Focus: What Was Stuxnet?

Ralph Langner is a jovial fellow with a quick wit, whose sense of whimsy is perhaps best illustrated by the fact that he wears cowboy boots. Wearing cowboy boots shouldn't be all that notable, until one realizes that Ralph is not from Texas, but Germany, and is not a cowboy, but a computer specialist. Langner is also incredibly inquisitive.

It was this combination that led him to play a role in the discovery of one of the most notable weapons in history; and not just cyber history, but history overall.

Since 1988, Ralph and his team of security experts had been advising on the safety of large-scale installations. Their special focus was industrial control systems, the computer systems like SCADA (short for "supervisory control and data acquisition") that monitor and run industrial processes. SCADA is used in everything from the management and operation of power plants to the manufacture of candy wrappers.

In 2010, like many other industrial control experts, Ralph grew concerned about a cyber "worm" of unknown origin that was spreading across the world and embedding itself in these control systems. Thousands of computers in places like India and the United States had been infected. But the bulk of the infections (roughly 60 percent) were in Iran. This led many experts to infer that either Iran had particularly poor cyber defenses for its SCADA-related programs, which made it more vulnerable, or a virus had initially targeted some site in Iran and, as one report put it, "subsequently failed in its primary purpose and run amok, spreading uncontrollably to unintended targets all over the world, and thus demonstrating how indiscriminate and destructive cyber weapons were likely to be."

Both turned out to be far from the case. Curious, Ralph began to dissect the code of "Stuxnet," as it became known. The more he and his team explored it, the more interested they became. It was a wonderfully complex piece of malware like none the world had ever seen. It had at least four new "zero days" (previously unknown vulnerabilities), utilized digital signatures with the private keys of two certificates stolen from separate well-known companies, and worked on all Windows operating systems down to the decade-old Windows 95 edition. The number of new zero days particularly stood out. Hackers prize zero days and don't like to reveal them when they don't have to. To use four at once was unprecedented and almost illogical given that one new open door is enough. It was a pretty good sign that Stuxnet's makers had enormous resources and wanted to be absolutely certain they would penetrate their target.

Stuxnet also slipped by the Windows' defenses using the equivalent of a stolen passport. To gain access to the "kernel," or operating system's control system, Stuxnet had to install a component

that could talk to the kernel. The authors chose a "device driver," a common tool that allows hardware devices to interact with the operating system. Windows uses a scheme of digital signatures to allow trusted hardware manufacturers to write device drivers that are trusted by the operating system. Unsigned drivers raise an alert for the user, while signed drivers do not. The drivers in Stuxnet were signed by two real companies in Taiwan, indicating that the authors had access to the secret signing keys—most likely stolen. Again, this is a rare style of attack: stolen signing keys are incredibly powerful, would have been well protected, and would be very valuable in any illicit market.

The malware's DNA revealed something even more interesting: Rather than being truly infectious, Stuxnet was hunting for something in particular. As Langner delved deeper, he discovered that Stuxnet was not going after computers or even Windows software in general, but a specific type of program used in Siemens's WinCC/PCS 7 SCADA control software. Indeed, if this software wasn't present, the worm had built-in controls to become inert. In addition, rather than trying to spread as widely as possible, as was the goal with past worms, Stuxnet only allowed each infected computer to spread the worm to no more than three others. It even came with a final safeguard; a self-destruct mechanism caused it to erase itself in 2012. Ralph realized that whoever made Stuxnet not only had a specific target in mind, but didn't want the code lingering in the wild forever. This was a very different worm, indeed.

But what was the target? This was the true mystery. Here Langner's background in working with industrial firms proved particularly useful. He figured out that Stuxnet was only going after a specific industrial controller, manufactured by Siemens, configured to run a series of nuclear centrifuges—but not just any old nuclear centrifuges you might have lying around the house, only a "cascade" of centrifuges of a certain size and number (984) linked together. Not so coincidentally, this was the exact setup at the Natanz nuclear facility, a suspected site in Iran's illicit nuclear weapons program.

Things got especially tricky once Stuxnet found its way into this target (it was later revealed that the delivery mechanism was infiltration through Iranian nuclear scientists' own laptops and memory sticks). Langner discovered that the cyberattack didn't shut down the centrifuges in any obvious manner. Instead, it ran a series of

subroutines. One, known as a "man in the middle," caused tiny adjustments in pressure inside the centrifuges. Another manipulated the speed of the centrifuges' spinning rotors, causing them to alternately slow down and then speed back up, throwing the rotors out of whack and ruining their work. On top of this, every so often the malware would push the centrifuge speeds past the designed maximum. So the centrifuges weren't just failing to produce refined uranium fuel, they were frequently breaking down and grinding to a halt from the damaging vibrations that the various random surges caused. At other times, the machines were literally spinning out of control and exploding.

The effect, Langner wrote, was "as good as using explosives" against the facility. In fact, it was better. The victim had "no clue of being under a cyber attack." For over a year, Stuxnet had been inside Iranian networks, but the nuclear scientists initially thought their facility was just suffering from a series of random breakdowns. The scientists just kept replacing the broken centrifuges with new ones, which would then get infected and break again. Soon, though, they wondered whether they were being sold faulty parts or were suffering from some kind of hardware sabotage. But the machines checked out perfectly every time, except for the fact that nothing was working the way it should.

