Cyberwar: How Terrorists Could Defeat the U.S., and Why They Won't

Analysis by The Cryptogon
http://www.cryptogon.com

WARNING: The information contained in this document is intended for educational purposes only. Anyone who attempts to undertake what is described in the "Possible Terrorist Scenario" section will be committing an act of war against the states involved. I am NOT encouraging anyone to carry out what is described in that section. I am exercising my First Amendment right to free speech to make people aware of the dangers posed to the global information infrastructure. Our society relies on these technologies, and an open discussion of the threats to these technologies is necessary in order to defend them.

:. Introduction

I wrote this essay because the Village Voice, like most other publications, is missing the point when it comes to Cyberwar. The Village Voice article (below) paints a pretty grim picture, but, in reality, the situation is much worse due to reasons the article doesn't discuss. My essay will examine the obvious, and almost never mentioned, threats to information systems, and the reasons why I feel the terrorists will not exploit these vulnerabilities.

:. The Real Threat To Information Systems Is Physical

Long ago (1996), I studied information warfare. I learned a fair amount about infrastructure vulnerabilities, low intensity conflict and strategic information warfare. Oooooooh Ahhhhh. Can you tell I read a few Rand Corporation and SAIC documents?

Here is the core of the matter:

If a terrorist group was actually interested in taking down the United States, they wouldn't go for the Lex Luthor style diabolical displays that make for good television. If they were serious, really serious, about delivering a kill-shot to the U.S., they would physically target the computers, and the data communications media, routers and switches that interconnect the networks. I will explain why terrorists have not, and probably will not, do this at the end of this essay.

What I found when I was in school is that the Department of Defense is literally frightened to death about physical information infrastructure attacks because THERE IS NO EFFECTIVE DEFENSE! You never hear about physical vulnerabilities because it's just not allowed to be talked about. It makes sense that Dumbo's Department of Homeland Security is not focusing on the types of things that really could take the U.S. down. There's just not much that any government can do.

All the hoo haa about viruses, hackers, etc. doesn't address the primary threat. The physical nature of information systems is their main vulnerability. If terrorists were to just start breaking shit, we would be in trouble. It's that simple.

:. Possible Terrorist Scenario

The following is the type of scenario for which no effective defense exists. Everyone knows it. The government knows it. The terrorists know it. Even some of the Rand authors refused to deal with this because it made their complex models useless.

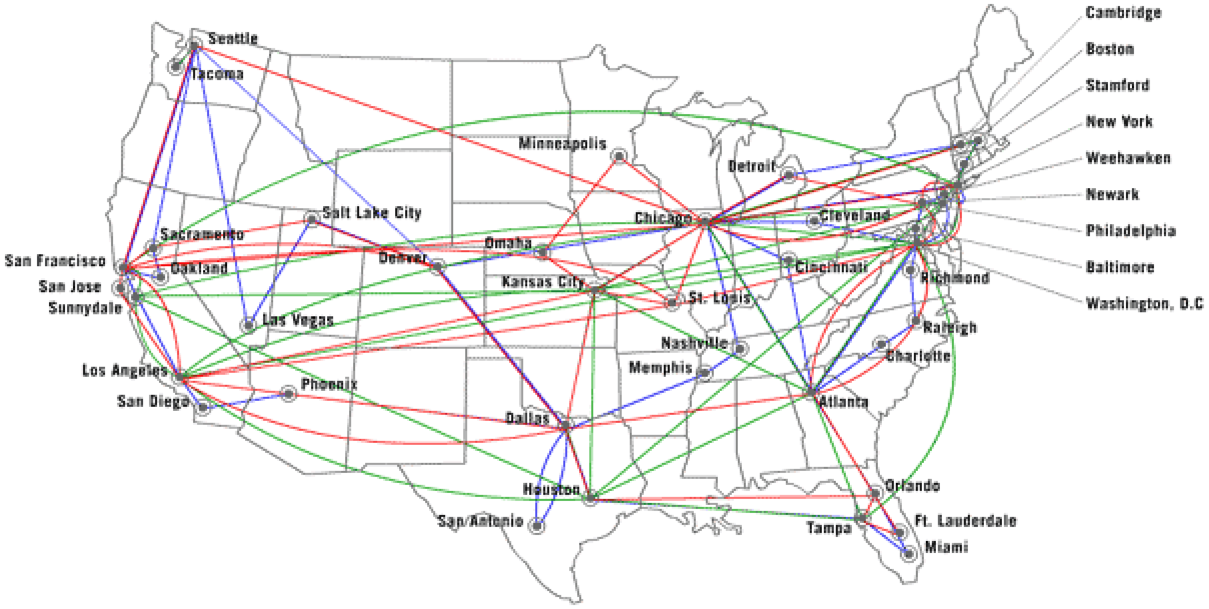
Terrorists use shovels to dig down into the ground until they find conduit that contains fiber optic filaments. They then take axes and begin smashing clean through the conduit. Terrorists will be focusing on the highest prestige targets: OC-192 and maybe even a couple of the bleeding edge OC-768 "fat pipe" connections. An OC-192 is an extremely fast data connection. Each OC-192 carries millions of Internet sessions, emails, phone calls, and financial transactions, simultaneously. OC-768 is generally considered to be the fastest connection, but there are not yet many of these deployed. Here is a speed chart for optical carrier circuits:

