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.

Almost as unusual as the raid itself was the political silence that followed. The public affairs offices of the Israeli government said nothing. Even more telling, Syria, which had been bombed, was silent. Slowly, the story started to emerge in American and British media. Israel had bombed a complex in eastern Syria, a facility being built by North Koreans. The facility was related to weapons of mass destruction, the news accounts reported from unnamed sources. Israeli press censors allowed their nation's newspapers to quote American media accounts, but prohibited them from doing any reporting of their own. It was, they said, a national security matter. Prompted by the media accounts, the Syrian government belatedly admitted there had been an attack on their territory. Then they protested it, somewhat meekly. Syrian President Assad asserted that what had been destroyed was "an empty building." Curiously, only North Korea joined Damascus in expressing outrage at this surprise attack.

Media accounts differed slightly as to what had happened and why, but most quoted Israeli government sources as saying that the facility had been a North Korean–designed nuclear weapons plant. If that was true, North Korea had violated an agreement with the United States and other major powers that it would stop selling nuclear weapons know-how. Worse, it meant that Syria, a nation on Israel's border, a nation that had been negotiating with Israel through the Turks, had actually been trying secretly to acquire nuclear weapons, something that even Saddam Hussein had stopped doing years before the U.S. invasion of Iraq.

Soon, however, self-anointed experts were casting doubt on the "Syria was making a nuclear bomb" story.

Satellite pictures, taken by reconnaissance satellite, were revealed by Western media. Experts noted that the site had little security around it before the bombing. Some contended that the building was not tall enough to house a North Korean nuclear reactor. Others pointed to the lack of any other nuclear infrastructure in Syria. They offered alternative theories. Maybe the building was related to Syria's missile program. Maybe Israel had just gotten it wrong and the building was relatively innocent, like Saddam Hussein's alleged "baby milk factory" of 1990 or Sudan's supposed aspirin plant of 1998, both destroyed in U.S. strikes. Or maybe, said some commentators, Syria was not the real target. Maybe Israel was sending a message to Iran, a message that the Jewish state could still successfully carry out surprise air strikes, a message that a similar strike could occur on Iranian nuclear facilities unless Tehran stopped its nuclear development program.

Media reports quoting unnamed sources claimed various degrees of American involvement in the raid: the Americans had discovered the site on satellite photography, or the Americans had overlooked the site and the Israelis had found it on satellite images given to them routinely by the U.S. intelligence community; the Americans had helped plan the bombing, perhaps persuading the Turkish military to look the other way as the Israeli attack formation sailed over
Turkey to surprise Syria by attacking from the north. Americans—or were they Israelis?—had perhaps sneaked into the construction site before the bombing to confirm the North Korean presence, and maybe verify the nuclear nature of the site. President George W. Bush, uncharacteristically taciturn, flatly refused to answer a reporter's question about the Israeli attack.

The one thing that most analysts agreed upon was that something strange had happened. In April 2008, the CIA took the unusual step of producing and publicly releasing a video showing clandestine imagery from inside the facility before it was bombed. The film left little doubt that the site had been a North Korean–designed nuclear facility. The story soon faded. Scant attention was paid when, seven months later, the UN's International Atomic Energy Agency (IAEA) issued its report. It had sent inspectors to the site. What the inspectors found was not a bombed-out ruin, nor did they come upon a beehive of renewed construction activity. Instead, the international experts were taken to a site that had been neatly plowed and raked, a site showing no signs of debris or construction materials. It looked like an unimproved home lot for sale in some desert community outside of Phoenix, perfectly anodyne. The disappointed inspectors took pictures. They filled plastic ziplock baggies with soil samples and then they left the banks of the Euphrates and flew back to their headquarters on an island in the Danube near Vienna. There they ran tests in their laboratories.

The IAEA announced; again to little attention, that the soil samples had contained unusual, "man-made," radioactive materials. For those few who had been following the mystery of Syria's Euphrates enigma, that was the end of the story, vindicating Israel's highly regarded intelligence service. Despite how unlikely it seemed, Syria in fact had been secretly fooling around with nuclear weapons, and the bizarre regime in North Korea had been helping. It was time to reassess the intentions of both Damascus and Pyongyang.

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. Moscow promised
to send experts and technicians right away. Maybe there had been an implementation problem, maybe a user error, but it would be fixed immediately. The Russian military-industrial complex did not need that kind of bad publicity about its products. After all, Iran was about to buy a modern air defense radar and missile system from Moscow. In both Tehran and Damascus, air defense commanders were in shock.

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. There are at least three possibilities for how they “owned” the Syrians. First, there is the possibility suggested by some media reports that the Israeli attack was preceded by a stealthy unmanned aerial vehicle (UAV) that intentionally flew into a Syrian air defense radar’s beam. Radar still works essentially the same way it began seventy years ago in the Battle of Britain. A radar system sends out a directional radio beam. If the beam hits anything, it bounces back to a receiver. The processor then computes where the object was that the radio beam hit, at what altitude it was flying, at what speed it was moving, and maybe even how big an object was up there. The key fact here is that the radar is allowing an electronic beam to come from the air, back into the ground-based computer system.

