Reprinted with permission from Chapter 7 of *Glass Houses: Privacy, Security, and Cyber Insecurity in a Transparent World*

JUNE 2017

INCREASINGLY WARM RELATIONS between Taiwan and the mainland turn sour in November 2016, when Beijing restricts certain airfreight traffic from the island in an attempt to protect its homegrown business in computer peripherals. Revelations in the *Taipei Times* of payoffs by PRC agents to several Taipei television news stations and civil servants in the governing Nationalist Party send tremors through the island and within the party. When the revelations are followed by the unmasking of a highly placed PRC spy in the office of the president, a third-party candidate for president of Taiwan—anticorruption but pro-mainland—throws his hat in the ring. His candidacy will produce a fractured vote, as in 2000 when Taiwan elected Chen Shui-bian from the DPP, or Democratic Progressive Party. Chen's four-year term—the only time since 1949 that Taiwan's government was not led by Nationalists—was a period of nonstop strife with the mainland. The elections will occur in late March.

February 10, 2017

A PLA navy destroyer in the South China Sea harasses commercial geological survey vessels from Vietnam and Brunei. These vessels are operating in their own exclusive economic zones, which conflict with those of China. They're looking for oil. The South China Sea is ringed by the Philippines, Malaysia, Brunei, Vietnam, and China, and by Taiwan to the north, but China ignores their overlapping claims. China claims the entire South China Sea not only as its exclusive economic zone but also as its sovereign national territory. China's foreign minister had told his Singaporean counterpart, while staring him down in a meeting in Hanoi in July 2010, "China is a big country and other countries [around the sea] are small countries, and that's just a fact."[1] In line with that neighborly view of international law, China had for several years been warning international oil companies against surveying off the coast of Vietnam, and on several occasions the PLA navy had chased their vessels away.

The South China Sea is one of the world's most crucial waterways. More than forty-one thousand ships pass through it every year. That's more than twice the ships that pass through Suez, and more than three times the number traversing the Panama Canal. From the southeast, the sea is a bottleneck: More than half the global merchant-fleet tonnage enters it every year through the Strait of Malacca, a skinny neck of water between the Indonesian island of Sumatra and the Malay Peninsula. For the U.S. Navy, the strait is one of the world's most important strategic passages, because it links the Pacific and Indian oceans. Control of the South China Sea would effectively give China control over the strait, and vice versa. Avoiding this passage would add thousands of miles to a voyage from Suez to Hong Kong.

February 16

Public opinion polls released in Taipei show a dead-even three-way split among likely voters in next month's presidential election.

February 22

The unarmed USNS *Sumner,* an oceanographic survey ship, is tracking the HAN-class attack submarine 405 as it leaves its base through a huge underground tunnel on Hainan Island, heading southeast. This cat-and-mouse game goes on every day between blue water navies. As the *Sumner* approaches 10° north latitude, however, a PRC Jianghu Ill-class frigate passes dangerously close in front of its bow and switches on its gunnery control radar. This is like cocking a pistol in someone's face at six feet. The *Sumner* veers sharply away, avoiding a confrontation. A shrill exchange of diplomatic protests follows, with the United States complaining about Chinese interference with international right of passage in the South China Sea, and the Chinese asserting that the United States was engaging in warlike activities within their exclusive economic zone. This is a replay of the dispute over the 2001 midair collision off Hainan Island between a U.S. Navy EP-3 surveillance plane and a Chinese fighter plane. This is not the first time PLA navy warships have bullied unarmed U.S. Navy survey vessels, but turning on the radar is a step up the escalation ladder, and both sides know it. In Taipei and Washington, reaction to the confrontation is immediate and loud.