This was perhaps the most insidious part of Stuxnet: it was an integrity attack par excellence. Stuxnet didn't just corrupt the process, it hid its effects from the operators and exploited their trust that the computer systems would accurately and honestly describe what was taking place. Iranian engineers didn't even suspect a cyberattack; their systems were air-gapped from the Web, and up to this point worms and viruses had always had an obvious effect on the computer, not the hardware. Eventually, the Iranian scientists suffered low morale, under the impression that they couldn't do anything right; seventy years earlier a bunch of Americans had built an atomic bomb using slide rulers, and they couldn't even get their modern-day centrifuges to work. Overall, Langner likened the Stuxnet effect to the cyber version of "Chinese water torture."

When Ralph Langer revealed his findings on his blog, the little-known German researcher quickly became an international celebrity. First, he had exposed a top-secret campaign of sabotage (later leaked to have been a collaborative effort between US and

Israeli intelligence agencies, known as "Olympic Games"), and second, it was a find of global importance. A new kind of weapon long speculated about but never seen, a specially designed cyber weapon, had finally been used.

at Is the Hidden Lesson of Stuxnet? The Ethics of Cyberweapons

musket of cyberwarfare. What will be its rifle? Its AK-47? Its omb?"

Donath of Harvard University described Stuxnet as a dem- f a new kind of weapon that could only get better. But d that these better weapons would promote a new on and global risk. "Stuxnet was the absolute game yber thinker Mikko Hypponen. "We are entering countries start stocking weapons, only it isn't eactors they're stocking, but it's cyberweap- orry that not enough people took notice of r we will all lose," says Leslie Harris of the Technology.

ings, perhaps, but it was also notable ittle worm was a superb illustration

networks. But what really stands out compared to traditional weapons is how small its physical impact was, especially compared to the intense stakes. The target was a nuclear bomb-making program, one that had already been targeted by diplomatic efforts and economic sanctions. While it's certainly arguable whether preemptive action against the Iranian program is justifiable, this is when the question of proportionality becomes relevant. Stuxnet broke nothing other than the nuclear centrifuges that had been illegally obtained by Iran to conduct illicit research. Moreover, it neither hurt nor killed anyone. By comparison, when Israel attempted to obstruct Iraqi nuclear research in 1981, its forces dropped sixteen 2,000-pound bombs on a research site during "Operation Opera," leveling it and killing eleven soldiers and civilians.

But discrimination also matters when judging the ethics of these attacks. At face value, Stuxnet would seem to have been incredibly indiscriminant. While limited in its promiscuity compared to prior malware, this was a worm that still got around. It infected not just targets in Iran but thousands of computers across the world that had nothing to do with Iran or nuclear research. Many lawyers see this fact of cyber weapons as proof of their inherent violation of "prevailing codes of international laws of conflict, as they go beyond just the original target and deliberately target civilian personnel and infrastructure."

While Stuxnet lacked discretion under the old way of thinking, its very design prevented harm to anyone and anything beyond the intended target. This kind of discrimination was something never previously possible in a weapon. As George Lucas, a philosopher at the US Naval Academy, wrote in an assessment of Stuxnet's ethics, "you happen to be running a large array of exactly 984 Siemens simultaneously, you have nothing to fear from this worm." Ultimately, the ethics of Stuxnet and cyber weapons more generally are a part of the story you care about most. Do you care about the kind of weapon permitted a precedent with Iran or nuclear research? Or thousands of people and collateral damage

History may render the ultimate judgment of Stuxnet, however. As Ralph Langner put it, the fascinating new weapon he discovered "could be considered a textbook example of a 'just war' approach. It didn't kill anyone. That's a good thing. But I am afraid this is only a short-term view. In the long run it has opened Pandora's box."

"Cyberwar, Ugh, What Are Zeros and Ones Good For?": Defining Cyberwar

"Be it resolved by the Senate and House of Representatives of the United States of America in Congress assembled, that the state of war between the United States and the Government of Bulgaria, which has thus been thrust upon the United States, is hereby formally declared."

This June 5, 1942, text describes the last time the United States actually declared war. The declaration covered the minor Axis powers, who were feeling left out after the first post–Pearl Harbor vote to go to war against Nazi Germany, Japan, and Italy. In the years since, America has sent troops to Korea and Iraq and launched airstrikes into places like Yugoslavia, Cambodia, and Pakistan, but the United States has not formally declared war on another state. Wars have been declared on various other things, however: President Johnson's 1964 "Nationwide War on the Sources of Poverty"; Nixon's 1969 "War on Drugs"; and what some conservative leaders more recently claim is a secret "War on Christmas."

The disconnect between an actual state of war and the far more frequent uses and misuses of the concept of "war" is important to keep in mind when discussing a term like "cyberwar." War is used to describe an enormously diverse set of conditions and behaviors, from a state of armed conflict between nations (World War II) to symbolic contestations (New York City's "war on sugar"). As for "cyberwar," the term has been used to describe everything from a campaign of cyber vandalism and disruption (the "Russian Estonian cyberwar," as it is too often called) to an actual state of warfare utilizing cyber means. Indeed, in 2010 *The Economist* ran a cover story on cyberwar that portrayed it as everything from military conflict to credit card fraud.