Radar is inherently an open computer door, open so that it can receive back the electronic searchers it has sent out to look for things in the sky. A stealthy Israeli UAV might not have been seen by the Syrian air defense because the drone would have been coated with material that absorbs or deflects a radar beam. The UAV might, however, have been able to detect the radar beam coming up from the ground toward it and used that very same radio frequency to transmit computer packets back down into the radar’s computer and from there into the Syrian air defense network. Those packets made the system malfunction, but they also told it not to act there was anything wrong with it. They may have just replayed a do-loop of the sky as it was before the attack. Thus, while the radar beam might later have bounced off the attacking Eagles and Falcons, the return signal did not register on the Syrian air defense computers. The sky would look just like it had when it was empty, even though it was, in actuality, filled with Israeli fighters. U.S. media reports indicate that the United States has a similar cyber attack system, code-named Senior Suter.

Second, there is the possibility that the Russian computer code controlling the Syrian air defense network had been compromised by Israeli agents. At some point, perhaps in the Russian computer lab or in a Syrian military facility, someone working for Israel or one of its allies may have slipped a “trapdoor” into the millions of lines of computer code that run the air defense program. A “trapdoor” (or “Trojan Horse”) is simply a handful of lines of computer code that look just like all the other gibberish that comprise the instructions for an operating system or application. (Tests run by the National Security Agency determined that even the best-trained experts could not, by visually looking through the millions of lines of symbols, find the “errors” that had been introduced into a piece of software.)

The “trapdoor” could be instructions on how to respond to certain
circumstances. For example, if the radar processor discovers a particular electronic signal, it would respond by showing no targets in the sky for a designated period of time, say, the next three hours. All the Israeli UAV would have to do is send down that small electronic signal. The "trapdoor" might be a secret electronic access point that would allow someone tapping into the air defense network to get past the intrusion-detection system and firewall, through the encryption, and take control of the network with full administrator's rights and privileges.

The third possibility is that an Israeli agent would find any fiber-optic cable of the air defense network somewhere in Syria and splice into the line (harder than it sounds, but doable). Once on line, the Israeli agent would type in a command that would cause the "trap-door" to open for him. While it is risky for an Israeli agent to be wandering around Syria cutting into fiber-optic cables, it is far from impossible. Reports have suggested for decades that Israel places its spies behind Syrian borders. The fiber-optic cables for the Syrian national air defense network run all over the country, not just inside military installations. The advantage of an agent in place hacking into the network is that it does not cause the operation to rely upon the success of a "takeover packet" entering the network from a UAV flying overhead. Indeed, an agent in place could theoretically set up a link from his location back to Israel's Air Force command post. Using low-probability-of-intercept (LPI) communications methods, an Israeli agent may be able to establish "cove comms" (covert communications), even in downtown Damascus, beaming up to a satellite with little risk of anyone in Syria noticing.

Whatever method the Israelis used to trick the Syrian air defense network, it was probably taken from a playbook they borrowed from the U.S. Our Israeli friends have learned a thing or two from the programs we have been working on for more than two decades. In 1990, as the United States was preparing to go to war with Iraq for the first time, early U.S. cyber warriors got together with Special Operations commandos to figure out how they could take out the extensive Iraqi air defense radar and missile network just before the initial waves of U.S. and allied aircraft came screeching in toward Baghdad. As the hero of Desert Storm, four-star General Norm Schwarzkopf, explained to me at the time, "these snake-eaters had some crazy idea" to sneak into Iraq before the first shots were fired and seize control of a radar base in the south of the country. They planned to bring with them some hackers, probably from the U.S. Air Force, who would hook up to the Iraqi network from inside the base and then send out a program that would have caused all the computers on the network all over the country to crash and be unable to reboot.

Schwarzkopf thought the plan risky and unreliable. He had a low opinion of U.S. Special Operations Command and feared that the commandos would become the first Americans held as prisoners of war, even before the war started. Even worse, he feared that the Iraqis would be able to turn their computers back on and would start shooting down some of the two thousand sorties of attacks he planned for the first day of the air war. "If you want to make sure their air defense radars and missiles don't work, blow them up first. That way they stay dead. Then go in and bomb your targets." Thus, most of the initial U.S. and allied air sorties were not bombing raids on Baghdad headquarters or Iraqi Army divisions, they were on the air defense radar and missile sites. Some U.S. aircraft were destroyed in those attempts, some pilots were killed, and some were taken prisoner.

When, thirteen years later, the U.S. went to war with Iraq a second time, well before the initial waves of American fighter-bombers swept in, the Iraqi military knew that their "closed-loop" private, secure military network had already been compromised. The Americans told them.

Thousands of Iraqi military officers received e-mails on the Iraqi Defense Ministry e-mail system just before the war started.
Although the exact text has never been made public, several reliable sources revealed enough of the gist to reconstruct what you might have read had you been, say, an Iraqi Army brigadier general in charge of an armored unit outside of Basra. It would have read something like this:

This is a message from United States Central Command. As you know, we may be instructed to invade Iraq in the near future. If we do so, we will overwhelm forces that oppose us, as we did several years ago. We do not want to harm you or your troops. Our goal would be to displace Saddam and his two sons. If you wish to remain unharmed, place your tanks and other armored vehicles in formation and abandon them. Walk away. You and your troops should go home. You and other Iraqi forces will be reconstituted after the regime is changed in Baghdad.

Not surprisingly, many Iraqi officers obeyed the instructions CENTCOM had e-mailed them, on the secret Iraqi network. U.S. troops found many units had neatly parked their tanks in rows outside their bases, thus allowing U.S. aircraft to neatly blow them up. Some Iraqi army commanders sent their troops on leave in the hours before the war. Troops put on civilian clothes and went home, or at least tried to.

