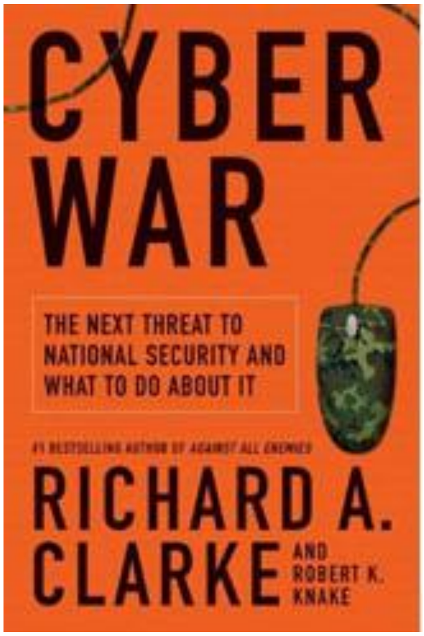
Cyber War—Excerpt

Chapter 1. Trail Runs


CYBER WAR
THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT
#1 BESTSELLING AUTHOR OF AGAINST ALL ENEMIES
RICHARD A. CLARKE
AND ROBERT K. KNAKE

A quarter-moon reflected on the slowly flowing Euphrates, a river along which nations have warred for five thousand years. It was just after midnight, September 6, 2007, and a new kind of attack was about to happen along the Euphrates, one that had begun in cyberspace. On the east side of the river, seventy-five miles south into Syria from the Turkish border, up a dry wadi from the riverbank, a few low lights cast shadows on the wadi's sandy walls. The shadows were from a large building under construction. Many North Korean workers had left the construction site six hours earlier, queuing in orderly lines to load onto buses for the drive to their nearby dormitory. For a construction site, the area was unusually dark and unprotected, almost as if the builder wanted to avoid attracting attention. Without warning, what seemed like small stars burst above the site, illuminating the area with a blue-white clarity brighter than daylight. In less than a minute, although it seemed longer to the few Syrians and Koreans still on the site, there was a blinding flash, then a concussive sound wave, and then falling pieces of debris. If their hearing had not been temporarily destroyed by the explosions, those on the ground nearby would then have heard a longer acoustic wash of military jet engines blanketing the area. Had they been able to look beyond the flames that were now sweeping the construction site, or above the illuminating flares that were still floating down on small parachutes, the Syrians and Koreans might have seen F-15 Eagles and F-16 Falcons banking north, back toward Turkey. Perhaps they would even have made out muted blue-and-white Star of David emblems on the wings of the Israeli Air Force strike formation as it headed home, unscathed, leaving years of secret work near the wadi totally destroyed.

Behind all of this mystery, however, was another intrigue. Syria had spent billions of dollars on air defense systems. That September night, Syrian military personnel were closely watching their radars. Unexpectedly, Israel had put its troops on the Golan Heights on full alert earlier in the day. From their emplacements on the occupied Syrian territory, Israel's Golani Brigade could literally look into downtown Damascus through their long-range lenses. Syrian forces were expecting trouble. Yet nothing unusual appeared on their screens. The skies over Syria seemed safe and largely empty as midnight rolled around. In fact, however, formations of Eagles and Falcons had penetrated Syrian airspace from Turkey. Those aircraft, designed and first built in the 1970s, were far from stealthy. Their steel and titanium airframes, their sharp edges and corners, the bombs and missiles hanging on their wings, should have lit up the Syrian radars like the Christmas tree illuminating New York's Rockefeller Plaza in December. But they didn't.

What the Syrians slowly, reluctantly, and painfully concluded the next morning was that Israel had "owned" Damascus's pricey air defense network the night before. What appeared on the radar screens was what the Israeli Air Force had put there, an image of nothing. The view seen by the Syrians bore no relation to the reality that their eastern skies had become an Israeli Air Force bombing range. Syrian air defense missiles could not have been fired because there had been no targets in the system for them to seek out. Syrian air defense fighters could not have scrambled, had they been fool enough to do so again

against the Israelis, because their Russian-built systems required them to be vectored toward the target aircraft by ground-based controllers. The Syrian ground-based controllers had seen no targets.
By that afternoon, the phones were ringing in the Russian Defense Ministry off Red Square. How could the Russian air defense system have been blinded? Syria wanted to know.