Defining cyberwar need not be so complicated. The key elements of war in cyberspace all have their parallels and connections to warfare in other domains (the real kind, not the symbolic "war between the sexes" kind). Whether it be war on land, at sea, or in the air, or now in cyberspace, war always has a political goal and mode (which distinguishes it from crime) and always has an element of violence. Currently, the US government's position is that to meet this definition of the use of force, a cyberattack would have to "proximately result in death, injury or significant destruction." That is, even if conducted through cyber means, the effect must be physical damage or destruction. To provide a parallel, a plane dropping bombs is engaged in air warfare; a plane dropping leaflets, not so much.

Knowing when cyberwar begins or ends, however, might be more challenging than defining it. Most wars don't actually have the clear start and negotiated ends that World War II had. Instead, their starts and ends blur. For instance, the United States may not have formally declared war on North Korea in 1950, but it's hard to argue that a conflict in which 5.3 million perished was just a "police action," as President Truman called it at the time. In turn, while the Korean War, as the history books record it, has never formally ended with a peace treaty, the actual fighting ceased in 1953.

Cyberwar's lines can be just as fuzzy. "We in the US tend to think of war and peace as an on-off toggle switch—either at full-scale war or enjoying peace," says Joel Brenner, former head of counterintelligence under the US Director of National Intelligence. "The reality is different. We are now in a constant state of conflict among nations that rarely gets to open warfare.... What we have to get used to is that even countries like China, with which we are certainly not at war, are in intensive cyberconflict with us."

This may be where cyberwar has more in common with more informal concepts of conflict like the Cold War, during which constant conflict didn't actually result in direct, open violence. Indeed, the editor of *Foreign Policy* magazine, David Rothkopf, has argued we may be entering the era of the "cool war," not only because of the remote nature of the attacks but because "it can be conducted indefinitely—permanently, even—without triggering a shooting war. At least, that is the theory."

A War by Any Other Name? The Legal Side of Cyber Conflict

"The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all."

This sentence opens Article 5 of the Washington Treaty, which in 1949 established the North Atlantic Treaty Organization, or NATO. It is one of the most important passages ever written in international politics. These simple words outlined the concept of "collective defense," which created the most successful alliance in history. This "All for one, one for all" approach to sharing risk and response allowed the United States and its allies to stand together, taking them from the start of the Cold War to the fall of the Berlin Wall and beyond, including their collective response to the 9/11 attacks on the United States and subsequent deployment half a world away to Afghanistan.

But in April 2007, NATO and its collective defense ideals faced a twenty-first-century test. A new alliance member, Estonia, was one of Europe's most wired states. The majority of its citizens conducted everything from their banking to their voting online. Suddenly, Estonian banks, media web pages, and government websites were hit with a large-scale denial of service attack. While the attack resulted from a series of botnets that had captured over a million computers in seventy-five countries, as we read about earlier, Estonia quickly pointed the finger at its neighbor Russia, with whom it was embroiled in a political dispute over the move of a statue honoring Russian soldiers from World War II. Estonia's foreign minister called for help, believing that the massive cyberattack threatened its security and hence the alliance's as a whole. It argued that under the Washington Treaty NATO was obliged to defend against this start of a new "cyberwar."

While they were concerned about the attacks, however, the other members of NATO didn't think Article 5 applied. Estonia was being bullied in cyberspace, but no one was dead or hurt and no property was actually destroyed or damaged. It didn't look like the start of a war, at least as NATO understood it, and certainly wasn't worth the alliance risking an actual war with Russia. Instead, the defense ministers of NATO waited a few weeks to issue a joint statement deploring the cyberattacks and sent technical experts to aid Estonia in unblocking its networks. Amusingly, while NATO's political

leaders judged that the cyberattacks were not an act of war, NATO's Department of Public Diplomacy later created a short film about the episode entitled *War in Cyberspace*.

The Estonia case is instructive because it shows the back and forth that takes place between old laws and new technologies, especially when it comes to the question of what constitutes an act of war in the cyber realm. Much of today's thinking on the laws and statecraft of war dates to the post–World War II 1945 UN Charter and 1949 Geneva Conventions. The challenge is that concepts developed back when computers used punch cards don't necessarily apply as clearly to the cyber realm.

In international law, for instance, an "aggression" that would justify going to war is described by the UN Charter as a "use of force against the territorial integrity . . . of a state." The problem is that this assumes only a physical world of clearly demarcated borders. This was perfectly acceptable back in 1945 but not in the contemporary world; cyberattacks don't use physical force, take place in a geographic realm, nor necessarily involve only states.

That old laws are growing more challenging to apply doesn't mean, however, that the cyber world is the Wild West. There are nascent efforts to either update the old codes or create new ones. For example, after the confusion over the Estonia incident, the NATO Cooperative Cyber Defence Centre of Excellence commissioned twenty law professors to formally examine how the known laws of war apply to cyberspace, in a document entitled the "Tallinn Manual on the International Law Applicable to Cyber Warfare." The manual laid out their ideas on everything from what self-defense might mean in the cyber world to a controversial (but logical) argument that any civilian fighting in a cyberwar loses legal protections as a civilian. While an important effort, it has no legal standing, and obviously a number of nations outside of NATO, such as Russia, were less than enthusiastic about the manual's findings. Even more, certain NATO members like the United States were not quick to embrace the manual they had sponsored.