The conflict between freedom of navigation and exclusive economic zones has been an unresolved sore point among maritime powers and coastal powers since the advent of the UN Convention on the Law of the Sea in 1982. The convention has been ratified or acceded to by 161 nations.* The United States signed it in 1994 and generally abides by it, but the U.S. Senate has never ratified it. It has been so widely accepted, however, that it has arguably become customary international law, regardless of ratification. The convention requires that nations "refrain from any threat or use of force against the territorial integrity or political independence of any State."[3]The Chinese regard this provision as a weapon—not warfare exactly; call it "lawfare."[4]

February 23

The Chinese foreign minister summons the U.S. ambassador in Beijing and tells him in blunt terms that the Chinese government regards with the utmost

gravity the conduct of warlike activities, including espionage, within its exclusive economic zone and sovereign territory, and China reserves the right to take all necessary measures to prevent their recurrence. In diplomatspeak, this is a threat to sink U.S. surveillance ships in the South China Sea—but it is not made public.

An hour later, through public channels that are well covered by the international media, the foreign minister states that, consistent with the convention's requirement that nations resolve their differences peacefully, China proposes immediate bilateral consultations to avoid further confrontations between naval vessels of the United States and the PRC. In response to a planted question, the minister rejects the suggestion of a regional conference on the issue. The same day, the Web site of the English-language *China Daily* quotes a "senior government source" suggesting that the United States should exert itself more strenuously to bring renegade Taiwanese politicians into line. After all, such a course would be in accordance with the American One-China Policy, which has not changed since the Nixon administration. China's only interest, the source says, is regional peace and stability.

March 19

China's naval confrontations and aggressive rhetoric have the opposite effect on Taiwanese politics than Beijing intended. By a squeaky margin in a split vote, Taiwan elects a DPP government that is implacably anti-PRC.

April—May

U.S. attempts to cool off the new Taipei government get nowhere. Beijing condemns U.S. hypocrisy and meddling in "purely regional" issues and begins to reinforce mobile missile units on the mainland coast opposite Taiwan, raising the threat of invasion. On April 11, the PLA announces that its East Sea Fleet will begin amphibious exercises with the 1st Army Group, Nanjing Military Region. It simultaneously warns South Korea and the United States against holding naval exercises in the Yellow Sea, which China also claims. Intense consultations

are held in New York. Over private U.S. and very public PRC objections, Taipei announces a referendum on independence, to be held in mid-September. A red line is about to be crossed.

June 19

It's Sunday, and the East Coast of the United States is sweating through the worst heat wave since the brutal summer of '10. The lead editorial of the *New York Times* sharply criticizes the Taipei government. The United States had been prepared to go to war over Soviet arms in Cuba, it says; Taiwan is even closer to mainland China than Cuba is to Florida. It recalls that Douglas MacArthur called Taiwan an "unsinkable aircraft carrier" off the Chinese coast, but surely bellicose World War II-era metaphors like that have become irrelevant; no one envisions invading China. And what was America's interest in Taiwan, really? Economic integration between the island and the mainland was already extraordinary. The principal U.S. interest in this regional issue, opines the *Times,* is that it be resolved peacefully. Though the *Times* is left of center, its point of view resonates widely with an American public that still suffers significant unemployment and has no taste for more wars in far-off places.

In another editorial on the same day, as New York experiences its first rolling brownouts in years, the same newspaper notes that calls for voluntary curtailment of energy use by both the White House and the mayor of New York City have been unavailing. The paper calls for aggressive regulation of energy use. It runs a story on the front page about three homeless people who have died from heat prostration in New York. Similar stories run in Atlanta, Washington, and Cleveland, which are all experiencing record heat.

June 21

Bilateral talks at the UN in New York break down as China, in an attempt to "encourage" diplomatic progress and warn Taiwanese voters, restricts commercial aviation between the island and the mainland. The following day a PLA navy frigate leaves the port at Ningbo, guns sheathed, and stands off Taipei in view

of land for twelve hours. It later circumnavigates the island and returns to base. Several amphibious units on the mainland go on active alert.

June 22

A carrier group from the Seventh Fleet, led by the USNS *Gerald R. Ford,* the United States' first superclass carrier, steams east, ready for war.

June 23

Washington—12:20 P.M.

The temperature reaches 105 degrees for the third straight day. The electricity grid in the northeastern United States goes out. The *Times's* immediate online editorial says, in effect, "We told you so."