Cyber warriors around the world, however, were not surprised. This was how war would be fought in the information age, this was Cyber War. When the term “cyber war” is used in this book, it refers to actions by a nation-state to penetrate another nation’s computers or networks for the purposes of causing damage or disruption. When the Israelis attacked Syria, they used light and electric pulses, not to cut like a laser or stun like a taser, but to transmit 1’s and 0’s to control what the Syrian air defense radars saw. Instead of blowing up air defense radars and giving up the element of surprise before hitting the main targets, in the age of cyber war, the Israelis ensured that the enemy could not even raise its defenses.

The Israelis had planned and executed their cyber assault flawlessly. Just how they did it is a matter of some conjecture.

Chapter 2. 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 Scott's case, he looks a lot like the bright, fit, earnest officers who populate the world's most potent military. That is not quite our image of hackers, whom movies have portrayed as acned, disheveled guys with thick glasses. To attract more of those with the skills needed to understand how to fight cyber war, however, the Air Force seems to think it may have to bend the rules. "If they can't run three miles with a pack on their back, but they can shut down a SCADA system," mused Air Force Major General William Lord, "we need to have a culture where they can fit in." (A SCADA system is the software that controls networks such as electric power grids.) That progressive attitude reflects the U.S. Air Force's strong desire to play the leading role for the U.S. in cyber war. That service was the first to create an organization for the purpose of combat in the new domain: U.S. Air Force Cyber Command.

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 Home-land 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 strategy 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?

Chapter 3. 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?

Cyberspace is all of the computer networks in the world and everything they connect and control. It's not just the Internet. Let's be clear about the difference. The Internet is an open network of networks. From any network on the Internet, you should be able to communicate with any computer connected to any of the Internet's networks. Cyberspace includes the Internet plus lots of other networks of computers that are not supposed to be accessible from the Internet. Some of those private networks look just like the Internet, but they are, theoretically at least, separate. Other parts of cyberspace are transactional networks that do things like send data about money flows, stock market trades, and credit card transactions. Some networks are control systems that just allow machines to speak to other machines, like control panels talking to pumps, elevators, and generators.

What makes these networks a place where militaries can fight? In the broadest terms, cyber warriors can get into these networks and control or crash them. If they take over a network, cyber warriors could steal all of its information or send out instructions that move money, spill oil, vent gas, blow up generators, derail trains, crash airplanes, send a platoon into an ambush, or cause a missile to detonate in the wrong place. If cyber warriors crash networks, wipe out data, and turn computers into doorstops, then a financial system could collapse, a supply chain could halt, a satellite could spin out of orbit into space, an airline could be grounded. These are not hypotheticals. Things like this have already happened, sometimes experimentally, sometimes by mistake, and sometimes as a result of cyber crime or cyber war. As Admiral Mike McConnell has noted, "information managed by computer networks—which run our utilities, our transportation, our banking and communications—can be exploited or attacked in seconds from a remote location overseas. No flotilla of ships or intercontinental missiles or standing armies can defend against such remote attacks located not only well beyond our borders, but beyond physical space, in the digital ether of cyberspace."

Why, then, do we run sophisticated computer networks that allow unauthorized access or unauthorized commands? Aren't there security measures? The design of computer networks, the software and hardware that make them work, and the way in which they were architected, create thousands of ways that cyber warriors can get around security defenses. People write software and people make mistakes, or get sloppy, and that creates opportunities. Networks that aren't supposed to be connected to the public Internet very often actually are, sometimes without their owners even knowing. Let's look at some things in your daily life as a way of explaining how cyber war can happen. Do you think your condominium association knows that the elevator in your building is, like ET in the movie of the same name, "phoning home"? Your elevator is talking over the Internet to the people who made it. Did you know that the photocopier in your office is probably doing the same thing? Julia Roberts's character in the recent movie Duplicity knew that many copying machines are connected to the Internet and can be hacked, but most people don't know that their copier could even be online. Even fewer think about the latest trick, shredders that image. Just before all those sensitive documents pass through the knives that cut them into little pieces, they go by a camera that photographs them. Later, the cleaning crew guy will take his new collection of pictures away to whoever hired him.

