Chapter Eight

# THE AGENDA

Invisibly, military units from over a score of nations are moving into a new battlespace. Because the units are unseen, parliaments and publics have not noticed the movement of these forces. Because their first skirmishes have been isolated and involved only simple weapons, few have thought that cyber warriors could do more. Because most of the major military powers are also one another's trading partners, commentators cannot envision the circumstances that could turn their relations to hostility. Because the United States has been at war in one nation for seven years and in another for nine, is struggling with its worst-ever recession, and is diverted by partisanship, the "bandwidth" of its policy elites is already consumed. Thus, with attention diverted elsewhere, we may be laying the groundwork for cyber war.

There may be parallels in the early years of the last century.

Barbara Tuchman in *The Proud Tower* describes a world similarly diverted from the realization that its various militaries were preparing devastating forces without contemplating the horrific consequences of their use. Then, as she describes in the sequel, *The Guns of August*, a spark caused those forces to be activated. Von Schlieffen's elaborate military use of Germany's massive new freight rail network literally set wheels in motion that could not be stopped. The military use of the new chemical industry added an element of destructiveness. The use of chemical weapons did far more damage than anyone had anticipated. Today our military is developing elaborate plans for a new kind of war, once again using a technology originally designed for commercial use. As in the period one hundred years ago, those plans have received little public scrutiny.

There have been few times in our history when the American academic community, the media, and the Congress have focused on a potential problem and together cast so much light on an issue that controls were put in place that averted calamity. The issue of strategic nuclear war, referenced much in this book, is the clearest example. A new technology had burst upon the world and the U.S. military had seen in it a way to achieve military dominance and, through that, peace. At airbases with the signs "Peace Is Our Profession," the plans called for early and massive use of nuclear weapons in a war, against cities and civilian targets. Not until the research community focused a public klieg light on those plans and the larger issue of how to fight nuclear war, were rational controls and plans developed and adopted.

Today at U.S. Cyber Command, and at its related agencies, some of our nation's most intelligent, patriotic, and undercompensated government employees, military and civilian, are putting plans and capabilities in place to achieve "dominance in cyberspace" to maintain this country's security and preserve the peace. In other nations, cyber war units are also preparing. As part of that preparation, cyber warriors are placing trapdoors in civilian networks, placing logic bombs in electric power grids, and seeding infrastructure for destruction. They believe that their new form of warfare is an advance, not just because of its use of the latest technology, but because it does not involve explosives and direct lethality. Like the Predator pilots who sit in the United States, killing Taliban in Pakistan by remote control, they could subconsciously think that because they live in a peaceful suburban environment, the effects of their destruction on the other side of the world may somehow be clean and neat, unlike "real war."



When in a period of rising tensions, in some future crisis now unforeseen, a cyber warrior of some nation is ordered to "send a message" to the potential adversary by using one of the logic bombs already in place, will it forestall or will it trigger a broader shooting war? Perhaps because the opponent is misled about who started the war, other nations will be drawn in. Possibly, the cyber warrior in one of the score of nations with capability will act without authority, initiating a conflict. Alternatively, it may be a hacker who uses a cyber weapon for destruction rather than crime, or discovers and sets off a logic bomb left behind by someone else. The cyber war that ensues could be incredibly rapid and global.

When an American President sends U.S. forces to bomb a rogue state's nuclear weapons factory or terrorist camp, that nation may not be able to respond against our impressive conventional military forces. And yet, for a small investment in a cyber war capability, it may respond by destroying the international financial system, in which it has very little stake. The asymmetry of what it costs to counter our conventional military versus the minimal investment required for a cyber war capability will tempt other nations, and perhaps criminal cartels and terrorist groups as well.

Because the U.S. invented the Internet and has perhaps led in cyber espionage and the creation of cyber war tools, it may have

developed an implicit arrogance, causing us to assume that no one could humble America in a cyber war. Our cyber warriors and, to the extent that they think of cyber war, our national security leaders in general, may take comfort in the fact that we could perhaps see a cyber attack coming. They may think that we could block some of it, and they may believe we could respond in kind, and then some. The reality is that a major cyber attack from another nation is likely to originate in the U.S., so we will *not* be able to see it coming and block it with the systems we have now or those that are planned. Yes, we may be able to respond in kind, but our nation will still be devastated by a massive cyber attack on civilian infrastructure that smacks down power grids for weeks, halts trains, grounds aircraft, explodes pipelines, and sets fires to refineries.