Optical Carrier Level	Data Rate
OC-1	51.84 Mbps
OC-3	155.52 Mbps
OC-12	622.08 Mbps
OC-24	1.244 Gbps
OC-48	2.488 Gbps
OC-192	10 Gbps
OC-256	13.271 Gbps
OC-768	40 Gbps

"What!?" you ask, "Many of these cables are buried a few feet underground and sitting unprotected, all over the place?"

Yes. That is correct.

The basic map below shows several OC-192 transcontinental and intercity connections. Different colors indicate different network operators. Company names have been removed:



NOTE: A 21 year old hacker recently obtained a large communications company's SECRET map. That would be the one that shows exactly where all the data pipes are located. Reports indicate that it was a single large pdf file. He obtained the information using nothing but his web browser. He entered the private network through a misconfigured proxy server.

Now that fiber is being sliced, another team of terrorists activates an electro magnetic (EM) pulse weapon inside one or more of a certain company's data centers. This company provides long haul data transport, co-location and dialup services for most of the largest companies in the world. (Company not named on purpose.) Now, another OC-192 is cut. And another. And maybe a few more around the U.S. Without warning, backbone connections in gateway cities such as Los Angeles, San Jose, San Francisco, Denver, Chicago, Washington DC, New York, and Boston are going down simultaneously.

Maybe the terrorists will also target undersea cables where they come ashore in Japan, California, New York, and various places in Europe. Now, on the nodes that are still alive in the U.S., terrorists unleash a few hundred zombie boxes that start a systematic denial of service (DOS) attack on any machine on a different network that can still respond to requests. For added effect, the terrorists make sure the zombie boxes are located on VERY fast networks, such as those found in universities and corporations.

As a backup to insure chaos, a few more EM pulse weapons blow some backbone routers (that have already had their fiber links severed). So, now we have cut fiber and blown core routers. *I’m shaking my head because the thought of this is truly frightening* At this point, the Pentagon would have to get involved. The president would declare a state of emergency. Note: 80% of military communications use public information infrastructures (most of which are now either down or hopelessly jammed with traffic).

The military does, however, have physically hardened, isolated and classified networks that probably would not be affected by the wider chaos.

Think it couldn't get any worse? Maybe the terrorists start taking out some or all of the thirteen root domain name server systems (I think there are still 13) or interrupting communications to those root servers. (Thankfully, a couple of these systems are located in places that have people with guns guarding them.) These root servers are used by thousands of other lower level domain name systems and receive about 300 million requests per day.

Domain name systems are used to translate human readable URLs, like **www.cryptogon.com** into machine usable IP addresses like 209.115.132.59. There is much concern about the root DNS systems. Many articles on this topic are easily accessible. Much of the concern, however, is focused on hackers DOSsing the root servers. Again, this misses the point.

What is the physical security like at the non-military root DNS facilities?

I’ve driven by one of the buildings hundreds of times because I used to live near it. It looks just like any other small office building. How long would this place hold up against a few armed terrorists who were willing to die TO BRING DOWN A ROOT DNS NODE? Think about it. The same goes for the data centers mentioned previously. Surely these places should have armed security. But even if they did, are they prepared to stop terrorists who have no intention of ever getting out alive?