Your elevator and copier “phoning home” is supposed to be happening, the software is working properly. But what if your competitor has a computer programmer who wrote a few lines of code and slipped them into the processor that runs your photocopier? Let’s say those few lines of computer code instruct the copier to store an image of everything it copies and put them into a compressed data (or zip) file. Then, once a day, the copier accesses the Internet and—ping!—it shoots that zip file across the country to your competitor. Even worse, on the day before your company has to submit a competitive bid for a big contract—ping!—the photocopier catches fire, causing the sprinklers to turn on, the office to get soaked, and your company to be unable to get its bid done in time. The competitor wins, you lose.

Chapter 4. The Defense Fails

Even though historians and national security officials know that there are numerous precedents for institutions thinking their communications are secure when they are not, there is still resistance to believing that it may be happening now, and to us. American military leaders today cannot conceive of the possibility that their Secret (SIPRNET) or Top Secret intranet (JWICS) is compromised, but several experts I spoke to are convinced that it is. Many corporate leaders also believe that the millions of dollars they have spent on computer security systems means they have successfully protected their company's secrets. After all, if anybody had gotten inside their secret files, the intrusion detection system software would have sounded an alarm. Right?

No, not necessarily. And even if the alarm did go off, in many cases that would not have caused anyone to do anything very quickly in response. There are ways of penetrating networks and assuming the role of the network administrator or other authorized user without ever doing anything that would cause an alarm. Moreover, if an alarm does go off, it is often such a routine occurrence on a large network that nothing will happen in response. Perhaps the next day someone will check the logs and notice that a couple of terabytes of information were downloaded and transmitted outside of the network to some compromised server, the first stop on a multistage trip intended to obscure the final destination. Or, perhaps, no one will notice that anything ever happened. The priceless art is still on the museum walls. And if that is the case, why should the government or the bottom-line-conscious executive do anything?

I mentioned in chapter 2 the 2003 phenomenon code-named Titan Rain. Alan Paller, a friend who runs the SANS Institute, a cyber security education and advocacy group, described what happened on one afternoon in that case, November 1, 2003.
At 10:23 p.m. the Titan Rain hackers exploited vulnerabilities at the U.S. Army Information Systems Engineering Command at Fort Huachuca, Arizona.
At 1:19 a.m. they exploited the same hole in computers at the Defense Information Systems Agency in Arlington, Virginia.
At 3:25 a.m. they hit the Naval Ocean Systems Center, a Defense Department installation in San Diego, California.
At 4:46 a.m. they struck the U.S. Army Space and Strategic Defense installation in Huntsville, Alabama.

There were lots of days like that. Not only were Defense facilities hit, but terabytes of sensitive information left NASA labs, as well as the computers of corporations such as Lockheed Martin and Northrop Grumman, which have been given contracts worth billions of dollars to manage security for DoD networks. Cyber security staffs tried to figure out the techniques being used to penetrate the networks. And their blocking efforts seemed to work. One participant in these defensive efforts told us that "Everyone was all self-congratulatory." He shook his head, pulled a grimace, and added softly, ". . . till they realized that the attacker had just gone all stealthy, but was probably still stealing us blind. We just couldn't see it anymore." The case names Moonlight Maze and Titan Rain are now best thought of as fleeting glimpses of a much broader campaign, most of which went unseen. It may seem somewhat incredible that terabytes of information can be removed from a company's network without that company being able to stop it all from going out the door. In the major cases we know about, the companies or federal organizations usually did not even detect that an exfiltration of data had occurred until well after it had taken place. All of these victims had intrusion-detection systems that are supposed to alarm when an unauthorized intruder attempts to get on a network. Some sites even had the more advanced intrusion-prevention systems, which not only alarm but also automatically take steps to block an intruder. The alarms remained silent. If you have a mental image of every interesting lab, company, and research facility in the U.S. being systematically vacuum cleaned by some foreign entity, you've got it right. That is what has been going on. Much of our intellectual property as a nation has been copied and sent overseas. Our best hope is that whoever is doing this does not have enough analysts to go through it all and find the gems, but that is a faint hope, particularly if the country behind the hacks has, say, a billion people in it.