The reality is that the "process of formalizing rules for cyberspace will likely take decades given the differing priorities among various governments," reports *Foreign Policy* magazine. This seems to leave a massive vacuum in the interim. So until the old treaties are updated or new ones are accepted for the cyber world, there is

a third option: apply existing laws' basic principles and values to cyberspace. Charles Dunlap, a military lawyer who retired as a US Air Force major general and now teaches at Duke University Law School, notes, "A cyber attack is governed by basically the same rules as any other kind of attack."

The primary way to determine when a cyberattack constitutes the kind of "use of force" that legally justifies war is to weigh its effects. What did the act do to the real world, regardless of the fact that it happened via cyber means? Look to the amount of damage, caused or intended, and establish parallels.

Focusing on impact is important because it recognizes that not all attacks have to involve traditional armed violence. Indeed, in international law an enemy that uses unarmed means to intentionally divert a river to flood a neighboring state or set fires to burn wildly across the border would still be committing an armed act of aggression equivalent to the use of guns for the same effect.

The same logic applies in reverse. You wouldn't go to war if someone defaced your posters in the street, so neither should a government if an enemy defaces its websites. By comparison, when the action causes death and destruction, the discussion moves into the realm of war. If your power plant explodes in a fiery blast that kills thousands, whether the cause was an actual bomb or logic bomb is not a major distinguishing factor.

The real challenge is the gray area in the middle, incidents between destruction and disruption, such as a denial-of-service attack. When it was under attack, Estonia wanted NATO to declare that its sovereignty had been violated, which would have triggered the collective self-defense article of the NATO treaty. In the virtual world perhaps it had been, but not in the physical world. Here again, even these seemingly new forms of attack have parallels to guide us. While they may not have imagined cyberspace, the 1940s-era statesmen who wrote the UN Charter did imagine things like the interruption of "postal, telegraphic, radio, and other means of communications." Such interruptions were certainly frowned upon, but they did not constitute war. Professor James Hendler, former chief scientist at the Pentagon's Defense Advanced Research Projects Agency (DARPA), says that in the case of Estonia, the attacks were "more like a cyber riot than a military attack." It was disruptive, but it wasn't war.

Another example in Estonia's neighborhood serves as illustration. In 2008, the nation of Georgia also got in a dispute with its larger neighbor. Just as in Estonia, Georgian websites suffered denial-of-service attacks, as we saw earlier, thought to have been coordinated by Russian sources. The attacks crippled the websites' operations for several days and limited the Georgian government's ability to communicate with its people and the outside world. At the same time, several brigades of Russian tanks crossed into Georgia, and Russian bombers and missiles pummeled the country, causing over 1,300 casualties. The difference in impact was stark. The cyberattacks alone were not war, but a war was clearly taking place.

The severity of the attack is not the only thing to keep in mind. There are all sorts of actions that could ultimately spark a chain of events that cause the same death and destruction as real war. A young boy drops a banana, upon which a diplomat slips. The diplomat goes to the hospital instead of peace talks. The peace talks consequently fail and war breaks out. We can conceptualize how the boy's action helped lead to war, but was his dropping the banana an act of war? Of course not; the invasion was the action that mattered when looking to judge how the war actually started. Cause is not the same as effect.

This points to the second key determinant of when a cyberattack becomes an act of war: directness and measurability. There must be some fairly direct and intended link between cause and effect. This factor is often applied to distinguish acts of espionage from acts of war. The theft of government secrets could certainly lead to soldiers losing their lives one day by revealing to the enemy, for instance, how a plane operates or the location of a secret base. But it is only if and when the war starts that this theft could ever have that impact. This indirectness is why nations have traditionally not gone to war over acts of espionage, be they physical or increasingly now virtual. No one likes to be the victim of espionage, to be sure. But spying is cast more as part of the rough game of statecraft that nations play rather than the all-out breaking of international rules that starts real wars.

An important part of these discussions, however, is often forgotten. While we'd like to think that law is the guide to our behavior, clearly delineating when a cyberattack escalates into war is not just an issue of law or just for the lawyers to decide. As the great

philosopher of war Carl von Clausewitz wrote, "War is not an independent phenomenon, but the continuation of politics by different means." War is political. And by being political, it is also always interactive. That is, there are sides to the war, each with their own goals, actions, and responses, each trying to bend the other to its will.

This fundamentally political nature of war means that all of these questions on when a cyberattack reaches the realm of war will come down to making tough political decisions, in what Clausewitz would see as a digital version of his famous "fog of war," the messy, fast-moving, unclear circumstances that always accompany war. Ultimately, cyberwar is what we in the real world believe it to be. "At the end of the day, it's the President who gets to decide if this is war or something else," explains Jim Lewis, a senior fellow at the Center for Strategic and International Studies. "The standard is ambiguous. Deciding when something is an act of war is not automatic. It's always a judgment."

What Might a "Cyberwar" Actually Look Like?
Computer Network Operations

Like so many stories in the world of cybersecurity, Operation Orchard began with simple human carelessness. In 2006, a senior official in the Syrian government left his laptop computer in his hotel room while visiting London. When he went out, agents from Mossad, the Israeli intelligence agency, snuck into his room and installed a Trojan horse onto the laptop to allow them to monitor his communications. That was bad enough for the Syrians.