Although willing to hack into Iraq’s network to engage in a psychological campaign prior to the onset of the conventional attack, the Bush Administration was apparently unwilling to destroy Saddam Hussein’s financial assets by cracking into the networks of banks in Iraq and other countries. The capability to do so existed, but government lawyers feared that raiding bank accounts would be seen by other nations as a violation of international law, and viewed as a precedent. The counsels also feared unintended consequences if the U.S. cyber bank robberies hit the wrong accounts or took out entire financial institutions.

The second U.S.-Iraq war, and the more recent Israeli attack on Syria, had demonstrated a new use of cyber war. One use of cyber war is to make a conventional (the U.S. military prefers the term “kinetic”) attack easier by disabling the enemy’s defenses. Another use of cyber war is to send propaganda out to demoralize the enemy, distributing e-mails and other Internet media in place of the former practice of dropping pamphlets. (Recall the thousands of pieces of paper with instructions in Arabic and stick-figure drawings dropped on Iraqi forces in 1991, telling them how to surrender to U.S. forces. Thousands of Iraqis brought the pamphlets with them when they did surrender.)

The raid on the Syrian nuclear facility and the U.S. cyber activity that preceded the invasion of Iraq are examples of the military using hacking as a tool to assist in a more familiar kind of war. The use of cyberspace by nation-states for political, diplomatic, and military goals does not, however, have to be accompanied by bombing raids or tank battles. A small taste of what a stand-alone cyber war could look like came, somewhat surprisingly, in a little Hanseatic League city of 400,000 people on the shores of the Baltic. The city of Tallinn had become, once again, the capital of an independent Estonia in 1989 when the Soviet Union disintegrated and many of its component republics disassociated themselves from Moscow and the U.S.S.R. Estonia had been forced to become part of the Soviet Union when the Red Army “liberated” the Baltic republic from the Nazis during what the Russians call “the Great Patriotic War.”

The Red Army, or at least the Communist Party of the Soviet
Union, didn’t want Estonians, or any other East Europeans, to forget the sacrifices that were made “liberating” them. Thus, in Tallinn, as in most East European capitals, they erected one of those giant, heroic statues of a Red Army soldier that the Soviet leaders had such a fondness for. Often these bronze stood atop the graves of Red Army soldiers. I first stumbled upon such a statue, almost literally, in Vienna in 1974. When I asked the police protecting it why neutral Austria had a giant Communist soldier in its downtown, they told me that the Soviet Union had put it up right after the war and that had required the Austrians to promise never to take it down. Indeed, the statue is specifically protected in the treaty the U.S. and Austria signed, along with the Soviets, when American and Soviet troops left Austria in 1950. Back in the 1970s, the Viennese almost uniformly described the enormous bronze as “the only Russian soldier in Vienna who did not rape our women.” It seems these statues mean a great deal to the Russians, just as the overseas graves of American World War II dead are sacred ground to many American veterans, their families, and their descendents. The giant bronze statues also had significant meaning to those who were “liberated,” but that meaning was something entirely different. The statues and the dead bodies of Red Army soldiers under them were, symbolically, lightning rods. In Tallinn, the statue also attracted cyber lightning.

Tensions between ethnic Russians living in Estonia and the native Estonians themselves had been building ever since the little nation had declared its independence again at the end of the Cold War. The majority of Estonians sought to remove any sign of the five oppressive decades during which they had been forced to be part of the Soviet Union. In February 2007, the legislature passed a Forbidden Structures Law that would have caused anything denoting the occupation to be taken down, including the giant bronze soldier.

Estonians still resented the desecration of their own veterans’ graves that had followed the appearance of the Red Army.

Moscow complained that moving the bronze soldier would defame the heroic Soviet dead, including those buried around the giant bronze. Seeking to avoid an incident, the Estonian President vetoed the law. But public pressure to remove the statue grew, just as a Russian ethnic group dedicated to protecting the monument and an Estonian nationalist group threatening to destroy it became increasingly militant. As the Baltic winter warmed into spring, the politics moved to the street. On April 27, 2007, now known as Bronze Night, a riot broke out between radicals from both ethnic factions, with the police and the statue caught in the middle. Authorities quickly intervened and moved the statue to a new, protected location in the military cemetery. Far from quelling the dispute, the move ignited indignant nationalist responses in the Moscow media and in Russia’s legislature, the Duma.

This is when the conflict moved into cyberspace. Estonia, oddly, is one of the most wired nations in the world, ranking, along with South Korea, well ahead of the United States in the extent of its broadband penetration and its utilization of Internet applications in everyday life. Those advances made it a perfect target for cyber attack. After Bronze Night, suddenly the servers supporting the most often utilized webpages in Estonia were flooded with cyber access requests, so flooded that some of the servers collapsed under the load and shut down. Other servers were so jammed with incoming pings that they were essentially inaccessible. Estonians could not use their online banking, their newspapers’ websites, or their government’s electronic services.

What had hit Estonia was a DDOS, a distributed denial of service attack. Normally a DDOS is considered a minor nuisance, not a major weapon in the cyber arsenal. Basically it is a preprogrammed
flood of Internet traffic designed to crash or jam networks. It is “distributed” in the sense that thousands, even hundreds of thousands, of computers are engaged in sending the electronic pings to a handful of targeted locations on the Internet. The attacking computers are called a “botnet,” a robotic network, of “zombies,” computers that are under remote control. The attacking zombies were following instructions that had been loaded onto them without their owners’ knowledge. Indeed, the owners usually cannot even tell when their computers have become zombies or are engaged in a DDoS.