One bright spot in this overall picture of data going out the door unhindered is what happened at Johns Hopkins University's Advanced Physics Laboratory (APL), outside Baltimore. APL does hundreds of millions of dollars of research every year for the U.S. government, from outer-space technology to biomedicine to secret "national security" projects. APL did discover in 2009 that it had huge amounts of data being secretly exfiltrated off its network and they stopped it. What is very telling is the way in which they stopped it. APL is one of the places that is really expert in cyber security and has contracts with the National Security Agency. So one might think that they were able to get their intrusion systems to block the data theft. No. The only way in which these cyber experts were able to prevent their network from being pillaged was to disconnect the organization from the Internet. APL pulled the plug and isolated its entire network, making it an island in cyberspace. For weeks, APL's experts went throughout the network, machine by machine, attempting to discover trapdoors and other malware. So the state of the art in really insuring that your data does not get copied right off your network appears to be to make sure that you are in no way connected to anybody. Even that turns out to be harder than it may seem. In large organizations, people innocently make connections to their home computers, to laptops with wi-fi connections, to devices like photocopiers that have their own connectivity through the Internet. If you are connected to the Internet in any way, it seems, your data is already gone.

The really good cyber hackers, including the best government teams from countries such as the U.S. and Russia, are seldom stumped when trying to penetrate a network, even if its operators think the network is not connected in any way to the public Internet. Furthermore, the varsity teams do something that causes network defenders to sound like paranoids. They never leave any marks that they were there, except when they want you to know. Think of Kevin Spacey's character's line in the movie The Usual Suspects: "The greatest trick the devil ever pulled was convincing the world he didn't exist."

Chapter 5. Toward a Defensive Strategy

Military theorists and statesmen, from Sun Tzu to von Clausewitz to Herman Kahn, have for centuries defined and redefined military strategy in varying ways, but they tend to agree that it involves an articulation of goals, means (broadly defined), limits (perhaps), and possibly sequencing. In short, military strategy is an integrated theory about what we want do and how, in general, we plan to do it. In part because Congress has required it, successive U.S. administrations have periodically published a National Security Strategy and a National Military Strategy for all the world to read. Within the military, the U.S. has many substrategies, such as a naval strategy, a counterinsurgency strategy, and a strategic nuclear strategy. The U.S. government has also publicly published strategies for dealing with issues wherein the military plays only a limited role, such as controlling illegal narcotics trafficking, countering terrorism, and stopping the proliferation of weapons of mass destruction. Oh yes, there is also that National Strategy to Secure Cyberspace dating back to 2003; but there is no publicly available cyber war strategy.

In the absence of a strategy for cyber war, we do not have an integrated theory about how to address key issues. To prove that, let's play Twenty Questions and see if there are agreed-upon answers to some pretty obvious questions about how to conduct cyber war:

- What do we do if we wake up one day and find the western half of the U.S. without electrical power as the result of a cyber attack?
- Is the advent of cyber war a good thing, or does it place us at a disadvantage?
- Do we envision the use of cyber war weapons only in response to the use of cyber war weapons against us?
- Are cyber weapons something that we will employ routinely in both small and large conflicts? Will we use them early in a conflict because they give us a unique advantage in seeking our goals, such as maybe effecting a rapid end to the conflict?
- Do we think we want to have plans and capabilities to conduct "stand-alone" cyber war against another nation? And will we fight in cyberspace even when we're not shooting at the other side in physical space?
- Do we see cyberspace as another domain (like the sea, airspace, or outer space) in which we must be militarily dominant and in which we will engage an opponent while simultaneously conducting operations in other domains?
- How surely do we have to identify who attacked us in cyberspace before we respond? What standards will we use for these identifications?
- Will we ever hide the fact that it was us who attacked with cyber weapons?
- Should we be hacking into other nations' networks in peace-time? If so, should there be any constraints on what we would do in peacetime?
- What do we do if we find that other nations have hacked into our networks in peacetime? What if they left behind logic bombs in our infrastructure networks?
- Do we intend to use cyber weapons primarily or initially against military targets only? How do we define military targets?
- Or do we see the utility of cyber weapons being their ability to inflict disruption on the economic infrastructure or the society at large?
- What is the importance of avoiding collateral damage with our cyber weapons? How might avoiding it limit our use of the weapons?