But one man's poor computer security turned out to have more significant consequences when the Israelis began to examine the files that the official had stored on the laptop's hard drive, including pictures. One photo in particular caught the Israelis' attention. It showed an Asian man in a blue tracksuit standing next to an Arab man in the middle of the Syrian desert. It could have been innocuous, but then Mossad identified the two men as Chon Chibu, a leader of the North Korean nuclear program, and Ibrahim Othman, director of the Syrian Atomic Energy Commission. Combined with other documents lifted from the hard drive, such as construction plans and photos of a type of pipe used for work on fissile materiel, the Israelis realized the laptop was an atomic alarm bell. The Syrians

were secretly constructing a facility at al Kibar to process plutonium, a key step in the assembly of a nuclear bomb, with aid from North Korea (an International Atomic Energy Agency investigation would later confirm the Israeli suspicions).

This news led to Operation Orchard, the next key part of the cyber story. Just after midnight on September 6, 2007, seven Israeli F-15I fighter jets crossed into Syrian airspace. They flew deep into the Syrian interior and dropped several bombs, leveling the Kibar complex depicted in the photos. The whole time the planes were in Syrian airspace, the air defense network never fired a shot.

Reportedly, the Syrian defense didn't even detect the jets, meaning they didn't even know they were under attack until the bombs started to go off. Yet Syrian radar officers hadn't all turned traitor that night. Rather, their technology had. If initially planting the Trojan horse into the Syrian officials laptop had been about finding secret information via cyber means, this was its cousin, a cyber operation with a military outcome. The Israelis had successfully penetrated the Syrian military's computer networks, allowing them to see what the Syrians were doing as well as direct their own data streams into the air defense network. This caused the Syrian radar operators to see a false image of what was really happening as the Israeli jets flew across the border. By effectively turning off the Syrian air defenses for the night, the Israelis not only got to their target without any losses, but they also did so with a much smaller force.

Orchard is a great illustration of the concepts behind "computer network operations," as such military cyberattack operations are dubbed. While much is shrouded in secrecy about the rise of such operations, one of the first known US military exercises in this space was "Eligible Receiver," a test of computer network operations in 1997. In many ways it was akin to the Fleet Problems of the 1920s, when the US Navy first experimented with aircraft carriers, or the Louisiana Maneuvers of 1940, when the US Army evaluated mechanized tank forces. After a small "red team" of computer experts gained access to the computers at the US Pacific Command's headquarters as well as the 911 emergency phone systems in nine US cities, the Pentagon decided that, just as with the airplane or the tank, the time had arrived for computers to play a part in military operations. Indeed, the naysayers were hushed the very next year when

hackers compromised over five hundred Pentagon computers in an incident that became known as "Solar Sunrise."

Today, the vast majority of the world's militaries have some sort of planning or organization in place for cyber warfare. These plans can be thought of as the "Five D's plus One." The US Air Force describes cyberwar as the ability "to destroy, deny, degrade, disrupt, [and] deceive," while at the same time "defending" against the enemy's use of cyberspace for the very same purpose.

Such military programs range from focused infiltrations and raids like Israel's Operation Orchard to broader efforts like the US military's "Plan X," a $110 million program designed to "help warplanners assemble and launch online strikes in a hurry and make cyber attacks a more routine part of U.S. military operations." But across the world, what the *New York Times* called "a new type of warfare" actually has much in common with war as it has always been conducted. The computer used as a military weapon is just a tool. Just as with the spear, the airplane, or the tank, it simply aids in achieving the goals that are part of any military operation.

Before battle begins, a smart commander engages in what is known as "intelligence preparation of the battlefield." Much as Allied efforts to crack Axis radio codes proved crucial to victory in World War II, intercepted digital communications can be just as critical today. As the Israelis did in Orchard, this part of cyber warfare is about deploying one's digital weapons even before the battle has begun, infiltrating networks, gathering information, and potentially even laying the groundwork for more aggressive action. For example, some of the information inside US military computers suspected to have been targeted by Chinese military hackers includes unit deployment schedules, resupply rates, materiel movement schedules, readiness assessments, maritime prepositioning plans, air tasking for aerial refueling, and "the logistics status of American bases in Western Pacific theater." This kind of data might prove useful if war ever broke out. And, as the 2013 Snowden leaks showed, US cyber warriors are gathering the same information about their potential adversaries in China and elsewhere.

But the difference between current cyber efforts and past intelligence collection programs is how computer network operations also allow aggressive actions inside the enemy's communications once the shooting has begun. It's the difference between reading the

enemy's radio signals and being able to seize control of the radio itself.

The modern military is what some folks call "network-centric," utilizing computers bound together in a "system of systems" to coordinate across great distances with digital speed. But these advantages can create vulnerabilities. If you can compromise an enemy's networked communications, you move from knowing what they're doing, which is advantage enough, to potentially changing what they're doing.

Inside a foe's communications networks, one can disrupt or even disable command and control, keeping commanders from sending out orders, units from talking to each other, or even individual weapons systems from sharing needed information. In one example, over one hundred American defense systems, from aircraft carriers to individual missiles, rely on the Global Positioning System (GPS) to locate themselves during operations. In 2010, an accidental software glitch knocked 10,000 of the military's GPS receivers offline for over two weeks, including the US Navy's X-47 prototype robotic fighter jet. Cyber warfare would, in effect, make such software glitches deliberate.