A user may notice that the laptop is running a little slowly or that accessing webpages is taking a little longer than normal, but that is the only indicator. The malicious activity is all taking place in the background, not appearing on the user’s screen. Your computer, right now, might be part of a botnet.

What has happened, often weeks or months before a botnet went on the offensive, is that a computer’s user went to an innocent-looking webpage and that page secretly downloaded the software that turned their computer into a zombie. Or they opened an e-mail, perhaps even one from someone they knew, that downloaded the zombie software. Updated antivirus or firewall software may catch and block the infections, but hackers are constantly discovering new ways around these defenses.

Sometimes the zombie computer sits patiently awaiting orders. Other times it begins to look for other computers to attack. When one computer spreads its infection to others, and they in turn do the same, we have the phenomenon known as a “worm,” the infection worming its way from one computer through thousands or millions. An infection can spread across the globe in mere hours.

In Estonia the DDoS was the largest ever seen. It appeared that several different botnets, each with tens of thousands of infected machines that had been sleeping, were now at work. At first, the Estonians thought that the takedown of some of their webpages was just an annoyance sent at them from outraged Russians. Then the botnets started targeting Internet addresses most people would not know, not those of public webpages, but the addresses of servers running parts of the telephone network, the credit-card verification system, and the Internet directory. Now over a million computers were engaged in sending a flood of pings toward the servers they were targeting in Estonia. Hansapank, the nation’s largest bank, was staggered. Commerce and communications nationwide were being affected. And the attacks did not stop.

In most previous eruptions of a DDoS attack, one site would be hit for a few days. This was something different. Hundreds of key sites in one country were being hit week after week, unable to get back up. As Internet security experts rushed to Tallinn from Europe and North America, Estonia brought the matter before the North Atlantic Council, the highest body of the NATO military alliance. An ad hoc incident response team began trying countermeasures that had been successful in the past with smaller DDoS attacks. The zombies adapted, probably being reprogrammed by the master computers. The attacks continued. Using trace-back techniques, cyber security experts followed the attacking pings to specific zombie computers and then watched to see when the infected machines “phoned home” to their masters. Those messages were traced to controlling machines, and sometimes further traced to higher-level controlling devices. Estonia claimed that the ultimate controlling machines were in Russia, and that the computer code involved had been written on Cyrillic-alphabet keyboards.

The Russian government indignantly denied that it was engaged in cyber war against Estonia. It also refused Estonia’s formal diplomatic request for assistance in tracing the attackers, although a standing bilateral agreement required Moscow to cooperate. Informed that the attacks had been traced back to Russia, some government officials admitted that it was possible perhaps that patriotic
Russians, incensed at what Estonia had done, were taking matters into their own hands. Perhaps.

But even if the "patriotic Russians" theory were to be believed, it left unanswered the question of why the Russian government would not move to stop such vigilantism. No one doubted for a minute that the KGB's successors had the ability to find the culprits and to block the traffic. Others, more familiar with modern Russia, suggested that what was at work was far more than a passive Russian police turning a blind eye to the hooliganism of overly nationalist youth. The most adept hackers in Russia, apart from those who are actual government employees, are usually in the service of organized crime. Organized crime is allowed to flourish because of its unacknowledged connection to the security services. Indeed, the distinction between organized criminal networks and the security services that control most Russian ministries and local governments is often blurry. Many close observers of Russia think that some senior government officials permit organized crime activity for a slice of the profits, or, as in the case of Estonia, for help with messy tasks. Think of Marlon Brando as the Godfather saying, "Someday... I will call upon you to do a service for me..."

After Bronze Night, the Russian security services had encouraged domestic media outlets to whip up patriotic sentiment against Estonia. It is not a stretch to imagine that they also asked organized crime groups to launch the hackers in their employ, perhaps even giving those hackers some information that would prove helpful. Did the Russian government security ministries engage in cyber attacks on Estonia? Perhaps that is not the right question. Did they suggest the attacks, facilitate them, refuse to investigate or punish them? And, in the end, does the distinction really matter when you are an Estonian unable to get your money out of a Hansapank ATM?

Following the cyber attack, NATO moved to create a cyber defense center. It opened in 2008, a few miles from the site where the giant bronze soldier had originally stood. On the original site of the bronze soldier there is a nice little grove of trees now. Unfortunately, the NATO center in Tallinn was of little use when another former Soviet satellite republic, Georgia, and Mother Russia got into a tussle over some small disputed provinces.

The Republic of Georgia lies directly south of Russia along the Black Sea, and the two nations have had a decidedly unequal relationship for well over a century. Georgia is geographically slightly smaller than the state of South Carolina and has a population of about four million people. Given its location and size, Georgia has been viewed by Moscow as properly within the Kremlin's "sphere of influence." When the original Russian empire began to disintegrate after the Russian Revolution, the Georgians tried to make a break for it while the Russians were too busy fighting each other, declaring Georgian independence in 1918. As soon as the Russians finished fighting each other, however, the victorious Red Army quickly invaded Georgia, installed a puppet regime, and made Georgia part of the Union of Soviet Socialist Republics. Soviet control of Georgia lasted until 1991, when, as the central Russian government was again in turmoil, Georgia once more took the opportunity to declare independence.

Two years later, Georgia lost control of two territories, South Ossetia and Abkhazia. Supported by Moscow, the local Russian populations in those territories succeeded in defeating the ragtag Georgian army and expelling most Georgians. The territories then set up "independent" governments. Although still legally part of Georgia as far as the rest of the world was concerned, the regions relied on Russian funding and protection. Then, in July 2008, South
Osetian rebels (or Russian agents, depending upon whose version of events you trust) provoked a conflict with Georgia by staging a series of missile raids on Georgian villages.