:. How Would The Terrorists Know Where To Attack?

Oh, but the terrorists would need to know where all these Achilles heels are located. That information must be hard to find.

Please. Don't make me laugh. One can find the locations of the root DNS facilities within seconds. As for fiber locations, I just did a casual search and HIGHLY detailed maps are plentiful and in plain view. I'm even more concerned than I was before I started writing this. The situation has gotten much worse since I was in school, not better. I just closed the webpages I was looking at. I didn’t want to know any more information.

For the terrorists, targeting information that couldn't be gleaned from open sources could be bought, stolen or maybe even found in the trash. Read about how intelligence agencies recruit officials of foreign governments. How hard would it be to compromise a janitor, network engineer, middle level manager, etc? Not hard. But such underhanded behavior probably wouldn't even be necessary since so much of the data is just sitting out there in the open.

:. Implications

The nightmare scenario above would collapse the world economy in a matter of days. No nukes. No chemical or biological weapons. The reality is that if some group accomplished 10% of what is described above, things would start to get VERY interesting in a hurry.

You always hear that the Internet was designed to route information around dead or crowded nodes. Well, what you don't hear is that this theory only applies when the amount of traffic on the system DOES NOT OVERWHELM the routers, switches and communications media. If transcon and intercity OC-192s and OC-768s start going down, the sudden traffic overflow onto the lower tiered intercity connections will bring everything to a grinding halt. Couple that with attacks on root DNS nodes and DOS attacks on systems still standing…

Put a fork in it, ladies and gentlemen. It's done.

Present this scenario to a room full of generals, computer experts, spooks, etc. and you would see a lot of thumb twiddling and blank gazes. My guess is that scenarios very similar to what you have just read keep a lot of people inside the government awake at night.

Another thing you don't hear about is that service providers are running their networks at or near capacity in order to avoid buying expensive equipment and additional fiber paths. So, what happens if a terrorist group takes out some backbone connections and key intercity links? The networks, already running at near maximum capacity, will get overloaded, thus preventing the vast majority of users from reaching their destinations. Again, put a fork in it. Watch what happens when Slashdot posts a link that sends hundreds of thousands of users to a low end web server on a slow connection.

What does all of this mean to the man on the street? The short answer is, the sun will still rise, the birds will still sing, but that's about it. Try to get cash from an ATM. Try to make a phone call. Try to drive your car on city streets with no working traffic lights. If you're a trader on Wall Street, try to fill orders. Oh, woops, you wouldn't have any orders... I think you get the picture. How long could this kind of scenario go on, nationwide, before the implications became global? Oh, woops, a few hours into that situation and soldiers are already deploying on a street corner near you...

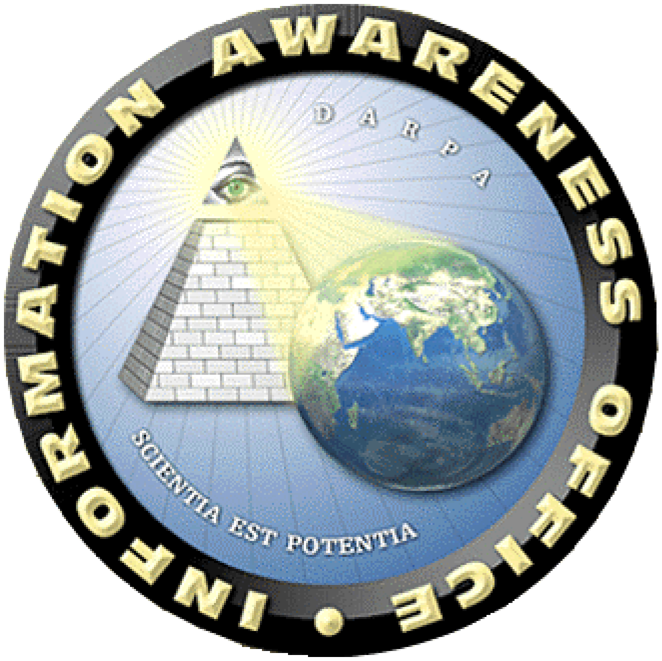
The imbeciles on the boob tube seem to mention airport security quite a bit. How often do you hear about vulnerabilities of fiber optic cables and data centers. How often do you hear about EM pulse weapons!? Or the fact that such weapons can be built for about $400? When was the last time you heard one of those painted-up, cable tv whores (male or female) discussing root domain name servers? *laughing*

Food for thought.