Washington—1:15 P.M.; Beijing—1:15 A.M. the following day

At a secret meeting in "the tank," a secure room in the basement of the White House, the president turns to the four-star commander of U.S. Cyber Command, who is also the NSA director, and demands to know whether our grid is being attacked, and if so, by whom. "Sir," she says, "under standing executive orders, the NSA has nothing to do with protecting civilian networks. That's DHS's responsibility."

Annoyed, the president turns to the secretary of homeland security. "Well, damn it! Are we being attacked or not?"

The secretary, whose chief qualification for the job is that he ran the president's victorious campaign in Ohio, turns to his new undersecretary for cyber-defense, who stammers, "Sir, uh, we're evaluating that now. Very aggressively, sir."

Washington—1:21 P.M.; Honolulu—?:21 A.M.

A marine colonel enters the tank and hands the president an urgent intelligence report from the U.S. Transportation Command, aka TRANSCOM: Five Marine F/A18-Cs from Guam, bound for Okinawa, have ditched in the Pacific, eight hundred miles from their intended rendezvous point with a tanker that was to

have refueled them in midair. "All pilots successfully ejected, CSAR ongoing," the colonel says.

"What the hell is CSAR?"

"Combat search and rescue, sir. It will be some hours before we can get them out, sir."

Washington—1:24 P.M.

TRANSCOM reports that just before Mayday calls went out, radio traffic from the ditched fighters indicated their rendezvous coordinates were different from those given to the tanker—for reasons the TRANSCOM commander will later be unable to explain to the secretary of defense. This is a Whiskey-Tango-Foxtrot moment—military slang for "What the fuck?"

Washington—2:09 P.M.; Beijing—2:09 A.M. the following day CNN, Fox, BBC, and Al Jazeera are running PLA video showing Chinese sailors heroically plucking our exhausted fliers from heavy seas, safe and sound and expressing gratitude to their saviors. The frigate happened to be in the right place at the right time, at some distance from its usual area of operation.

Washington—3:15 P.M.; Honolulu:—9:15 A.M.

An hour later—following a video hookup between the president, the secretary of defense, and the commander of U.S. Pacific Command, or PACOM, overlooking Pearl Harbor—an additional carrier group detaches from the Fifth Fleet in the Indian Ocean and sails full speed for the Strait of Malacca.

June 24

Washington—12:41 A.M.; Honolulu—6:41 P.M. the evening before A Chinese submarine surfaces undetected within half a mile of the *Gerald R. Ford* in midocean. The sub is powered by a quiet electric drive engine developed in a top-secret U.S. Navy program. Satisfied it has been seen, the Chinese ship submerges and disappears. The message is unmistakable: You can't see us coming—and we could sink you if we wanted to.

Washington—9:45 A.M.; California—6:45 A.M.

The traffic control system in San Diego begins to blink. Back in the tank, the DHS secretary reports that his analysts have concluded that, yessir, we are being attacked. "No kidding," the president mutters. He authorizes CYBERCOM (the U.S. Cyber Command) to retaliate against six specific parts of the Chinese grid.

Washington—10:32 A.M.; Beijing—10:32 P.M.

The Chinese have taken four of the six intended targets offline; they can't be taken down remotely. The other two targets are hit: Xiamen and Chengdu go dark.

Washington—12:00 P.M.; San Diego— 9:00 A.M.; Honolulu:—3:00 A.M.

The San Diego grid goes down, followed by the grids in Seattle (another big navy base) and Honolulu. In California's Central Valley, turbines in three electric generators mysteriously blow up. The secretary of energy tells the president that this kind of equipment takes twelve to twenty-four months to replace.

"What?!" the president says. "Don't I have emergency powers to deal with that?"

"We don't make those generators in this country anymore, Mr. President—haven't made them for years."

"Who does make them?"

"India, sir. The Indians make them, and the Chinese."

Meanwhile, for reasons the USPACOM commander in Honolulu can't understand, we begin losing track of several more Chinese submarines. Frantic efforts by the director of White House communications have kept the story of the blown-up generators offthe evening news, but it won't stay quiet long.

Washington—3:00 P.M.