The Georgian army, predictably, responded to the missile strikes on its territory by bombing the South Ossetian capital city. Then, on August 7, Georgia invaded the region. Not surprised by this turn of events, the Russian army moved the next day, quickly ejecting the Georgian army from South Ossetia. Precisely at the same time that the Russian army moved, so did its cyber warriors. Their goal was to prevent Georgians from learning what was going on, so they streamed DDOS attacks on Georgian media outlets and government websites. Georgia’s access to CNN and BBC websites were also blocked.

In the physical world, the Russians also bombarded Georgia and took over a small chunk of Georgian territory that was not in dispute, allegedly to create a “buffer zone.” While the Georgian army was busy getting routed in Ossetia, rebel groups in Abkhazia decided to take advantage of the situation and push out any remaining Georgians, with a little help from their Russian backers. The Russian army then took another little slice of Georgian land, as an additional buffer. Three days later, most of the fighting was over. French President Nicolas Sarkozy brokered a cease-fire in which the Russians agreed to withdraw from Georgia immediately and to leave the disputed territories once an international peacekeeping force arrived to fill the security vacuum. That force never arrived, and within a few weeks Russia recognized South Ossetia and Abkhazia as independent states. The declared independent states then invited their Russian benefactors to stay.

In the U.S., except then presidential candidate John McCain, who tried to portray it as a national security crisis for America, all of this activity in Georgia seemed remote and unimportant. As soon as most Americans reassured themselves that the news reports they heard about the invasion of Georgia did not really mean Russian army troops or General Sherman again marching on Atlanta, they tuned out. The event’s true significance, beyond what it revealed of the Russian rulers’ thinking about their former empire, lies in what it exposed of their attitudes toward the use of cyber attacks.

Before fighting broke out in the physical world, cyber attacks hit Georgian government sites. In the initial stages, the attackers conducted basic DDOS attacks on Georgian government websites and hacked into the web server of the President’s site to deface it, adding pictures that compared the Georgian leader, Mikheil Saakashvili, to Adolf Hitler. It had seemed trivial, even juvenile, at first. Then the cyber attacks picked up in intensity and sophistication just as the ground fighting broke out.

Georgia connects to the Internet through Russia and Turkey. Most of the routers in Russia and Turkey that send traffic on to Georgia were so flooded with incoming attacks that no outbound traffic could get through. Hackers seized direct control of the rest of the routers supporting traffic to Georgia. The effect was that Georgians could not connect to any outside news or information source and could not send email out of the country. Georgia effectively lost control of the nation’s “.ge” domain and was forced to shift some government websites to servers outside the country.

The Georgians tried to defend their cyberspace and engage in “work-arounds” to foil the DDOS attack. The Russians countered every move. Georgia tried to block all traffic coming from Russia. The Russians rerouted their attacks, appearing as packets from China. In addition to a Moscow-based master controller for all the botnets being used in the attacks, servers in Canada, Turkey, and, ironically, Estonia were also used to run botnets.

Georgia transferred the President’s webpage to a server on Google’s blogspot in California. The Russians then set up mock presidential sites and directed traffic to them. The Georgian banking sector shut
down its servers and planned to ride out the attacks, thinking that a temporary loss of online banking was a better bargain than risking the theft of critical data or damage to internal systems. Unable to get to the Georgian banks, the Russians had their botnets send a barrage of traffic to the international banking community, pretending to be cyber attacks from Georgia. The attacks triggered an automated response at most of the foreign banks, which shut down connections to the Georgian banking sector. Without access to European settlement systems, Georgia's banking operations were paralyzed. Credit-card systems went down as well, followed soon after by the mobile phone system.

At their peak, the DDOS attacks were coming from six different botnets using both computers commandeered from unsuspecting Internet users and from volunteers who downloaded hacker software from several anti-Georgia websites. After installing the software, a volunteer could join the cyber war by clicking on a button labeled "Start Flood."

As in the Estonian incident, the Russian government claimed that the cyber attacks were a populist response that was beyond the control of the Kremlin. A group of Western computer scientists, however, concluded that the websites used to launch the attacks were linked to the Russian intelligence apparatus. The level of coordination shown in the attacks and the financing necessary to orchestrate them suggest this was no casual cyber crusade triggered by patriotic fervor. Even if the Russian government were to be believed (namely, that the cyber storm let loose on Georgia, like the previous one on Estonia, was not the work of its official agents), it is very clear that the government did nothing to stop it. After all, the huge Soviet intelligence agency, the KGB, is still around, although with a slightly different organizational structure and name. Indeed the KGB's power has only increased under the regime of its alumnus, Vladimir Putin. Any large-scale cyber activity in Russia, whether done by government, organized crime, or citizens, is done with the approval of the intelligence apparatus and its bosses in the Kremlin.

If it was, as we suspect, effectively the Russian government that asked for the "vigilante" DDOS and other cyber attacks as a stand-alone punishment of Estonia and later conducted them as an accompaniment to kinetic war on Georgia, those operations do not begin to reveal what the Russian military and intelligence agencies could do if they were truly on the attack in cyberspace. The Russians, in fact, showed considerable restraint in the use of their cyber weapons in the Estonian and Georgian episodes. The Russians are probably saving their best cyber weapons for when they really need them, in a conflict in which NATO and the United States are involved.