Alternatively, the attack might not try to disable or jam these communications but instead attack the information within them, feeding the enemy false reports via its own devices. "Information warfare" is how the military has traditionally described operations that try get inside the enemy's mind and influence decision-making. Now the idea is to use modern information technologies to the same ends. The objectives might be highly strategic, such as false commands from top leaders, to more tactical insertions along the lines of what the Israelis did in Orchard, compromising individual weapons systems and their sensors.

One of the more interesting potential effects of such attacks is how success might be multiplied by the impact on the minds of the users of the networks under attack. Only a relatively small percentage of attacks would have to be successful in order to plant seeds of doubt in any information coming from a computer. Users' doubt would lead them to question and double-check everything from their orders to directions. This illustrates again the notion of trust, which was so important in Part I. The impact could even go beyond the initial disruption. It could erode the trust in the very networks needed by modern military units to work together effectively;

it could even lead some militaries to abandon networked computers for anything important and set their capacity back decades.

Such technological abstinence sounds extreme, especially when computers have proven so useful in modern war. But imagine if you had a memo that you needed to get to your boss with absolutely no mistakes, at the risk of losing your job. Would you e-mail it if there were a 50 percent risk of it somehow being lost or changed en route? Or would you just hand-deliver it? What about if the risk were 10 percent? How about just 1 percent, but still at the risk of losing your job? Then apply the same risk tolerances when it's your life in battle rather than your job. How do your risk numbers change?

Computer network operations, though, won't just be limited to targeting command and control with indirect effects. As more and more unmanned systems are introduced into warfare (the US military has over 8,000 "drones" like the famous Predator and Reaper, while over eighty countries now have military robotics programs), targeting command-and-control networks opens up even more direct avenues of attack. These robotic weapons systems all link into computer networks, providing everything from GPS location to remotely controlled operations. Here again, the very same networking that allows drones to strike targets with precision thousands of miles away also opens up new possibilities of disruption and even co-option. What we enter is an era of "battles of persuasion."

One could never co-opt the flight of a bullet, steering it away from where the gunner shot it. Nor has anyone proven able to brainwash a bomber pilot in midair and shift his allegiance. But if the computers on robotic weapons systems are compromised, they could be "persuaded" to do the opposite of what their owners intended. This creates a whole new type of combat, where the goal may not be merely to destroy the enemy's tanks but to hack into his computer networks and make his tanks drive around in circles or even attack each other.

And, of course, cyberwar might see computers used in the same way that other weapons have been used to cause destruction and loss of life among enemy forces. As opposed to traditional kinetic attacks (a blade, a bullet, an explosion), these would involve more destruction through indirect means. Many military systems like ship engines operate under SCADA programs, meaning that they can be targeted in much the same way that the Stuxnet virus caused Iranian

centrifuges to spin out of control. In 2009, for instance, an employee at the Shushenskaya dam in Siberia accidentally turned on an unused turbine with a few mistaken keystrokes, leading to the release of a massive "water hammer" that destroyed the plant and killed seventy-five people. This is the computer software version of how allied planes in World War II and Korea dropped bombs on dams, using the ensuing wave to destroy enemy targets in the flood's path.

As in traditional war, though, what sounds easy in description can prove hard in execution. This is not just due to the complexity of target systems and the operations needed to exploit them, but because every war, even in cyberspace, has at least two sides. Every potential operation meant to attack and defeat a foe would be met by the opponent's efforts to keep the enemy out or threats of an equivalent attack to make the aggressor think twice about conducting it.

These difficulties drive adversaries to instead go after "soft targets," as has long been the case in traditional modes of war. In theory, war is only a contest among warriors. In reality, well over 90 percent of the casualties in the last decades of war have been civilians. Unfortunately, one can expect the same dynamic in cyberwar.

The more conventional type of civilian targeting in computer network operations would attack civilian networks and operators viewed as directly or indirectly supporting the military enterprise. These range from civilian contractors, who provide much of the supply and logistics support to modern militaries (about half of the American force in places like Afghanistan and Iraq were actually private contractors), to the infrastructure that the military relies on for its operation, such as ports and railroads. Of note, the computer networks that these civilian forces rely upon often don't have the same levels of security as military networks because they lack similar resources, standards, and incentives. The result is they make particularly choice targets. In one 2012 Pentagon-sponsored war game we participated in, a simulated enemy force hacked the contractor company supplying the logistics of a US force, with the simple purpose of transposing the barcodes on shipping containers. It seems a minor change with little impact. But had it been a real attack, US troops in the field would have opened up a shipping pallet expecting to find ammunition and instead only found toilet paper.

The history of warfare shows that it's not just those who directly support the military who might cross the cyber firing line. When

new technologies like the airplane expanded forces' reach beyond the front lines, militaries gradually expanded who they defined as a legitimate target. First, it was only those working directly for the military. Then it was those engaged in the war effort, such as workers at a tank factory. Then it was the workers' houses. And by the end of World War II, all the sides had engaged in strategic bombing against the broader populace, arguing that the best way to end the war was to drive home its costs to all civilians. Given civilians' greater vulnerability to cyberattacks, we should expect nothing less as part of any cyberwar. Thanks to the modern military's dependence on civilian networks, they might even make up a new center of gravity to target.