:. The Ties That Bind The Elite To The Terrorists

Now that I've laid out the nightmare scenario that could actually bring down the U.S., let me explain why I DON'T think it will happen. The elite (bankers, manufacturers, media and the governments that serve them) need the Internet. They can't move trillions of dollars around per day without the Internet. What happens to the richest country in the world without its money? Remember, today, information equals money. You take away the information, you take away the money. You take away the flow of information, you take away the flow of money. Terrorists who knock down buildings, kill lots of people and make lots of smoke, fire and noise serve the interests of one group of people: The elite.

They also want to use the Internet to monitor the levels of public dissent and have created an organization called the Information Awareness Office to do so. One look at the logo should be enough to indicate the nature of this agency. And no, that logo isn't a joke:



If you would like to know more about the Information Awareness Office, please see my essay on it below.

Given the usefulness of the Internet (moving money and spying on people), I think there is a covert connection between various elite factions and the top echelons of "international terrorism." If this connection didn't exist, and if the terrorists actually wanted to destroy "Western Civilization," why haven't they? You just read how they could do it above. Why have they instead perpetrated a stunningly visual and public act of terrorism (9/11) that will only serve to increase the power of their alleged enemy, the United States Government? Why not strike at the enemy's money (information) and its ability to move money (Internet)? Because the terrorists serve at the convenience of the elite, and the Internet is too valuable as a money moving and dissident tracking system. While this may sound totally ridiculous to many, such an arrangement would explain a large number of things. Try to imagine the current draconian policies and expansionary wars going forward without the 9/11 incidents.

Do you see what I mean? The police state clamp down and ridiculous wars for resources wouldn't be possible on the scale required. When one thinks about the situation in those terms, the end of terrorism would be last thing the elite would want. Terror drives the citizenry into the waiting arms of the government. This makes the job of the intelligence agencies much easier. They know most people are afraid for their lives, afraid to speak out and just plain dumb. The spooks are then free to focus mostly on dissidents who realize that the entire God damn thing is a fraud.

"For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill."

---Sun Tzu, *The Art of War*

Although I don't agree with what these people are up to, my hat is off to them. One can't help but to have some amount of respect for the diabolical genius of this. The elite finally woke up and grokked the core philosophies of the East and combined them with the military might of the West. Unfortunately, they're using their insights to enslave the planet. The people of the world don't even know they're at war, or who the real enemy is.

-END-

WARNING: The information contained in this document is intended for educational purposes only. Anyone who attempts to undertake what is described in the "Possible Terrorist Scenario" section will be committing an act of war against the states involved. I am NOT encouraging anyone to carry out what is described in that section. I am exercising my First Amendment right to free speech to make people aware of the dangers posed to the global information infrastructure. Our society relies on these technologies, and an open discussion of the threats to these technologies is necessary in order to defend them.

NOTE: I locked this file to minimize the chances of reposting without the disclaimer. I don't want the suit wearing goons knocking on my door with a printout of what I discussed above, minus the disclaimer. If you're smart enough to pull text out of this file, and you freaks know who you are, I only ask that you please be sure to include the disclaimer if you repost this information. ☺ Thanks.

The Threat of Cyberwar Looms Large. Our Best Homeland Defense May Be Surprisingly Small.

Virtually Helpless

by **Josh Martin**
September 11 - 17, 2002

(illustration: McKibillo)

The next time this country is targeted by terrorists, the primary weapon may be an object no bigger than your thumbnail: a computer chip.

Without bombs, bullets, or missiles—without even setting foot on U.S. soil— cyberterrorists could disable the nation's phone systems, plunge cities into blackout, sever water supplies, scramble military communications, steal classified files, clog emergency-response lines, cripple highways, and ground planes. By commandeering vulnerable home PCs and using them to bombard the servers that make modern life possible, they could shutter our markets and take out key links like the Federal Reserve, which every day transfers $2 trillion over the wires. With a few keystrokes, they could wreak damage on a scale not easily imagined, and for pennies on the dollar.