For years U.S. intelligence officials had thought that if any nation were going to use cyber weapons, even in the small ways demonstrated in Estonia and Georgia, the likely first movers would be Russia, China, Israel, and, of course, the United States. The nation that joined that club in the summer of 2009 came as a surprise to some.

It was a little after seven p.m. in Reston, Virginia, on the last Monday in May 2009. Outside, the rush-hour traffic was beginning to thin on the nearby Dulles Airport Access Road. Inside, a flat screen at the U.S. Geological Survey had just indicated a 4.7 magnitude earthquake in Asia. The seismic experts began narrowing in on the epicenter. It was in the northeastern corner of the Korean Peninsula, specifically forty-three miles from a town on the map called Kimchaoe. The data showed that there had been a similar event very nearby in October 2006. That one had turned out to be a nuclear explosion. So did this one.

After years of negotiating with the U.S., as well as with China and Russia, the weird, hermetic government of North Korea had decided to defy international pressure and explode a nuclear bomb,
for the second time. Their first attempt, three years earlier, had been characterized by some Western observers as something like a "partial fizzle." In the ensuing hours after this second blast, U.S. Ambassador to the United Nations Susan E. Rice was attached to the phone in her suite at New York's Waldorf Towers. She consulted with the White House and the State Department, then she began to call other UN ambassadors, notably the Japanese and South Koreans. The South Korean who is the head of the UN, Secretary General Ban Ki-moon, agreed to an emergency meeting of the Security Council. The outcome of that feverish round of diplomatic consultations was, eventually, further international condemnation of North Korea and further sanctions on the impoverished tyranny. A decade and a half's worth of diplomacy to prevent a North Korean nuclear capability had come to naught. Why?

Some observers of the Pyongyang government explained that the destitute North had no other leverage to extract concessionary loans, free food, and gifts of oil. It had to keep selling the same thing over and over, a promise not to go further with its nuclear capability. Others pointed to the ruined ill health of the strange man known in the North as the Dear One, Kim Jong-il, the leader of the Democratic People's Republic of Korea. The tea-leaf readers believed that the Dear One knew that he was fading and had selected Number Three Son, Kim Jong-un, a twenty-five-year-old, to succeed him. To prevent the United States, or South Korea, from taking advantage of the transition period, the analysts claimed, the North believed it had to rattle its sabers, or at least its atoms. The pattern with North Korea in the past had been to threaten, get attention, give a taste of what awful things might happen, then offer to talk, and eventually to cut a deal to enrich their coffers.

If the detonation was designed to provoke the United States and others to rush with offers of wheat and oil, it failed. Having condemned the explosion and announced the movement of defensive

missiles to Hawaii, as June moved on, the U.S. leadership shifted its focus back to health care reform, Afghanistan, and self-flagellation over its own intelligence activities. Somewhere in the bureaucracy an American official publicly announced that the U.S. would again be conducting a cyber war exercise known as Cyber Storm to test the defense of computer networks. The 2009 exercise would involve other nations, including Japan and Korea, the one in the south. North Korean media soon responded by characterizing the pending exercise as a cover for an invasion of North Korea. That kind of bizarre and paranoid analysis is par for the course with North Korea. No one in Washington thought twice about it.

As the July 4 break began in Washington, bureaucrats scattered to vacation homes on East Coast beaches. Tourists in Washington swarmed to the National Mall, where a crowd of several hundred thousand watched the "rockets' red glare" of a sensational fireworks display, a signature of the Fourth of July holiday. On the other side of the world, the association of rockets and the Fourth was not lost on some in the North Korean leadership. In outer space, a U.S. satellite detected a rocket launch from North Korea. Computers in Colorado quickly determined that the rocket was short-ranged and was fired into the sea. Then there was another rocket launch. Then another and another. Seven North Korean rockets were fired on the Fourth of July. Whether a plea for help, or mere saber rattling, it certainly seemed like a cry for attention. But that cry did not stop there. It moved into cyberspace.

Right before the Fourth of July holiday, a coded message was sent out by a North Korean agent to about 40,000 computers around the world that were infected with a botnet virus. The message contained a simple set of instructions: telling the computer to start pinging a list of U.S. and South Korean government websites and international companies. Whenever the infected computers were turned on, they silently joined the assault. If your computer was one of the zombies,
you might have noticed your processor was running slowly and your Web requests were taking a bit longer to process, but nothing too out of the ordinary. Yes, it was another DDOS attack by zombies in a botnet. At some time over the weekend, the U.S. government did notice when dhs.gov and state.gov became temporarily unavailable. If anyone actually thought of consulting the Department of Homeland Security terrorist threat level before deciding to go watch the fireworks on the National Mall, they would not have been able to gain that information from the Department of Homeland Security's website.

Each of those zombie computers was flooding these sites with requests to see their pages in another distributed denial of service attack. The U.S. websites were hit with as many as 1 million requests per second, choking the servers. The Treasury, Secret Service, Federal Trade Commission, and Department of Transportation web servers were all brought down at some point between July 4 and July 9. The NASDAQ, New York Mercantile, and New York Stock Exchange sites were also hit, as was the Washington Post. The DDOS aimed at the White House failed, however. To prevent the first DDOS attack against the White House in 1999, I had arranged with a company known as Akamai to route traffic seeking the White House website to the nearest of over 20,000 servers scattered around the world. When the Korean attack hit in 2009, the DDOS went to the White House servers nearest the source of the attacker. Thus, only sites hosting the White House website in Asia had trouble. White House spokesperson Nick Shapiro apologized in a halfhearted way to any web surfers in Asia who might not have been able to get onto the White House site. Then the second and third waves hit.