As scary as this all sounds, it's important to note two key differences between war in the cyber realm and other past modes of conflict. First, unlike previous transitions in warfare, cyber is unlikely to immediately multiply the level of destructive power in ways that previous technological innovations did. Because of its reliance on indirect effects, cyber's effects will have less long-term destructive impact. That is, attacks that change GPS codes or shut down the energy grid would be quite devastating. But they would be nowhere near the destruction visited by explosive-filled bombs and incendiaries upon Dresden or the permanent irradiation of Hiroshima.

Second, the weapons and operations in cyberwar will be far less predictable than traditional means, leading to greater suspicion of them among military commanders. For instance, the blast radius of a bomb can be projected to exacting standards; not so the radius of most malware. Most cyberattacks rely on the second- and even third-order effects that might result, and while these widen the impact, they can also have unexpected outcomes. During the Iraq war, for instance, US military officers were very excited by the prospects of taking down an enemy computer network facilitating suicide bombings. But the operation accidentally took down over 300 other servers in the wider Middle East, Europe, and the United States, opening a whole new can of worms. Similarly, Stuxnet was specifically tailored to target just a few Iranian centrifuges and yet ended up spreading to well over 25,000 other computers around the world.

In the end, we are still at the early stages of conceptualizing what cyberwar will look like. Predicting the future of computer network

operations now is akin to those who laid out their visions of air war in the early days of "flying machines" at the turn of the last century. Some of their predictions proved right, like the idea that planes would bomb cities, while others proved woefully wrong, like the prediction that airplanes would render all other forms of war obsolete.

The same is likely to happen with cyberwar. It will prove to be fantastically game-changing, introducing real-world capabilities and operations that once seemed science fiction. But even in a world with digital weaponry, war will still be a chaotic domain. This means that war, even cyber-style, will still remain a waste of resources and efforts better spent elsewhere.

Focus: What Is the US Military Approach to Cyberwar?

Do you know what "9ec4c12949a4f31474f299058ce2b22a" means? If so, the US military may have a job for you.

The answer is actually a wonderful summary of where the US military stands in its approach to cybersecurity. This code appears in the logo of the US military's Cyber Command, a revolutionary new military organization formed in 2010. In cryptography, a hash is a one-way function that creates a unique "fingerprint" of a file. The MD5 (Message-Digest algorithm 5) hash was a widely used way to add security by detecting tampering in files. The code above is the MD5 hash of Cyber Command's mission statement, which reads: "USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks; and prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries." There is an irony, however. The same year Cyber Command put the code on its logo, the US Department of Homeland Security announced that it was moving the US government away from the MD5 hash for its computer systems. The once sophisticated code was now too easy to break.

Cyber Command brings together all components of the US military that work on cyber issues, from the Army's Ninth Signal Command to the Navy's Tenth Fleet (the Fleet Cyber Command). All

told, the organization boasts a cyber warrior force of just under 60,000 personnel, with headquarters located at Fort Meade, Maryland. Its location was deliberate, placing CYBERCOM, as it is known, next door to the National Security Agency, the spy agency that focuses on signals and information intelligence and protection. This allows the two agencies to share resources at the field level, such as the hundreds of PhDs in mathematics, computer science, engineering, and other fields who work there, all the way up to the top. Currently, the director of the NSA and the commander of CYBERCOM is the same person. General Keith Alexander was named the head of both organizations simultaneously, or "double-hatted" in military parlance.

While some see this pairing as natural, given the two entities' close responsibilities, many worry about blurring the lines between a military command and a civilian spy agency. There is a question as to which mentality will prevail: the spy's inclination to watch and learn or the warrior's inclination to act? There is also a worry about one person trying to take on too many different roles at once.

In contrast, others worry that CYBERCOM is not distinct enough, not merely from the NSA but from the military services that source it. Much as the Air Corps was once part of the Army before evolving into its own service (the Air Force) in 1947, some feel that Cyber Command, too, needs to become its own military branch. Two US Army officers have observed that the current military services are "properly positioned to fight kinetic wars, and they value skills such as marksmanship, physical strength, the ability to leap out of airplanes and lead combat units under enemy fire. Unfortunately, these skills are irrelevant in cyber warfare. Technical expertise isn't highly valued in the three services. Just look at military uniforms: no decorations or badges honoring technical expertise."

Regardless, CYBERCOM is growing rapidly in both size and perceived importance inside the US military. Indeed, the Pentagon's 2013 budget plan mentioned "cyber" 53 times. Just a year later, the 2014 budget plan discussed "cyber" 147 times, with spending on CYBERCOM's headquarters alone set to effectively double (all the more notable as the rest of the US military budget was being cut).

The strategy that guides CYBERCOM draws from the overall idea that cyberspace is a new domain of both possibilities and risks, and the US military had better do its utmost to protect its ability to use this domain (its traditional "freedom of maneuver") as well as

preserve the initiative, and prevent others from using it to their full potential (establishing "dominance"). As Lieutenant General Jon Davis, the deputy commander of CYBERCOM, describes, the US military is treating cyber issues with a whole new level of seriousness. "This is now commander's business; this is no longer admin tech business."

The current plan runs over twelve pages in its unclassified version and thirty pages in the classified form. In sum, CYBERCOM focuses on five objectives: treat cyberspace as an "operational domain" as the rest of the military does the ground, air, or sea; implement new security concepts to succeed there; partner with other agencies and private sector; build relationships with international partners; and develop new talent to spur new innovation in how the military might fight and win in this space. As part of this mission, CYBERCOM is to create and lead three types of cyber forces: "cyber protection forces" that will defend the military's own computer networks, regionally aligned "combat mission forces" that will support the mission of troops in the field, and "national mission forces" that will aid in the protection of important infrastructure.