The reality may also be that when the U.S. President wants to retaliate further, he will be the one who will have to escalate. He will be the one who will have to cross the cyber/kinetic boundary. And he may find, when he does, that even our conventional forces are cyber dependent. The U.S. military's reliance upon cyber systems exceeds the extensive dependence of the commercial infrastructure. The contractors required for America to fight a war may be immobilized by cyber attack. The allegedly hermetically sealed computer networks upon which the Department of Defense relies may prove porous and unavailable. Highly advanced technology in the conventional weapons and systems that give U.S. forces dominance (for example, the F-35 fighter and the Global Positioning System) may suddenly not work. We are not the only nation that can install a logic bomb.

With a nation in the dark, shivering in the cold, unable to get food at the market or cash at the ATM, with parts of our military suddenly impotent, and with the regional flashpoint that started it all going badly, what will the Commander-in-Chief do? Perhaps he will appoint a commission to investigate what went wrong. That



commission will read the work of another commission, one appointed by Bill Clinton in 1996, and be astonished to learn that this disaster was foreseen back then. They will note the advice of a non-government commission written in 2008 advising the next President to take cyber war seriously. They may, if they are diligent, find a National Academy of Sciences study on Offensive Information Warfare from 2009 that warned that cyber war policy was "ill-formed, undeveloped, and highly uncertain."

The post-disaster commission, a special committee of the Congress, or the next President would likely recommend a plan so that "this sort of thing can never happen again." Since we know now what has been recommended already, what hasn't worked, and why, perhaps we should not wait for a disaster to embark on a plan to deal with cyber war. If we strip away the luxuries and the things that would be nice to have, there are six simple steps that we need to take simultaneously and now to avert a cyber war disaster.

## 1. THINKING ABOUT THE UNSEEABLE

First, we must initiate a broad public dialogue about cyber war. A student looking to choose a graduate school asked me recently to recommend a university where she could take courses on cyber war. We scoured course catalogues and found none at any of the major security-policy schools, such as Harvard's Kennedy School, Princeton's Woodrow Wilson School, or Texas's Lyndon Johnson School. She asked what books she should read and we found some interesting titles, but few that really delved into the policy and technology of cyber war. Many that seemed promising turned out to use the phrase "information war" to mean psychological warfare or public diplomacy.

Perhaps there are few books on cyber war because so much of

the subject matter is secret. Maybe there should be public discussion precisely because so much of the work has been stamped secret. In the 1950s and 1960s, people like Herman Kahn, Bill Kaufmann, and Albert Wohlstetter were told that nuclear war was something that could not really be discussed publicly. One of Kahn's responses was a book called *Thinking About the Unthinkable* (1962), which contributed to a robust public dialogue about the moral, ethical, and strategic dimensions of nuclear war. Open research and writing done at MIT, Harvard, Princeton, Chicago, and Stanford also contributed. Bill Kaufmann's classes at MIT, Harvard, and the Brookings Institution taught two generations how to think about nuclear strategy and how to ask analytical questions, so that they could think on their own. Today at Harvard and MIT, the aptly named Project Minerva, an open research program on cyber war funded by the Defense Department, has begun. (I am reminded of Hegel's dictum that "the owl of Minerva always flies at dusk," meaning that wisdom comes too late.)

The mainstream media's treatment of cyber war has improved. Reporters at the *Wall Street Journal* and the *New York Times* have written on it since 2008. Public television's highly respected *Frontline* series did an hourlong examination in 2003, *Cyber War.* Television has focused much more on identity theft by cyber criminals because so many readers and viewers have already been victimized by cyber crime. Movies, however, have been filled with cyber war. In *Live Free or Die Hard*, a former government cyber security official who wasn't listened to (whom the *New York Times* reviewer said was reminiscent of me. Nonsense!) cripples national systems. In *Eagle Eye*, hacking causes high-tension lines to melt and general havoc to erupt. In *The Italian Job*, the hacking is limited to traffic lights, but in *Ocean's Eleven* there is a power blackout in Las Vegas. There are so many more that much of the moviegoing public has little trouble understanding what cyber war can do. High-level policy officials



apparently seldom make it to the movies. Or maybe they think it's all just fantasy. To make them understand that such scenarios can really happen, we need an exercise program to drive home the point. General Ken Minihan has been promoting the idea of an Eligible Receiver–type war game for the private sector. "We could scare the pants off them, the way we did for the President in '97."