The treasury secretary informs the president that the Chinese have begun selling Treasury notes on the open market. In the next hour, all market indexes go into free fall and trading halts on U.S. markets—but not overseas. The dollar is being clobbered. The secretary has spoken with the Chinese finance minister, who regretted very much that domestic economic pressures had caused them

to start selling. The consensus of his staff, the minister said, is that they should sell much more—half a trillion worth—but that he, the minister, felt they should hold the line for now at $100 million. He sincerely hopes to begin buying as soon as domestic conditions in China permit.

Washington—5:45 P.M.; Beijing—5:45 A.M.

The president of China calls the White House. I am happy to say, he tells our president, that your airmen are safe and sound in our military hospital in Xiamen, which has excellent modern electrical generating capability, and we look forward to releasing them in a day or so, when they are fit. I also want to say how much I regret the difficulties you are having with those old electric generators in California. My staff tells me the Indians have a terrible production backlog. So do we, Mr. President, but in light of the great value we place on Sino-American friendship, we would be pleased to replace these generators as a high priority, and on favorable terms. That might be particularly important to you in case others were to go down, perhaps in more critical locations.

"One moment." The president hits the mute button. "The son of a bitch is threatening to take out more generators. Can he do it?" The CYBERCOM commander looks at the DHS secretary. "Sir," the secretary says, clearing his throat. "Sir"—his voice has gone squeaky—"we don't know."

"Don't know! Didn't you assure me last week that your critical infrastructure protection program was a one hundred percent success? Didn't you?" The president is screaming. He turns to his secretary of energy: "The rest of the grid—is it safe?" The energy secretary shrugs and extends his hands as if to say, No idea, sir. At that point the secretary's BlackBerry goes off.

"Goddamn it," the president shouts, "I thought I told you never to bring one of those things in here!"

"Sorry, sir, I..."

"Sorry my ass. Get it out of here—now. For all you know, that thing is a direct pipe to Beijing." The DHS secretary turns pale and slips his hand into a pocket to make sure *his* BlackBerry is turned off. A colonel breaks in with a message: The Omaha Public Power District is reporting erratic behavior on its SCADA networks. Omaha is home to U.S. Strategic Command.

"Jesus Christ," the president says, and hits the mute button again.

"Mr. President," our president says, "thank you for your call. I'm sure you'd agree that it is in the interests of both of our countries to reduce the current dangerous level of tension. Our defense secretary is prepared to open talks with your side immediately to achieve that..."

"Mr. President," their president says, "I appreciate your attitude, but I think perhaps you do not understand. The progress of your carrier groups toward China's coast is an immediate threat to China's security and integrity, and we will not tolerate it, sir." And he repeats, his voice rising, "We will not tolerate it! If the carrier group from your Fifth Fleet does not alter its course within forty-five minutes"—he's now practically yelling—"we will disrupt the power grid in your northern midwestern states and throughout your Pacific coast. If this naval war party—or any American warship in the future—enters the Strait of Malacca we reserve the right to treat its progress as an act of war. If the *Gerald Ford* or its sister ships proceed east of 122 degrees east longitude, our missiles will sink them." Then, more quietly: "We respect your navy, Mr. President, but please-please do not underestimate our capabilities. They are based, as you undoubtedly know, on excellent technology!

"I do not wish to be impolite, Mr. President; I will not ask you to reply now. I will know your reply in forty-five minutes. I sincerely hope, Mr. President, that our foreign secretary and your secretary of state can meet within thirty-six hours to produce a joint communique' restating that the bedrock foundation of our relations since 19?2 remains intact, and that any effort by the current regime in Taipei to alter that foundation would be vigorously opposed by both of our governments. Thank you, Mr. President, and good-bye."

Click.

Half an hour later the carrier changes course.

Thus it was that in a dispute in 2017 that appeared to be entirely about Taiwan, the United States of America lost the freedom of navigation through the South China Sea. As a result, China's effective defense perimeter was pushed outward one thousand miles south of Indonesia and east of the Philippines, drawing Vietnam, Cambodia, Thailand, Malaysia, Singapore, Indonesia, Brunei, Papua New

Guinea, and the Philippines much more tightly into the ambit of Chinese "persuasion," and making it clear to the governments in Canberra and Tokyo that they had serious thinking to do about their geopolitical allegiances.