The best intelligence suggests that the next major military strike by the Bush administration, now drumming up support for an imminent war on Iraq, will draw in response an equally intense virtual assault. A report by Dartmouth College's Institute for Security Technology Studies examined cyberwar overseas—with particular attention to the conflicts in Serbia and the Middle East—and concluded that virtual onslaughts "immediately accompany physical attacks." By the logic of that analysis, if Bush moves on Saddam Hussein after the midterm elections, we would see the first full-on blitz before Christmas.

It's not as though the White House lacks all understanding of the danger. Last week, Bush officials brought to the readjourning Congress a plan to create a cabinet-level Department of Homeland Security. Lawmakers are weighing the president's request to provide the agency with $38 billion next year. But of that sum, only $364 million—less than 1 percent of the total budget—would go to shield the nation's most vulnerable front.

This low funding level reflects in part a faith in larger computer security investments by the Defense Department ($10 billion and climbing fast) and the private sector (especially banks, financial services, media, and other technology-dependent industries).

The real problem, critics argue, is that the feds won't, or can't, deal with America's agile, innovative, and occasionally criminal hackers—the experts with the street experience and technical know-how to prevent a catastrophe. Instead, most Homeland funds are going to what one cyberwar expert calls "the usual suspects," the same big players who built our now-endangered infrastructure: large, slow-moving defense contractors like Northrop

Grumman, Raytheon, and SAIC, mainline academic institutions, and established think tanks like the Rand Corporation.

"The concept of 'homeland security' is essentially retarded," says Michael Wilson, a former hacker and current partner in Decision Support Systems Inc., a Reno, Nevada-based consultancy advising sovereign states, companies, and the ultrarich about dealing with cyberwar. "The contracts are going to the very people who got us into this mess to begin with. None of them can tell you what the current cyber-threat is, and they don't know what to defend with."

Too young, too radical, and too often freighted with checkered pasts, hackers are a breed of cyberwarrior no government agency feels comfortable with. Because so few among the hacker ranks would even pass the first level of security clearance background checks, the feds are trying to manufacture their own, through programs like the Cyber Corps. Set up by President Clinton, it now trains students on six campuses in the defense of government institutions. Similar efforts to develop in-house cyberwarriors have been launched by the CIA, the FBI, and each branch of the nation's armed forces. But all these efforts are falling short. The federal government estimates it needs 100,000 computer security pros, up from the 37,000 thought necessary a year ago. Today, the entire Cyber Corps program has just 66 students.

Recognizing the failings of a conservative approach, some major defense contractors are in fact reaching out to "white-hat" hackers. "I don't deal with folks who are dancing too close to the line," says Adelle McIlroy, security practice lead with Internal Network Services, a spin-off from Lucent Technologies. "I look for someone who has learned their skills in the military. If they have a criminal history, I wouldn't hire them. I look for the ones who are smarter than thieves but who are not thieves themselves."

McIlroy believes the system will have to change, embracing more hackers to provide an effective defense. "Government agencies are going to have to change how they think, to be more adaptive," she says.

This view is an exception to the rule. Consider the response of one Raytheon spokesman: "There's no requirement to change. We believe we have the people to make it work."

Such breathtaking smugness, combined with the ease with which a cyberattack can successfully be launched, should be giving New York City officials the willies.

New York is the number one target of any retaliatory strike, because it remains the pre-eminent symbol of America's economic and technological might. From a cyberterrorist's perspective, it might not be an entirely open city—demand for computer security is growing fast—but it is still all too vulnerable. Every pipe out is potentially a crack for enemies to exploit. With DSL and cable connections quickly growing more popular, New York ranks among the top 25 cities in the nation for household Internet access. The city's financial, media, and entertainment industries could not exist without the servers and routers ordering the data, tracking and transferring money, and connecting us with the world beyond. New York is second only to Los Angeles in number of Web sites registered, and it has almost twice as many high-speed links as any city on the planet.

It is all very impressive. Yet none of the systems upon which the city's economic life depends could withstand the major denial-of-service attack terrorists are now capable of delivering. "The odds of some kind of cyberattack have gone from probability to a certainty," says Fred Rica, a threat-assessment guru with PricewaterhouseCoopers, LLP.

The question is, what scope of attack should the city expect? Rica's answer: Prepare for the worst.