Another 30,000 to 60,000 computers infected with a different variant of the virus were told to target a dozen or more South Korean government sites, Korean banks, and a South Korean Internet security company on July 9. The attackers were apparently convinced that the attacks on U.S. sites were no longer going to be effective after the government and major corporations began working with Internet service providers (ISPs) to filter out the attacks. At 6:00 p.m. Korea time on July 10, the final assault began. The now estimated 166,000 computers in seventy-four countries stared flooding the sites of Korean banks and government agencies.

Ultimately, the damage was contained. The attack did not attempt to gain control of any government systems, nor did it disrupt any essential services. But it was likely only meant as a shot across the bow. What we do know is that there was an agenda and motivation for the attack. This was not a worm simply released into the wilds of the Internet and allowed to propagate. Someone controlled and directed the attack and modified its target list to focus on the more vulnerable Korean sites.

The U.S. government has yet to directly attribute the attack to North Korea, though South Korea has not been shy about doing so. The timing of the attacks does suggest the North Korean regime is the prime suspect, but definite attribution is difficult. The infected computers attempted to contact one of eight "command and control servers" every three minutes. These servers sent instructions back to the infected zombie computers, telling them which websites to attack. The eight masters were in South Korea, the United States, Germany, Austria, and, interestingly, Georgia (the country).

The Korea Communications Commission has endorsed the judgment of a Vietnamese firm, Bach Khoa Internetwork Security (BKIS), that these eight servers were controlled from a server in Brighton, England. From there, the trail goes cold, though it does not look like the mastermind behind the attack was sitting in front of a keyboard near the beach in Brighton. South Korea's National Intelligence Service (NIS) suspects that a North Korean military research institute set up to destroy South Korea's communications
infrastructure was involved. The NIS said in a statement following the attack that it had evidence that pointed to North Korea.

The NIS maintains that the North Korean hacker unit, known as Lab 110, or the “technology reconnaissance team,” was ordered to prepare a plan for cyber attack on June 7. That order directed the unit to “destroy the South Korean puppet communications networks in an instant,” following the decision by the South Koreans to participate in Exercise Cyber Storm. The North called the exercise “an intolerable provocation as it revealed ambition to invade the DPRK.”

South Korea is now preparing for all-out cyber war with the North. Just before the attacks began, South Korea had announced plans for establishing a cyber warfare command by 2012. After the attacks, it sped up the timeline to January 2010. What the South’s new cyber warfare command will do the next time the North attacks in cyberspace is unclear.

If North Korea attacks in cyberspace again, options for responding are relatively limited. Sanctions cannot be made much tighter. Suspected food aid cannot be suspended further. Any military action in retaliation is out of the question. The 23 million residents of metropolitan Seoul live within range of North Korea’s artillery pieces, set along the demilitarized zone in what military planners refer to as “the kill box.”

There is also little possibility of responding in kind, since North Korea has little for either U.S. or South Korean cyber warriors to attack. In 2002, Donald Rumsfeld and other Bush Administration officials advocated the invasion of Iraq because Afghanistan was not a “target-rich” environment, with not enough military hardware, bases, or major infrastructure for the U.S. to blow up. North Korea is the cyber equivalent of Afghanistan.

Nightearth.com compiled satellite photos of the planet at night taken from space. Its composite map shows a well-lit planet. South Korea looks like a bright island separated from China and Japan by the sea. What looks like the sea, the Korean peninsula north of Seoul, is almost completely dark. North Korea barely has an electric grid. Fewer than 20,000 of North Korea’s 23 million citizens have cell phones. Radios and TVs are hardwired to tune only into official government channels. And as far as the Internet is concerned, the New York Times’s judgment from 2006 that North Korea is a “black hole” still stands. The Economist described the country as “almost as cut off from the virtual world as it is from the real one.” North Korea operates about thirty websites for external communication with the rest of the world, mostly to spread propaganda about its neighbor to the south. A handful of Western hotels are permitted satellite access, and North Korea does run a limited internal network for a few lucky citizens who can go to the Dear One’s website, but almost nowhere else.

While North Korea may not have invested much in developing an Internet infrastructure, it has invested in taking down the infrastructure in other countries. Unit 110, the unit suspected of carrying out the July cyber attacks, is only one of North Korea’s four cyber warfare units. The Korean People’s Army (KPA) Joint Chiefs Cyber Warfare Unit 121 has over 600 hackers. The Enemy Secret Department Cyber Psychological Warfare Unit 204 has 100 hackers and specializes in cyber elements of information warfare. The Central Party’s Investigations Department Unit 35 is a smaller but highly capable cyber unit with both internal security functions and external offensive cyber capabilities. Unit 121 is by far the largest and, according to one former hacker who defected in 2004, the best trained. The unit specializes in disabling South Korea’s military command, control, and communications networks. It has elements stationed in China because the Internet connections in North Korea are so few and so easily identified. Whether the Beijing government knows the full extent of the North Korean presence and activity is unclear, but
few things escape China's secret police, particularly on the Internet. One North Korean cyber war unit is reportedly located at the Shanghai Hotel in the Chinese town of Dandong, on the North Korean border. Four floors are allegedly rented out to Unit 110 agents. Another unit is in the town of Sunyang, where North Korean agents have reportedly rented out several floors in the Myohyang Hotel. Agents have apparently been spotted moving fiber-optic cables and state-of-the-art computer network equipment into these properties.