Congress, surprisingly, has held numerous hearings on cyber security and has tasked its Government Accountability Office to investigate. One GAO report asked whether the warnings that hackers could attack a power grid were true. GAO investigated one of the few power grids owned and operated by the federal government, the Tennessee Valley Authority's system. GAO reported back in 2008 that there were significant cyber security vulnerabilities on the TVA grid that left it open to attack. On cyber war, however, as distinct from cyber security in general, Congress has done little in the way of oversight, hearings, or legislation.

Congress is a federation of fiefdoms, subject to the vicissitudes of constant fund raising and the lobbying of those who have donated the funds. That situation has two adverse consequences with regard to congressional involvement in cyber war oversight. First, everyone wants his or her own fiefdom. Congress has resisted any suggestion, such as was made by Senator Bob Bennett (Republican of Utah), that there be one committee authorized to examine cyber security. As a result there are approximately twenty-eight committees and subcommittees involved in the issue and none with jurisdiction to think holistically. Second, Congress "eschews regulation" and spits it out. The influential donors from the information technology, electric power, pipeline, and telecommunications industries have made the idea of serious cyber security regulations as remote as public financing of congressional campaigns or meaningful limits on campaign contributions.

The dialogue we need will require meaningful academic research

and teaching, a shelf of new books, in-depth journalism, and serious congressional oversight.

## 2. THE DEFENSIVE TRIAD

The next item on the agenda to prevent cyber war is the creation of the Defensive Triad. As proposed earlier in this book, the Triad stops malware on the Internet at the backbone ISPs, hardens the controls of the electric grid, and increases the security of the Defense Department's networks and the integrity of its weapons. Much of the work in DoD has already begun as a result of President Bush's decision in his last year in office. The Defensive Triad is not an attempt, as my National Strategy for Cybersecurity was, to defend everything. The Triad is, however, designed to defend enough so as to cause another nation to think twice before launching a cyber war against us. A potential attacker needs to believe that much of his attack will fail and that its greatest effect will be retaliation of various sorts. Without the Defensive Triad, the U.S. should itself be deterred from acting in any way (not just in cyber war) that could provoke someone into a cyber war attack on America. Today we are so vulnerable to a devastating cyber war attack that U.S. leaders should walk cautiously.

We cannot build two of the three prongs of the Defensive Triad (the defense of the Tier 1 ISPs and of the electric power) without additional regulation. The argument I have made in the past about homeland security in general is that without using regulation the federal government is trying to achieve security with one of its arms tied behind its back. There was an era when federal regulations were overly intrusive and ineffective, but that is not inherent in the idea of the government asking industries to avoid doing some things and defining desired end states. At the Black Hat conference



in 2009 (discussed earlier), the cyber security expert and author Bruce Schneier made the same point, arguing that "smart regulation" that specifies the goal and does not dictate the path is needed to improve cyber security.

Our cyber war agenda must include regulation that requires the Tier 1 ISPs to engage in deep-packet inspection for malware and to do so with the highest standards of privacy protection and oversight. The ISPs must be given the legal protection necessary so that they do not have to fear being sued for stopping viruses, worms, DDOS attacks, phishing, and other forms of malware. Indeed, they must be required to do so by new regulations.

In order for the Department of Homeland Security to fulfill its role in the Defensive Triad, we must create a reliable and highly qualified component, perhaps a Cyber Defense Administration. The Cyber Defense Administration should be responsible for overseeing the deep-packet inspection system that the ISPs will run. It should also be responsible for monitoring the health of the Internet in real time, take over responsibility for regulating cyber security of the power sector from the Federal Energy Regulatory Commission (FERC), and provide a focal point for law enforcement activities related to cyber crime. The Cyber Defense Administration's most important role, however, would be to manage the defense of both the dot-gov domain and critical infrastructure during an attack.