The joint communique* that followed was the most vigorous statement of international cooperation that China and the United States had issued in many years and was hailed in Western capitals as a triumph of statesmanship.

The referendum proposal in Taiwan? That was defeated.

Could This Happen?

I'm not predicting this scenario, but it's well within the realm of possibility. And we would be foolhardy not to prepare for it. With the exception of successful attacks on our electricity grid—and we know the grid is vulnerable—virtually every aspect of this fictional scenario *has already happened.* The Chinese contention that their economic zone overrides the right to free navigation in international waters is a matter of record. Confrontations between PLA navy warships and unarmed vessels in the South China Sea have already occurred much as described. The capabilities of Chinese warships are in fact catching up fast with our own—because they're based in significant part on stolen U.S. Navy technology. The mismatch between the Department of Homeland Security's cyberresponsibilities and its capabilities (they're extremely weak) is well-known. Chinese hackers really have penetrated networks at TRANSCOM, which controls tanker refueling schedules. The incident of the Chinese submarine surfacing undetected amid a U.S. Navy carrier group really did happen. Diesel-electric generators that keep our lights on really do come from India and China; we don't make the big ones any longer. And of course the Peoples Republic of China is the largest holder of U.S. government debt. It would be foolhardy for U.S. government officials to believe that such events could not be made to occur in a choreographed sequence like the one described above. But so far in the United States we've been able to talk about this danger only

as an argumentative replay of the old black-and-white, war/not war dichotomy. Here's what the discussion sounds like so far:

> The United States is fighting a cyberwar today, and we are losing. It's that simple.
>
> —Admiral Mike McConnell, former director of national intelligence[5]

> The biggest threat to the open internet is not Chinese government hackers or greedy anti-net-neutrality ISPs, it's Michael McConnell, the former director of national intelligence.
>
> —Ryan Singel, blogger[6]

This kind of exchange easily degenerates into a shouting match that obscures the complexity of the problem, perpetuates confusion about the meaning of war, and confirms the Chinese view that American thinking on the subject is superficial. Words like *cyberwar, netwar,* and *information war* mean different things to different people. So let's simplify the issue and assume that these three terms are synonymous (as indeed they usually are), and then lets ask: What *is* a cyberwar, anyway?

At least six different situations have been called cyberwar:

1. Electronic propaganda

The Kosovo War in 1998—99 involved frantic competition for propaganda advantage using the Internet. None of the parties sought to bring the Net down. There were plenty of attacks on infrastructure, but they involved physical bombs, not logic bombs.

2. Massive DDOS attacks

The first Internet war was a series of DDOS attacks by Russians against Estonian banks and government institutions in 2007. This was indeed a cyberattack against a nation-state. We have suffered similar attacks in the United States. On July 4, 2009, for example,

a DDOS attack that *probably* originated in North Korea shut down the White House's Web site—but not its communications—for three days. We do not treat DDOS attacks as acts of war, however, and we are pretty good at fending them off. It is highly unlikely that the United States could be similarly paralyzed by such attacks. The U.S. communications infrastructure is too robust and redundant, and the country is much larger than Estonia.

3. Strategic cyberwar

A strategic cyberwar would be a solely electronic war against infrastructure—railways, the power grid, or air traffic control, for example—or against forces. This has not happened, and it is very unlikely to happen. Its effects would be too difficult to predict, in part because the state of an adversary's defenses would be uncertain. The diplomatic, electronic, and possibly physical consequences of attempting such an attack would also be too severe to warrant the risk. Just because a conflict begins in cyberspace doesn't mean it must remain there. In addition, a massive strategic attack could probably not be limited to a single target country, so the risk of disrupting international financial markets, telecommunications, and infrastructure would be significant. No nation wants to do that.