- If we are attacked with cyber weapons, under what circumstances would, or should, we respond with kinetic weapons? How much of the answer to this question should be publicly known in advance?
- What kind of goals specific to the employment of cyber weapons would we want to achieve if we conducted cyber war, either in conjunction with kinetic war or as a stand-alone activity?
- Should the line between peace and cyber war be brightly delineated, or is there an advantage to us in blurring that distinction?
- Would we fight cyber war in a coalition with other nations, helping to defend their cyberspace and sharing our cyber weapons, tactics, and targets?
- What level of command authority should authorize the use of cyber weapons, select the weapons, and approve the targets?
- Are there types of targets that we believe should not be attacked using cyber weapons? Do we attack them anyway if similar U.S. facilities are hit first by cyber or other weapons?
- How do we signal our intentions with regard to cyber weapons in peacetime and in crisis? Are there ways that we can use our possession of cyber weapons to deter an opponent?
- If an opponent is successful in launching a widespread, disabling attack on our military or on our economic infrastructure, how does that affect our other military and political strategies?

Didn’t do too well finding the answers anywhere in U.S. government documents, congressional hearings, or officials’ speeches? I didn’t, either. To be fair, these are not easy questions to answer, which is, no doubt, part of the reason they have not yet been knitted together into a strategy. As with much else, how one answers these and other questions will depend upon one’s experience and responsibilities, as well as the perspective that both create. Any general would like to be able to flip a switch and turn off the opposing force, especially if the same cannot be done to his forces in return. Modern generals know, however, that militaries are one of many instruments of the state, and the ultimate success of a military is now judged not just by what it does to the opponent, but by how well it protects and supports the rest of the state, including its underpinning economy. Military leaders and diplomats have also learned from past experiences that there is a fine line between prudent preparation to defend oneself and provocative activities that may actually increase the probability of conflict. Thus, crafting a cyber war strategy is not as obvious as simply embracing our newly discovered weapons, as the U.S. military did with nuclear weapons following Hiroshima.

Chapter 6. How Offensive?

In the seminal 1983 movie about computers and war, War Games, starring a young Matthew Broderick, the tinny computer voice asked haltingly, “Do you want to play a game of thermonuclear war?” Why don’t we play a game of cyber war in order to elucidate some of the policy choices that shape a strategy. DoD runs such exercises, called Cyber Storm, annually. The CIA’s annual cyber war exercise, Silent Horizon, has been happening since 2007. For the purposes of this analysis, I’ll make the same request of you that I made of students at Harvard’s Kennedy School and national security bureaucrats sitting around the White House Situation Room conference table: “Don’t fight the scenario.” By that I mean, do not spend a lot of time rejecting the premise that circumstances could happen someday that would result in the U.S. being on the edge of conflict with Russia or China.

When U.S. cyber warriors talk about the “big one,” they usually have in mind a conflict in cyberspace with Russia or China, the two nations with the most sophisticated offensive capability other than the U.S. No one wants hostilities with those countries to happen. Thinking about it, for the purposes of understanding what cyber war would look like, does not make it more likely. In fact, by understanding the risks of our current cyber war posture, we might reduce the chances of a real cyber war. And if, despite our intentions, a cyber war does happen, it would be best to have thought in advance about how it could unravel.

Certainly, I did not want to see the attack of 9/11 happen, but I had chaired countless “tabletop exercises,” or war game scenarios, to get myself and the bureaucracy ready in case something like it did happen. When it came, we had already thought through how to respond on the day of an attack and the few days thereafter. We spent enormous effort to try to prevent attacks, but we also devoted some time to thinking about what we would do if one succeeded. Had we not done so, that awful day would have been even worse. So, in that spirit of learning by visualizing, let’s think about a period of rising tensions between the U.S. and China.