All told, North Korea may have from 600 to 1,000 KPA cyber warfare agents acting in cells in the PRC, under a commander with the rank of Lieutenant Colonel. North Korea selects elite students at the elementary-school level to be groomed as future hackers. These students are trained on programming and computer hardware in middle and high school, after which they automatically enroll at the Command Automation University in Pyongyang, where their sole academic focus is to learn how to hack into enemy network systems. Currently 700 students are reportedly enrolled. They conduct regular cyber warfare simulated exercises against each other, and some infiltrate Japan to learn the latest computer skills.

The July 2009 attack, though not devastating, was fairly sophisticated. The fact that it was controlled and not simply released to do damage indiscriminately shows that the attackers knew what they were doing. The fact that it lasted for so many days is also a testament to the effort put into propagating the virus from several sources. These attributes suggest that the attack was not the work of some teenagers with too much time on their hands. Of course, North Korea sought "deniability," creating sufficient doubt about who did the attack so that they could claim it was not them.

While researchers have found that part of the program was written using a Korean-language web browser, that would just as likely implicate South Korean hackers for hire, of which there are many in that highly wired nation. These same researchers, however, are troubled by the fact that the code writer didn't try to disguise its Korean origin. Someone sophisticated enough to write the code should also have been sophisticated enough to cover his or her tracks. Perhaps whoever ordered the code written wanted that clue to be found.

The South Korean government and many analysts in the United States concluded that the person who ordered the attack was the Dear One, and that he had demonstrated North Korea's strength in cyberspace at the same time that he had done so with the rocket barrage. The message was: I am still in charge and I can make trouble with weapons that can eliminate your conventional superiority. Having sent that message, a few weeks later North Korean diplomats offered an alternative. They were prepared to talk, even to free two American prisoners. Shortly thereafter, in a scene reminiscent of the movie *Team America: World Police*, Bill Clinton was sitting down with the Dear One. Unlike the marionette portraying UN nuclear inspector Hans Blix in the movie, Clinton did not drop through a trapdoor into a shark tank, but it seemed likely that North Korea had placed trapdoors on computer networks on at least two continents.

Months after the July 2009 North Korean cyber activity, Pentagon analysts concluded that the purpose of the DDOS attacks may have been to determine what level of botnet activity from South Korea would be sufficient to jam the fiber-optic cables and routers leading out of the country. If North Korean agents in South Korea could flood the connection, they could effectively cut the country off from any Internet connection to the rest of the world. That would be valuable for the North to do in a crisis, because the U.S. employs those connections to coordinate the logistics of any U.S. military reinforcements. The North Korean preparation of the cyber battlefield continued. In October, three months after the DDOS attacks, South Korean media outlets reported that hackers had infiltrated the Chemicals Accident Response Information System and had withdrawn a significant amount of classified information on 1,350
hazardous chemicals. The hackers, believed to be North Koreans, obtained access to the system through malicious code implanted in the computer of a South Korean army officer. It took seven months for the South Koreans to discover the hack. North Korea now knows how and where South Korea stores its hazardous gases, including chlorine used for water purification. When chlorine is released into the atmosphere, it can cause death by asphyxiation, as demonstrated horribly on the battlefields of World War I.

The new “cyber warriors” and much of the media herald these incidents as the first public clashes of nation-states in cyberspace. There are other examples, including operations by China, Taiwan, Israel, and others. Some have called the Estonian case “WWI,” that is, Web War One.

Others look at these and other recent incidents and do not see a new kind of warfare. They see in the Israeli attack a new form of airborne electronic jamming, something that has been happening in other ways for almost half a century. The American actions in Iraq appear to these doubters to be marginal and mainly propaganda. In the Russian and North Korean activities the doubters see only harassment and nuisance-value disruption.

Of course, the Syrians, Iraqis, Estonians, Georgians, and South Koreans saw these events as far more than a nuisance. I tend to agree. I have walked through these recent, well-known cyber clashes mainly to demonstrate that nation-state conflict involving cyber attacks has begun. Beyond that incontestable observation, however, there are five “take-aways” from these incidents:

**Cyber war is real.** What we have seen so far is far from indicative of what can be done. Most of these well-known skirmishes in cyberspace used only primitive cyber weapons (with the notable exception of the Israeli operation). It is a reasonable guess that the attackers did not want to reveal their more sophisticated capabilities, yet. What the United States and other nations are capable of doing in a cyber war could devastate a modern nation.

**Cyber war happens at the speed of light.** As the photons of the attack packets stream down fiber-optic cable, the time between the launch of an attack and its effect is barely measurable, thus creating risks for crisis decision makers.

**Cyber war is global.** In any conflict, cyber attacks rapidly go global, as covertly acquired or hacked computers and servers throughout the world are kicked into service. Many nations are quickly drawn in. **Cyber war skips the battlefield.** Systems that people rely upon, from banks to air defense radars, are accessible from cyberspace and can be quickly taken over or knocked out without first defeating a country’s traditional defenses.

**Cyber war has begun.** In anticipation of hostilities, nations are already “preparing the battlefield.” They are hacking into each other’s networks and infrastructures, laying in trapdoors and logic bombs—now, in peacetime. This ongoing nature of cyber war, the blurring of peace and war, adds a dangerous new dimension of instability.

As later chapters will discuss, there is every reason to believe that most future kinetic wars will be accompanied by cyber war, and that other cyber wars will be conducted as “stand-alone” activities, without explosions, infantry, airpower, and navies. There has not yet, however, been a full-scale cyber war in which the leading na-
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.