where the President is, another officer thrusts a phone at you. It's the Deputy Secretary of Transportation. "Are we under attack?" she asks. When you ask why, she ticks off what has happened. The Federal Aviation Administration's National Air Traffic Control Center in Herndon, Virginia, has experienced a total collapse of its systems. The alternate center in Leesburg is in a complete panic because it and several other regional centers cannot see what aircraft are aloft and are trying to manually identify and separate hundreds of aircraft. Brickyard, the Indianapolis Center, has already reported a midair collision of two 737s. "I thought it was just an FAA crisis, but then the train wrecks started happening..." she explains. The Federal Railroad Administration has been told of major freight derailments in Long Beach, Norfolk, Chicago, and Kansas City.

Looking at the status board for the location of the President, you see it says only "Washington-OTR." He is on an "off the record," or personal, activity outside the White House. Reading your mind,
the Senior Duty Officer explains that the President has taken
the First Lady to a hip new restaurant in Georgetown. "Then put me
trough to the head of his Secret Service detail," says a breathless
voice. It's the Secretary of the Treasury, who has run from his office
in the building next to the White House. "The Chairman of the Fed
just called. Their data centers and their backups have had some sort
of major disaster. They have lost all their data. Its affecting the data
centers at DTCC and SIAC—they're going down, too." He explains
that those initials represent important financial computer centers in
New York. "Nobody will know who owns what. The entire financial
system will dissolve by morning."

As he says that, your eyes are drawn to a television screen reporting
on a derailment on the Washington Metro in a tunnel under the
Potomac. Another screen shows a raging flame in the Virginia sub-
urbs where a major gas pipeline has exploded. Then the lights in the
Situation Room flicker. Then they go out. Battery-operated emer-
gency spotlights come on, casting the room in shadows and bright
light. The television flat screens and the computer monitors have
gone blank. The lights flicker again and come back on, as do some of
the screens. There is a distant, loud droning. "It's the backup
generator, sir," the Duty Officer says. His deputy again hands you a
secure phone and mouths the words you did not want to hear: "It's for
you. It's POTUS."

The President is in the Beast, his giant armored vehicle that re-
sembles a Cadillac on steroids, on his way back from the restaurant.
The Secret Service pulled him out of the restaurant when the black-
out hit, but they are having a hard time getting through the traffic.
Washington's streets are filled with car wrecks because the signal
lights are all out. POTUS wants to know if it's true what his Secret
Service agent told him, that the blackout is covering the entire easter-
n half of the country. "No, wait, what? Now they're saying that

the Vice President's detail says it's out where he is, too. Isn't he in
San Francisco today? What time is it there?"

You look at your watch. It's now 8:15 p.m. Within a quarter of
an hour, 157 major metropolitan areas have been thrown into knots
by a nationwide power blackout hitting during rush hour. Poison
gas clouds are wafting toward Wilmington and Houston. Refineries
are burning up oil supplies in several cities. Subways have crashed in
New York, Oakland, Washington, and Los Angeles. Freight trains
have derailed outside major junctions and marshaling yards on four
major railroads. Aircraft are literally falling out of the sky as a result
of midair collisions across the country. Pipelines carrying natural
gas to the Northeast have exploded, leaving millions in the cold.
The financial system has also frozen solid because of terabytes of
information at data centers being wiped out. Weather, navigation,
and communications satellites are spinning out of their orbits into
space. And the U.S. military is a series of isolated units, struggling
to communicate with each other.

Several thousand Americans have already died, multiples of that
number are injured and trying to get to hospitals. There is more
going on, but the people who should be reporting to you can't get
through. In the days ahead, cities will run out of food because of the
train-system failures and the jumbling of data at trucking and distri-
bution centers. Power will not come back up because nuclear plants
have gone into secure lockdown and many conventional plants have
had their generators permanently damaged. High-tension transmis-
sion lines on several key routes have caught fire and melted. Unable
to get cash from ATMs or bank branches, some Americans will begin
to loot stores. Police and emergency services will be overwhelmed.

In all the wars America has fought, no nation has ever done this
kind of damage to our cities. A sophisticated cyber war attack by
one of several nation-states could do that today, in fifteen minutes,
without a single terrorist or soldier ever appearing in this country. Why haven't they done it by now, if they can? For the same reason that the nine nations with nuclear weapons haven't used one of them since 1945, because they need to have the political circumstances that cause them to believe such an attack would be in their interest. But unlike with nuclear weapons, where an attacker may be deterred by the promise of retaliation or by the radioactive blowback on his own country, launching a cyber attack may run fewer risks. In cyber war, we may never even know what hit us. Indeed, it may give little solace to Americans shivering without power to know that the United States may be about to retaliate in kind.

"While you were on the line with the President, sir, Cyber Command called from Fort Meade. They think the attack came from Russia and they are ready to turn out the lights in Moscow, sir. Or maybe it was China, so they are ready to hit Beijing, if you want to do that, sir?"

Chapter Three

The Battlespace

Cyberspace. It sounds like another dimension, perhaps with green lighting and columns of numbers and symbols flashing in midair, as in the movie The Matrix. Cyberspace is actually much more mundane. It's the laptop you or your kid carries to school, the desktop computer at work. It's a drab windowless building downtown and a pipe under the street. It's everywhere, everywhere there's a computer, or a processor, or a cable connecting to one.

And now it's a war zone, where many of the decisive battles in the twenty-first century will play out. To understand why, we need to answer some prior questions, like: What is cyberspace? How does it work? How can militaries fight in it?