The administration could provide the ISPs with known signatures of malware in real time, in addition to being a vehicle for the ISPs sharing what they themselves discover. The existing National Communications System, a four-decade-old office that worked on telephone availability in emergencies, and which was recently merged into the new National Cybersecurity and Communications Integration Center (NCCIC, but pronounced "*en*-kick"), could provide the ISPs with an out-of-band communications system that could pass these malware signatures. The Cyber Defense Adminis-

tration could draw on the expertise of the Pentagon and intelligence agencies, but the National Security Agency must not be given the mission of protecting domestic U.S. cyber networks. As uniquely skilled as NSA's experts are, they and their agency suffer from a public distrust exacerbated by the warrantless wiretapping ordered by Bush and Cheney.

Beyond regulating the ISPs, the other area of regulation needed is the electric power grid. The only way to secure the grid is to require encryption of commands to the devices running the system, along with authentication of the sender, and a series of completely out-of-band channels that are not connected to the companies' intranets or the public Internet. The FERC has not required that, but it did finally issue some regulations in 2008. It has not yet started to enforce them. When it does, do not expect much. That commission completely lacks the skills and personnel needed to ensure that electric power companies disconnect their controls from any pathway that a hacker could use. The mission of auditing the electric companies' compliance should also be given to the Cyber Defense Administration, where the expertise could be built and where the overly chummy relationship with the industry exhibited by the FERC would not get in the way of security.

The Cyber Defense Administration should also assume the cyber security responsibility for the myriad civilian federal departments and agencies, all of which are now forced to try to do cyber security on their networks. Also, consolidating in the proposed Cyber Defense Administration what is now done on cyber security by the Office of Management and Budget and the General Services Administration would increase the probability of achieving a center of excellence that could manage security on the government's own civilian (not Defense) networks.



### 3. CYBER CRIME

Because cyber criminals can become rental cyber warriors, we need as the third agenda item to reduce the level of cyber criminality that is plaguing the Internet. Cyber criminals have begun to penetrate the supply chains for both computer hardware and software manufacturers to inject malicious code. Instead of just using widely available hacking tools, cyber criminals are now starting to write their own specially designed code to beat security systems, as was the case in the theft of millions of credit card numbers from T.J. Maxx in 2003. These trends point to the growing sophistication of cyber criminals, and may indicate that the criminal threat could grow to become as sophisticated as the state-level threat. That suggests we need to increase our efforts to combat cyber crime.

Today both the FBI and the Secret Service investigate cyber crime, with help from Customs (now called Immigration and Customs Enforcement, or ICE) and the Federal Trade Commission. Yet companies and citizens across the country complain that their reports of cyber crime go unanswered. The Justice Department's ninety independent prosecutors scattered around the nation often ignore cyber crime because individual cyber thefts usually fall below the $100,000 minimum necessary for a federal case to be authorized. The U.S. attorneys are also often computer illiterate and do not want to investigate a crime where the culprit is in some other city or, worse yet, another country.

The President could assign the FBI and Secret Service agents who cover cyber crime to the proposed Cyber Defense Administration, along with attorneys to prepare cases for the Justice Department. A single national investigatory center within the Cyber Defense Administration, coordinating the work of regional teams, could develop the expertise, detect patterns, and engage in the international

liaison needed to increase the probability of arrest to the point where it might begin to be a deterrent. Today law enforcement in the U.S. does not begin to deter the world's cyber criminals. Today cyber crime does pay. To make it stop paying, the U.S. would need to make a substantially greater investment in federal law enforcement agencies' cyber crime capability. We will also have to do something about cyber crime sanctuaries.

In the late 1990s, international criminal cartels were laundering hundreds of billions of dollars through "banks" in a variety of mini-nations, usually island states, as well as several larger sanctuary nations. The major financial powers got together, agreed on a model law criminalizing money laundering, and told the sanctuary states to pass the law and enforce it. If they didn't, the countries were told that the major international financial nations would all stop clearing their local currencies and halt financial transactions with their banks. I had the pleasure of conveying that message to the Prime Minister of the Bahamas, where the law was promptly passed. Money laundering did not disappear, but it got a lot harder because there were fewer reliable sanctuaries. The signatories of the Council of Europe Convention on Cyber Crime should do the same kind of thing to cyber crime sanctuaries. Together they need to tell Russia, Belarus, and the other scofflaws that they either have to start enforcing laws against cyber crime or there will be consequences. One of the consequences would be to limit and inspect all Internet traffic entering nations from the scofflaw sanctuaries. It's worth a try.