While turning these ideas into an actual working military doctrine, three key concerns have bedeviled CYBERCOM planners. The first is the long-standing question over mission areas and responsibilities. The wider cybersecurity roles that CYBERCOM has taken on have pushed it closer and closer to the civilian sphere, creating a twofold problem. Not only is CYBERCOM continually operating on civilian and government computer networks that it must now seemingly defend, but these responsibilities are frequently competing with others who have a duty to monitor the same networks, including the private sector and other government agencies like the civilian Department of Homeland Security. To make a parallel to the expanded role of "national mission forces," when banks are moving physical money, it isn't the Pentagon that defends the cash, but rather a combination of hired security and the police. But when the cash is virtualized, CYBERCOM has now joined into the discussion.

The second big concern is how far can and should the US military go to maintain the freedom of maneuver it so desires in cyberspace. When the command was first formed, defense leaders like then Deputy Secretary of Defense William Lynn publicly talked about how CYBERCOM would simply busy itself with the "day-to-day

defense and protection of all DOD networks." Within four years, the new roles and strategy pushed well beyond that. As one CYBERCOM official put it, "We need the capabilities to do things offensively in cyber…everybody acknowledges that, but how we specifically employ that in an operational context is classified." Or, as a former National Security Agency watch officer put it, the goal is to ensure that US capabilities remain more advanced than those of potential adversaries. "Whatever the Chinese can do to us, we can do better."

Another strategic question is whether the United States can manage the way threats shift between the cyber domain and the real world and still maintain deterrence in both. It sees the concept of "equivalence" as key to addressing this question. As one report described, "If a cyber attack produces the death, damage, destruction or high-level disruption that a traditional military attack would cause, then it would be a candidate for a 'use of force' consideration, which could merit retaliation."

The idea is to send a message to adversaries that the US military plans to fight and win in cyberspace, but it reserves the right to play a different game if it doesn't like the outcome. Or, as one US military official put it more bluntly, "If you shut down our power grid, maybe we will put a missile down one of your smokestacks."

The central problems this strategy faces are whether cyberspace dominance is achievable and whether deterrence in cyberspace is workable in execution. Such posture requires knowing who your adversaries are, which is exceedingly difficult in cyberspace. As a study on American cyberattack policy and ethics concluded, "Absolute, unambiguous technical proof could be lacking, which forces more reliance on non-technical info than policy makers like."

Additionally, deterrence is not as effective against nonstate groups, which, of course, are major players in cyberspace. Not all are rational actors, and even those that are rational weigh costs and benefits very differently than governments with broad territories and populaces to defend. Nonstate groups frequently don't have fixed locales to target, and many of them would even welcome counterattacks. A response from the United States would provide the recognition that so many nonstate groups crave while possibly even generating public sympathy. There is also a deep concern that

the strategy of equivalence could be escalatory, cascading an attack in cyberspace into a much bigger conflict.

Perhaps the biggest issue cyber experts raise about US strategy, though, is whether it places too much emphasis on the offense. Indeed, budget plans in 2014 show the US Air Force spending 2.4 times as much on cyber offense research as on cyber defense. The concern goes beyond the traditional view that offense is the more destabilizing side (the worry that it encourages an attack mentality) and that defense is typically stabilizing (good defenses reduce the likely gains of any attack, discouraging offensive attacks in general). Rather, experts worry about the inherently seductive nature of cyber offense and the impact it might have on the military. As one report put it, offensive concepts like "cyber war, software exploit, digital catastrophe and shadowy cyber warriors" are much more glamorous than the defensive, like "security engineering, proper coding, protecting supply chains." Yet defense is where the United States should be putting more of its efforts, not just because of how it aids stability and deterrence, but as a senior US military official said bluntly, "We're already very good at offense, but we're just as bad at defense."

Regardless of where CYBERCOM and the broader US military come down on these issues in the years ahead, it's critical that the civilian side of the national security apparatus and civilian government leaders start to understand and contribute to them. Important plans and strategies for a powerful new technology are being made, but the broader civilian political system and populace has largely remained apart from the discussion. For example, the United States' strategic policy laying out its budding offensive cyber posture, is designed to "offer unique and unconventional capabilities to advance US national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging." But it only emerged in public discourse via leaks to newspapers, months after it had been decided.

It would be a mistake to draw a historic parallel between the destructive power of cyber weapons and nuclear bombs, as some civilian leaders have recently done (the head of the US Senate Armed Services Committee amusingly described a cyber weapon as just "like a WMD"). Yet there is a worrisome parallel in how civilian leaders nowadays, as in the past, might be caught off guard by how

operational plans actually make use of these new weapons. For instance, when General Curtis LeMay headed the new Strategic Air Command in the 1950s, he surprised civilian leaders when they finally got around to asking what he planned for American nuclear bomber forces, if there ever were a crisis with the Soviets. LeMay explained that he was not too concerned, because he'd just order a preemptive nuclear attack. "I'm going to knock the s**t out of them before they take off the ground." It's a good thing they asked and shut down such plans before the Cuban Missile Crisis just a few years later. Today's leaders might want to ask if there are any cyber equivalents.