Let’s call it Exercise South China Sea and set it a few years in the future. Not much has changed, except China has increased its dependence on the Net somewhat. For its part, the U.S. has not done much to improve its cyber defenses. We will have three teams, U.S. Cyber Command, the Chinese People’s Liberation Army (PLA) Cyber Division, and the Controllers, who play the part of everyone else. The Controllers also decide what happens as a result of the other two teams’ moves. Let’s say for the sake of the exercise that China has been aggressively pressing Vietnam and other ASEAN (Association of Southeast Asian Nations) countries to cede their rights to a vast and rich undersea area of gas and oil fields. (China has, in fact, claimed waters that run hundreds of miles to its south, along the coasts of Vietnam and the Philippines.) We will stipulate that there have been small clashes between their navies. In an irony of history, we will say that the government of Vietnam has asked the U.S. for military support, as have other nations in the region with claims on the contested waters. In response, the President has authorized a joint U.S.-ASEAN naval exercise and has dispatched two U.S. carrier battle groups, about twenty ships, including about 150 aircraft and several submarines. China and the U.S. have exchanged diplomatic notes and public pronouncements, with both countries essentially saying that the other one should stay out of the issue. American cable news networks have at this point started showing dramatic slides with the words “South China Sea Crisis.”

As our hypothetical exercise opens at Fort Meade, the team playing Cyber Command has been ordered by the Pentagon to prepare a series of steps it could take as the political situation escalates. The order from the Secretary of Defense is to develop options to:

First, dissuade the Chinese government from acting militarily over the contested waters. Second, failing that, to reduce to the maximum extent possible the ability of the Chinese military to pose a risk to U.S. and allied forces in the area. Third, in the event of increased tensions or the outbreak of hostilities, to be able to disrupt the Chinese military more broadly to reduce its ability to project force. Fourth, to occupy the Chinese leadership with disruption of their domestic infrastructure to the extent that it may cause popular and Party questioning of the Chinese government's aggressive behavior abroad. Fifth, throughout this period Cyber Command is to work with appropriate U.S. government agencies to prevent Chinese-government or Chinese-inspired cyber attacks on the U.S. military or significant U.S. infrastructure.

Chapter 7. Cyber Peace

The United States, almost single-handedly, is blocking arms control in cyberspace. Russia, somewhat ironically, is the leading advocate. Given the potential destabilizing nature and disadvantages of cyber war to the U.S., as discussed in the earlier chapters, one might think that by now the United States would have begun negotiating international arms control agreements that could limit the risks. In fact, since the Clinton Administration first rejected a Russian proposal, the U.S. has been a consistent opponent of cyber arms control.

Or, to be completely frank, perhaps I should admit that I rejected the Russian proposal. There were many who joined me; few U.S. government decisions are ever the responsibility of a single person. However, one of my jobs in the Clinton White House was to coordinate cyber security policy, including international agreements, across the government. Despite some interest in the State Department in pursuing cyber arms control, and although the U.S. had to stand almost alone in the U.N. in rejecting cyber talks, we said no. I viewed the Russian proposal as largely a propaganda tool, as so many of their multilateral arms control initiatives had been for decades. Verification of any cyber agreement seemed impossible. Moreover, the U.S. had not yet explored what it wanted to do in the area of cyber war. It was not obvious then whether or not cyber war added to or subtracted from U.S. national security. So we said no, and we have kept saying no for over a decade now.

Now that over twenty nations' militaries and intelligence services have created offensive cyber war units and we have gained a better understanding of what cyber war could look like, it may be time for the United States to review its position on cyber arms control and ask whether there is anything beneficial that could be achieved through an international agreement.

Often arms control negotiations have found difficulty in achieving agreement on something as basic as a definition of what it is that they were seeking to limit. I sat around the table for months with Soviet counterparts trying to define something as simple as "military personnel." For the purposes of discussion in this book, we won't have that kind of delay. Let's take the definition we used in chapter 1 and make it sound more like treaty language:

> Cyber warfare is the unauthorized penetration by, on behalf of, or in support of, a government into another nation's computer or network, or any other activity affecting a computer system, in which the purpose is to add, alter, or falsify data, or cause the disruption of or damage to a computer, or network device, or the objects a computer system controls.

With that definition and the U.S. asymmetrical vulnerabilities in mind, are there successes in other forms of arms control that could be ported into cyberspace, or new ideas unique to the characteristics of cyber war that could form the basis of beneficial arms control? What are the pitfalls of bad arms control to which we should give special attention and caution when thinking about limits on cyber war? How could an international agreement limiting some aspects of cyber war be beneficial to the United States, as well as operationally feasible and adequately verifiable?