## 4. CWLT

The fourth component of the agenda to address cyber war should be the equivalent of the Strategic Arms Limitation Treaty (SALT) for cyber war, a Cyber War Limitation Treaty, or CWLT (pronounced



"*see*-walt"). The U.S. should coordinate the proposal with its key allies in advance of suggesting it at the United Nations. As the name implies, it should limit cyber war, not seek some global ban on hacking or intelligence gathering. SALT and its follow-on Strategic Arms Reduction Treaty (START) not only accepted intelligence collection as an inevitability, they relied upon it and called for "noninterference" with it. Those treaties explicitly protected what they called "national technical means."

When arms control worked well, it had begun somewhat modestly and then expanded its scope in subsequent agreements as confidence and experience had grown. CWLT should begin by doing the following in an initial agreement:

- establish a Cyber Risk Reduction Center to exchange information and provide nations with assistance;
- create as international-law concepts the *obligation to assist* and *national cyber accountability*, as discussed earlier;
- impose a ban on *first-use* cyber attacks against civilian infrastructure, a ban that would be lifted when (a) the two nations were in a shooting war, or (b) the defending nation had been attacked by the other nation with cyber weapons;
- prohibit the preparation of the battlefield in peacetime by the emplacement of trapdoors or logic bombs on civilian infrastructure, including electric power grids, railroads, and so on; and
- prohibit altering data or damaging networks of financial institutions at any time, including the preparation to do so by the emplacement of logic bombs.

Later, after experience with CWLT One, we could examine whether to expand its scope. We should begin with a no-first-use ban on cyber attacks against civilian targets, rather than an outright ban, because nations should not be disingenuous when they sign

obligations. Nations that are engaged in a shooting war or have been the victims of cyber attack will probably employ cyber weapons. Moreover, we do not want to force nations that have been the victim of cyber attack to retaliate with kinetic weapons because of a ban on cyber attacks. The proposal does not preclude initial cyber attacks on military targets. Nor does it rule out preparation of the battlefield against military targets, because proposals to do so raise complex trade-offs and would overburden CWLT One. Nonetheless, lacing each other's military with logic bombs is destabilizing and we should say publicly that if we discover it happening to us we would consider it as a demonstration of hostile intent.

Non-state actors will be a problem for cyber arms control, but CWLT should shift the burden of stopping them to the states party to the convention. Nations would be required to rigorously monitor for hacking originating in their country and to prevent hacking activity from inside their territory. They would be required to act promptly to stop such activity when notified of it by other nations through an international Cyber Threat Reduction Center. That Center would be created by the treaty, paid for by signatories, and be staffed at all times by network and cyber security experts. The Center could also dispatch computer forensics teams to assist in investigations and to determine whether nations are actively and assiduously investigating reported violations. The treaty would include a concept of *national cyber accountability*, making it a treaty violation if a nation did not stop a threat when notified by the Center. It would also include the *obligation to assist* the Center and other signatories.

The treaty will also have to deal with the attribution problem, which is not just a matter of nations organizing their citizen hacktivists. The hacktivist problem might be addressed by the provisions in the treaty we have just discussed. Attribution is also a problem because nations route attacks through other countries and sometimes actually initiate them from another nation. The Center could



investigate claims by nations that they were not the source of an attack, and it could issue reports to allow the member states to judge if there had been a treaty violation by a particular state. If there had been a clear violation, the states party to the treaty could issue sanctions. The sanctions could range across a spectrum from, at the low end, denying visas or entry to specific individuals, to denying Internet connectivity to an ISP. At the higher end, nations could limit international Internet and telephone traffic flows for a country. The Center could put scanners on the points where traffic from the country came into other nations. Finally, of course, nations could refer the problem to the United Nations and recommend broader economic and other sanctions.

The treaty and the Center would only be concerned with cyber war. It would not become an international regulatory body for the Internet, as some have proposed. Burdening CWLT with that possibility will ensure that it is opposed by many interests in the U.S. and elsewhere. CWLT will not, by itself, stop attacks on civilian targets, but it will raise the price of trying them. The advent of CWLT as an international norm will also send a message to cyber warriors and their government masters that firing off a cyber attack is not the first thing that you do when your neighbor state has made you mad. Engaging in offensive cyber war against another country would become, after CWLT, a major step. Using it against a civilian infrastructure target would be a violation of international law. Nations that signed the CWLT might put in place good internal controls to prevent their own cyber warriors from starting something without proper authorization.