4. Electronic sabotage

Electronic sabotage operations generally occur through what is known as a supply chain operation—that is, compromising sensitive electronics to make them fail, as the CIA brilliantly did during the 1970s.[7] Starting during the detente years of the Nixon administration, the Soviet leadership understood that they were years behind the West in technology. So Soviet intelligence agencies geared up to steal from Western—especially American—sources what they lacked, particularly computers and microchip technology. To this day, no commercially viable computer chip has ever been manufactured in Russia. The Soviets packed trade and agriculture

delegations with intelligence officers, and in one case, a Soviet guest visiting Boeing put adhesive on the soles of his shoes to pick up metal samples. Still, nobody wanted to believe warnings from CIA counterintelligence officials that the Soviets were engaged in wholesale economic espionage, because nobody could *prove* these incidents were part of a grand design. Meanwhile, the Soviets, often through front companies, were stealing radar, machine tools, and semiconductors—all items that were embargoed to the Soviet bloc during the cold war. American views changed in July 1981, however, when the French disclosed to President Reagan that they had a Russian defector in place who had revealed the entire Soviet operation, known as Line X. The defector was Colonel Vladimir I. Vetrov, known to the French as Farewell. So in early 1982, the CIA and National Security Council officials proposed to launch a classic counterintelligence operation: Rather than roll up this espionage network, they would use it to advantage. They now had the Soviet shopping list, why not help them fill it—but with "improved" products designed to pass initial Soviet quality control tests but later fail? President Reagan readily approved the plan, and in due course, flawed microprocessors were built into Soviet military equipment, turbines designed to fail found their way into a gas pipeline, and thoughtfully imperfect plans wreaked havoc with chemical plants and a tractor factory.[8] William Safire of the *New York Times* finally broke this story in 2004. According to Safire's source, the Soviets wanted to automate the operation of their new trans-Siberian gas pipeline but lacked the technology to do so. They applied for an export permit, and when we rejected it, the KGB sent a spy into a Canadian company to steal what they needed. Farewell tipped us off to the plan. The CIA then made sure our friends got what they wanted—sort of. The goods the Soviets so cleverly filched were programmed to run the pumps to produce pressure far greater than what the pipeline joints and valves could

withstand. As Safire reported, "The result was the most monumental non-nuclear explosion and fire ever seen from space."[9]

Supply chain attacks involve corrupting a product at the place of manufacture or—more often—somewhere along the line between the manufacturers loading dock and the point of delivery. Supply chain integrity is a major concern of every large company, whether a food supplier, an electronic manufacturer, or a medical device company. The food supplier does not want to sell poison. The electronics firm wants software that does what it's supposed to do—and that does *not* do something else. The medical device company wants to know its titanium screws really are made of titanium and machined to the right tolerance. Counterfeits could kill patients and lead to massive liability. But food, electronics, and medical devices come from all over the world, so policing supply chains is a major headache—including for the military. The Pentagon has found counterfeit computer chips in military jets, for example.[10] The equipment on modern fighter aircraft uses hundreds of computer chips, but many of them come from abroad—which increases the ease of sabotage—because that's where most of the manufacturing capacity has moved. Whether the Pentagon fell for a foreign intelligence service's supply chain operation (probably not) or simply bought chips from a corrupt contractor intent on making more money, counterfeits invariably mean degraded performance. In January 2010, a software flaw in the Pentagon's GPS network disrupted satellite communications. In 2007, six brand-new stealth F-22 Raptor jets were lucky to find their way back to base when their computers went down."

5. Operational cyberwar

Cyberoperations as part of hot war are here to stay. This is operational cyberwar, and it has already occurred at least three times. In 2003, before U.S. and coalition troops moved into Iraq, the

U.S. military already owned Iraq's supposedly closed military communications system, and U.S. commanders used their control to great effect. They not only successfully frightened many Iraqi commanders into surrendering without a fight, they also gave the Iraqis instructions, which were followed, on how to park their armor close together before abandoning it—so we could blow it up more efficiently.[12]