Chapter 8. The Agenda

“It’s POTUS”

Those were the words our hypothetical White House official heard in chapter 2. Most of the time, those are words you never want to hear, at least when somebody is shoving a phone in your direction in a crisis. The sixth element of our agenda is, however, Presidential involvement. I know that everyone working on a policy issue thinks the President should spend a day a week on his or her pet rock. I don’t.

The President should, however, be required to approve personally the emplacement of logic bombs in other nations’ networks, as well as approve the creation of trapdoors on a class of politically sensitive targets. Because logic bombs are a demonstration of hostile intent, the President alone should be the one who decides that he or she wants to run the destabilizing risks associated with their placement. The President should be the one to judge the likelihood of the U.S. being in armed conflict with another nation in the foreseeable future, and only if that possibility is high should he or she authorize logic bombs. Key congressional leaders should be informed of such presidential decisions, just as they are for other covert-actions. Then, on an annual basis, the President should review the status of all major cyber espionage, cyber war preparation of the battlefield, and cyber defense programs. An annual cyber defense report to the President should spell out the progress made on defending the backbone, securing the DoD networks, and (let me hear you say it) protecting the electric power grid.

In this annual checkup, the President should review what Cyber Command has done: what networks they have penetrated, what options would be available to him in a crisis, and whether there are any modifications needed to his earlier guidance. This review would be similar to the annual covertaction review and the periodic dusting off of the nuclear war plan with the President. Knowing that there is an annual checkup keeps everybody honest. While he is reviewing the cyber war strategy implementation, the President could annually get a report from our proposed Cyber Defense Administration on its progress in securing government agencies, the Tier 1 ISPs, and (all together now) the power grid.

Finally, the President should put reducing Chinese cyber espionage at the top of the diplomatic agenda, and make clear that such behavior amounts to a form of economic warfare.

As I suggested earlier, the President should use the occasion of his annual commencement address at a military service academy, looking out over the cadets or midshipmen and their proud families, to promulgate the Obama Doctrine of Cyber Equivalence, whereby a cyber attack on us will be treated the same as if it were a kinetic attack and that we will respond in the manner we think best, based upon the nature and extent of the provocation. I suggested that he add a proposal for a global system of National Cyber Accountability that would impose on nations the responsibility to deal with cyber criminals and allegedly spontaneous civilian hack-tivists, and an Obligation to Assist in stopping and investigating cyber attacks. It would be a sharp contrast to the Bush Doctrine, announced at West Point, that expressed the sentiment that we should feel free to bomb or invade any nation that scares us, even before it does anything to us.

To follow up such a spring speech at an academy, the President should then in September give his annual address at the opening of the United Nations General Assembly session. Looking out from that green granite podium at the leaders or representatives of nine-score countries, he should say that

The cyber network technology that my nation has given to the world has become a great force for good, advancing global commerce, sharing medical knowledge that has saved millions of lives, exposing human rights violations, shrinking the globe, and, through DNA research, making us more aware that we are all descendants of the same African Eve.

But cyberspace has also been abused, as a playground for criminals, a place where billions of dollars are annually siphoned off to support cartels' illicit activities. And it has already been used by some as a battlespace. Because cyber weapons are so easily activated and the identity of an attacker can sometimes be kept secret, because cyber weapons can strike thousands of targets and inflict extensive disruption and damage in seconds, they are potentially a new source of instability in a crisis, and could become a new threat to peace.

Make no mistake about it, my nation will defend itself and its allies in cyberspace as elsewhere. We will consider an attack upon us through cyberspace as equivalent to any other attack and will respond in a manner we believe appropriate based on the provocation. But we are willing, as well, to pledge in a treaty that we will not be the first in a conflict to use cyber weapons to attack civilian targets. We would pledge that and more, to aid in the creation of a new international Cyber Risk Reduction Center, and undertake obligations to assist other nations being victimized by attacks originating in cyberspace.

Cyber weapons are not, as some have claimed, simply the next stage in the evolution of making war less lethal. If they are not properly controlled, they may result in small disagreements spiraling out of control and leading to wider war. And our goal as signers of the United Nations Charter is, as pledged in San Francisco well over half a century ago, "to save succeeding generations from the scourge of war." I ask you to join me in taking a step back from the edge of what could be a new battlespace, and take steps not to fight in cyberspace, but to fight against cyber war.

It could be a beautiful speech, and it could make us safer.