## 5. CYBERSPACE AT MIDDLE AGE

The fifth element of fighting cyber war is research on more secure network designs. The Internet is now forty, entering midlife, yet it has not changed much from its early days. Yes, bandwidth certainly has grown, as has wireless connectivity, and mobile devices have proliferated. But the underlying design of the Internet, which was done without any serious thought to security, is unaltered. Although many software glitches and security issues were supposed to have disappeared when Microsoft replaced its earlier buggy operating systems with Vista and now Windows 7, problems persist with all of the most ubiquitous software programs.

When I asked the head of network security for AT&T what he would do if someone made him Cyber Czar for a day, he didn't hesitate. "Software." Ed Amoroso sees more security issues in a day than most computer security specialists see in a year. He has written four books on the subject and teaches an engineering course on cyber security. "Software is most of the problem. We have to find a way to write software which has many fewer errors and which is more secure. That's where the government should be funding R&D." Hackers get in where they don't belong, most often because they have obtained "root," or administrator status, through a glitch they have discovered in the software. There are two research priorities created by that phenomenon. We have to do a better job of finding the errors and vulnerabilities in existing software, which is a matter of testing in various ways. But at the same time we need to find a process for writing new applications and operating systems from scratch with close to zero defects.

As much as people fear robots and artificial intelligence (without knowing that there are already a lot of both at work today), it may be worth thinking about using artificial intelligence to write new



code. It would mean coming up with a set of rules for writing secure and elegant code. The rules would have to be extensive and iterated with testing. The project would be sufficiently large that it would require government research funding, but it should be possible gradually to develop an artificial intelligence program that could respond to requests to write software. The artificial code writer could compete with famous software designers, much as IBM's Big Blue played against human chess masters. Drawing on the open source movement, it could be possible to get the world's experts to contribute to the process.

The work that was done to create the Internet forty years ago has been enormously valuable, far more so than the inventors ever thought then that it would be. Now the funders of the original Internet should fund an attempt to do something better. Today cyber research is fragmented and, according to a presidential advisory board, cyber security research is dangerously underfunded. Cyberspace also needs a fresh look from designers who are freed to think of new protocols, new ways of authenticating, and advanced approaches for authorizing access, seamlessly encrypting both traffic and data at rest.

There are some signs of renewed life at DARPA (the Defense Advanced Research Projects Agency), which funded much of the early Internet development. After years of abandoning research on the public Internet, things have begun to change. In October 2009, DARPA granted a contract to a consortium including defense contractor Lockheed and router manufacturer Juniper Networks to design a new basic protocol for the Internet. For decades, the Internet has been breaking traffic up into little digital packets, each with its own address space, or "header." The header has the basic *to* and *from* information. The protocol or format for these packets is named TCP/IP (Transport Control Protocol/Internet Protocol). For the gods and founders of the Internet, TCP/IP is as sacred as the Ten

Commandments are to some religious groups. What DARPA is now looking for is something to replace TCP/IP. Shock and horror! The new Military Protocol would allow for authentication of who sent every packet. It would permit prioritization of the packets, depending upon the purpose of the communication. It might even encrypt the content. The Military Protocol would be used initially on the Pentagon's networks, but just think what it could do for the Internet. It could stop most cyber crime, cyber espionage, and much of cyber war. DARPA has no estimated ready date for the Military Protocol, nor any idea about how the conversion process from TCP/IP would occur. Nonetheless, it is just that kind of thinking that could make the Internet secure someday.

We should not throw out what we have until we are sure that the alternative really is better and that the conversion process is feasible. What might that something new look like? In addition to the Internet, cyberspace might consist of many more intranets, but these would be highly heterogeneous, running one of several different protocols. Some of the intranets might have "thin clients," which are not skinny guys looking for a lawyer, but computer terminals that use well-controlled servers or mainframes rather than having an extensive hard drive on every desk. Centralized mainframes (yes, the old mainframe) that, if they failed, would be backed up by redundant hardware at other locations, could manage intranets to prevent security violations and configuration mismanagement at the nodes. The intranets' traffic would run on separate fibers from the public Internet and could be switched by routers that did not touch the public Internet. Data could be scanned for malware and backed up in redundant data farms, some of which would always be disconnected from the network in case of a corrupting system failure. All of these new intranets could use constant scanning technologies to detect and prevent anomalous activity, intrusions, identity theft, malicious software, or unauthorized exporting of data. The



intranets could encrypt all data and require that a user prove with two or three reliable methods who he is before he could access the intranet. If the new nets were "packet switched," as the Internet is now, the user's authenticated identity could be embedded in each packet. Most important, these networks could constantly monitor for and prevent connectivity to the Internet.