The second and most breathtaking instance of operational cyberwar occurred in 2006, when the Israeli air force fighter-bombers flew undetected along the Turkish-Syrian border and blew up a nuclear weapons facility the North Koreans were building for Syria. The next day the media carried the story of the bombing but not the backstory: Syria's air force didn't even scramble to meet the attack because Syria's tip-top Russian-made radar (which Iran also uses) showed nothing unusual. Syrian military radar operators might as well have been looking at cartoon pictures of the clear night sky—pictures made in Tel Aviv. This was indeed electronic magic of an advanced sort, and worthy of the name cyberwar.[13]

The third instance of operational cyberwar occurred in 2008, when Russia invaded Georgia. Though the Russians contend the Georgians started the cyberfight, the Russians definitely finished it, paralyzing Georgian communications. In the future, cyberoperations will accompany all hot wars. In this chapter, my fictional example illustrates how cyberoperations could also be used in connection with operational hot war threats in ways that actually avoid a hot war—but lead to a dishonorable peace with strategic implications.

6. The criminal-terrorist symbiosis

Cyberoperations are cheap. The physical tools of the trade are not secret, and they're readily available the world over. What separates advanced nation-state capabilities from the lesser capabilities of criminal organizations and terrorists is expertise, not expensive equipment, and expertise is bound to proliferate. When Chinas Dr. Shen

> wrote more than twenty years ago, "[E]very computer has the potential to be an effective fighting unit; and every ordinary citizen may write a computer program for waging war,"[14] he had in mind a version of peoples war waged on behalf of the Chinese state. But the ability to wreak havoc on networks is not limited to nation-states and their proxies. Al-Qaeda and other terrorist groups are thinking about network disruption, and so are groups of a different ilk:
>
> > We do not believe that only nation-states have the legitimate authority to engage in war and aggression. And we see cyberspace as a means for non-state political actors to enter present and future arenas of conflict, and to do so across international borders.[15]

This is the bravado of the Electronic Disturbance Theater, a hac-tivist group "working at the intersections of radical politics, recombinant and performance art, and computer software design."[16] This kind of talk would have been unthinkable, literally, only a few years ago. The idea that a collection of artsy, self-righteous geeks would have either the nerve or the imagination to issue a threat of "war and aggression" against nation-states was so preposterous that no one would have thought of it when war was synonymous with the concentrated application of heat, blast, and fragmentation, as it had been since the time of Napoleon. But if this group's bravado was exaggerated, and their skill thus far limited, their threats are no longer entirely preposterous. In 1998, in order "to demonstrate solidarity with the Mexican Zapatistas," its members organized DDOS attacks against Mexican president Zedillo s Web site, and later against President Clintons White House Web site, and then against the Web sites of the Pentagon and the Frankfurt and Mexican stock exchanges.[17] If those tactics seem ho-hum now, they did not seem so in 1998, and the skill level of nonstate groups is increasing.

In the late 1990s the Chinese authors of *Unrestricted Warfare* predicted exactly these sorts of "sundry monstrous and virtually insane destructive acts" by groups like EDT. They also pointed out the

asymmetric advantage that nonstate actors would have, because a nation-state "adheres to certain rules and will only use limited force to obtain a limited goal," whereas terrorists (artistic or otherwise) "never observe any rules and ... are not afraid to fight an unlimited war using unlimited means."[18] In the intervening years the convergence of criminal and terrorist organizations has given the EDT manifesto a far more sinister ring than it had when it came from a group interested in "recombinant performance art." Crime finances terrorism, and terrorism in turn enhances the market for criminal extortion. For instance, large-scale drug dealing financed the Madrid bombings in 2004, which were set off electronically. Spanish police later seized nearly $2 million in drugs and cash from the plotters. Indeed, almost half the groups on the U.S. government's list of terrorist organizations raise money through drug trafficking.[19] As a general rule, large criminal enterprises are increasingly networked rather than hierarchical, both in their organization and in their means of communication.[20]

In 2000 the U.S. National Intelligence Council predicted that in "the next 15 years, transnational criminal organizations will become increasingly adept at exploiting the global diffusion of sophisticated information, financial, and transportation networks." The council predicted that these organizations would form ad hoc alliances both with one another and with political movements. With income from trafficking in arms, narcotics, women, children, and illegal immigrants, they would corrupt unstable and economically fragile states, insinuate themselves into businesses, and cooperate with insurgents on specific operations.[21] By 2008 the council's predictions were even more ominous: "For those terrorist groups active in 2025, the diffusion of technologies and scientific knowledge will place some of the world's most dangerous capabilities within their reach." These groups will "inherit organizational structures, command and control processes, and training procedures necessary to conduct sophisticated attacks."[22]

In a word, advanced network operations will cease to be the special province of a few advanced states. Nonstate actors, who cannot be deterred with threats of cyber retaliation, have crashed the party.