A lot of people will hate that idea. Many of the Internet's earliest advocates strongly believe that information should be free and freely disseminated, and that essential to that freedom is the right to access information anonymously. The "open Internet" people believe that if you wish to read *The Communist Manifesto*, or research treatments for venereal disease, or document China's human rights violations, or watch porn online, your access to that information will not be free if anyone knows that you are looking at it.

But does that mean that everything should be done on one big, anonymous, open-to-everyone network? That's how Vint Cerf and others see the Internet, and they'll be damned if they're gonna agree to change it. When I worked in the White House, I proposed something I called "Govnet," a private network for the internal working of federal agencies that would deny access to those who could not really prove who they were (maybe with a special fob). Vint Cerf thought that was an awful idea, one that would erode the open Internet, beginning a trend of cutting it up into lots of little networks. Privacy advocates, whose cause I usually support, hated Govnet, too. They thought it would force everyone accessing the public webpages of government agencies to identify themselves. Of course, the public webpages would not have been on Govnet. They would still have been on the public Internet. But in the face of opposition like that, Govnet did not happen. It is probably time that we revisit the Govnet concept now.

In addition to Govnet for critical functions of the federal government, where else might we want such secure networks? For airline

operations and air traffic control, railroad operations, medical centers, certain research activities, operations of financial institutions, controlling space flight, and, of course (say it with me), for the power grid. All of these institutions would still need an Internet-facing presence off the intranet, to communicate outside the closed community of the intranet. But there would be no real-time connection between the secure networks and the Internet. Indeed, ideally the protocol, applications, and operating systems would be incompatible.

There would still be a public Internet, of course, and we would all still use it for entertainment, information, buying things, sending e-mail, fighting for human rights, learning about medical problems, looking at pornography, and engaging in cyber crime. But if we worked at a bank, the IRS, or the train company, or (say it loudly) the electric company, we would use one of these new secure, special-purpose intranets when we were at work. Cyber war could still target these intranets, but their diversity, their use of separate routers and fiber, and their highly secured internals would make it very unlikely that they could all be taken down. Vint Cerf and those devoted to one big everybody-goes-everywhere, interconnected web won't like it, but change must come.

## 6. "IT'S POTUS"

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

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



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

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

As I suggested earlier, the President should use the occasion of his annual commencement address at a military service academy,

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

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

> The cyber network technology that my nation has given to the world has become a great force for good, advancing global commerce, sharing medical knowledge that has saved millions of lives, exposing human rights violations, shrinking the globe, and, through DNA research, making us more aware that we are all descendants of the same African Eve.
>
> But cyberspace has also been abused, as a playground for criminals, a place where billions of dollars are annually siphoned off to support cartels' illicit activities. And it has already been used by some as a battlespace. Because cyber weapons are so easily activated and the identity of an attacker can sometimes be kept secret, because cyber weapons can strike thousands of targets and inflict extensive disruption and damage in seconds, they are potentially a new source of instability in a crisis, and could become a new threat to peace.
>
> Make no mistake about it, my nation will defend itself and its allies in cyberspace as elsewhere. We will consider an attack upon us through cyberspace as equivalent to any other attack and will respond in a manner we believe appropriate based on the provocation. But we are willing, as well, to pledge in a treaty that we will not be the first in a conflict to use cyber weapons to attack civilian targets. We would pledge that and more, to aid in the creation of a new international Cyber Risk Reduction Center, and undertake obligations to assist other nations being victimized by attacks originating in cyberspace.
>
> Cyber weapons are not, as some have claimed, simply the next stage in the evolution of making war less lethal. If they are not properly controlled, they may result in small disagreements spiraling out of control and leading to wider war. And our goal as signers of the United Nations Charter is, as pledged in San Francisco well over half a century ago, "to save succeeding generations from the scourge of war." I ask you to join me in taking a step back from the edge of what could be a new battlespace, and take steps not to fight in cyberspace, but to fight against cyber war.

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