But When Is It War?

Is Admiral McConnell right to say that we're already fighting a cyberwar? Or are his critics right that he's just engaging in scare tactics? Make no mistake about it: Our government and our corporate enterprises are being attacked relentlessly, McConnell is certainly right about that. But calling these attacks war transforms the dispute into an argument about categories and not about the nature of the world. Determining when an attack amounts to war is important, but it won't enlighten us about the nature and urgency of the threat or how to deal with it. It won't even tell us how to respond to specific attacks. These attacks are coming in waves and are growing more sophisticated every week. Yet we use the term *cyberattack* to include everything from network nuisances to systematic espionage to disabling electronic sabotage. Estonia's networks were systematically attacked from Russia, but when faced with deciding whether that was war, NATO said no. So attack and war are not necessarily the same thing.

The war/not war question has also become more difficult—and less useful—because the line between war preparation and war fighting has become blurred. Consider what happens, for instance, when network operators in Country A penetrate the electric grid of Country B. And let's assume that Country As infiltrators intend only to look around and figure out how the network is configured; they have no intention of disrupting the grid, though they may want to do that later. In the course of that operation, however, Country A doesn't simply sneak into the system; it also makes changes to the network—like creating backdoors to enable it to get back in later. But looking around, or surveying, a computer network is not an act of war. It's just spying. Everybody does it.

Now suppose Country As intention is more sinister. Assume it is intentionally laying the groundwork for sabotage. In U.S. military doctrine, this is called preparing the battlespace, and if our side were

doing it, it would be done by the armed forces under the military legal authorities found in Title 10 of the United States Code—not under the intelligence authorities of Title 50. We did this on the eve of the second Iraq war in 2003, when we took over Iraqi networks. We used some of them for propaganda, and we took some of them down.[23] Most other countries don't bother with such cumbersome and sometimes artificial distinctions between military and intelligence authorities, however; they just do the operation. But regardless of legal authorities, *what they would do if they were preparing sabotage is exactly the same as if they were just looking around:* They'd create backdoors to enable them to attack the network later.

How would we know the difference between an intelligence operation (not war) and a preconflict subversion of a U.S. network (possibly an act of war)? The answer is: *We couldn't*—not unless the attacker went further and left destructive logic bombs that were instructed to go off later, *and* unless we discovered the trick. But logic bombs are just a few lines of computer code buried in a software program that might contain a million or more lines of it. And as we learned in earlier chapters, in the current state of technology they're almost always impossible to discover. This is one reason why offensive cyberoperations currently enjoy a great advantage over defensive ones. So the answer remains: In almost every case imaginable the line between an electronic intelligence operation and a presabotage act of electronic war is impossible to see. This is why penetrations of military and infrastructure networks cannot be dismissed as "just espionage."

Nor is it wise to conclude blithely that the Chinese (or the Russians, or any other actual or potential adversary) don't intend to go to war with the United States. Even assuming that assessment is currently correct (it probably is), intentions can change on a dime. Capabilities and defenses cannot. They take a long time to build. A nation that puts its faith in a potential adversary's benign intentions rather than its own strength and capabilities is a nation that is psychologically and practically incapable of defending itself.

++

Thanks to the author, Joel Brenner, and to Penguin Group for granting permission to reproduce and distribute Chapter 7 of *Glass Houses: Privacy, Security, and Cyber Insecurity in a Transparent World* to the participants of the government sponsored C3E Workshop at the United States Military Academy at West Point, NY on 14 January 2014 as part of the author's presentation on that date.