Opening skirmishes have already taken place. "Banks and financial service organizations are experiencing a lot of benign attacks on the parameters of their systems," says Steve Buerle, security practice director with ThruPoint, Inc., one of the country's leading cyber-detective agencies.

Indeed, while no overt cyberwar has been declared on the U.S., the country's defenses are clearly being tested. According to officials at CERT (the federally funded Computer Emergency Response Team, based at Carnegie Mellon University), the number of "incidents"—cases of malicious hacking—is growing rapidly. Between 1994 and 2001, the yearly number of virtual break-ins at the country's defense agencies grew from 225 to 40,076. Breaches at private companies and other government agencies grew at only a slightly lower rate, increasing from 2340 to 52,658.

The Bush administration has made several attempts to set up meaningful protection, such as the Federal Computer Incident Response Center and the Cyber Warning and Information Network. But the very nature of cyberwarfare puts large and complex organizations—private or public—at a disadvantage.

As a result, although most computer systems now in place in New York's major private and public institutions have some form of protective software, almost all of them are sitting ducks. Rica points out that part of the reason for this is that as systems age, they become more vulnerable. Moreover, even when new defensive software is available, companies and agencies don't always have the money or the inclination to buy in.

Cheaper and faster are the hackers, people Michael Wilson says should be deployed to defend the city and the nation at large. "We've been relying on people in the spook establishment who have an arm's length of clearances and are ostensibly squeaky clean, but it just doesn't work," he says. "For you to be any good in this area, you have to have done moves on the street. But that kind of person can't pass clearance tests."

Others agree. "We need to treat hackers today the way we treated German rocket scientists after World War II," says John Arquilla, senior consultant with the Rand Corporation. "Hackers can be cultivated rather than punished. They are an underutilized resource."

Much of that resource waits untapped, right in the heart of Gotham. "New York has the world's largest hacker community," says Wilson. Of the 1000 top hackers in the world, he believes 20 are to be found here in the city, along with between 200 to 300 cyberwarriors known as "script kiddies." Those numbers might sound small, but in cyberwarfare, every hacker is an army.

Commissioning a major defense contractor to craft a response to cyberwar is like sending a tank to do the work of a scooter. "The U.S. defense establishment is trying to instill a mindset that is inherently foreign to the people they've selected to do the job," warns Wilson. "You need to build a defensive organization that can react like a 14-year-old."

Indeed, organized military response has been shockingly poor, at best. Despite the $1.6 billion the Pentagon spent on computer defenses last year, the General Accounting Office recently blasted the DOD for having networks "beset by vulnerabilities." When the Defense Department tested itself, it held an exercise in which teams from the National Security Agency used hacker programs to break into 36 Pentagon computer networks and nine city power grids and 911 systems, all at once. According to one source close to that exercise, Pentagon systems administrators were able to detect just two of the mock attacks.

There have also been real incidents in which only a dose of perverse luck prevented disaster. During the Gulf War, Dutch hackers stole information about U.S. troop movements from Defense Department computers and tried to sell it to the Iraqis, who thought it was a hoax and turned it down.

That case shows how hard it can be to predict who will try to break in. But correctly identifying the attacker is as important as knowing what systems are being bombed. In 1998, more than 500 Pentagon computer systems were compromised in a series of attacks code-named "Solar Sunrise." The assault was first thought to have originated in the United Arab Emirates but later found to have been the work of a couple of California high school students and their 17-year-old Israeli mentor.

Homeland Security will have to move quickly to distinguish a serious foe from a juvenile pest. And it will need to make a realistic determination of who is capable of launching an attack in the first place.

Bush administration efforts to show that Al Qaeda terror cells are planning to launch cyberattacks against the U.S. may appeal to public imagination, but there has been little indication that Osama bin Laden has the cadre of geeks needed to launch such an operation.

Still, plenty of others have the resources to pull it off. Intelligence agencies have identified 20 countries and two dozen terror rings that are developing cyberwar technology. Among them, the U.S. ranks first in terms of money being invested. The list of other players includes both friends and enemies: China, Russia, France, Germany, Israel, Iran, Iraq, Libya, Cuba, Britain, France, and North Korea. Groups known to employ cyberweapons range from Hamas in the Middle East to Chiapas rebels in Mexico to the Falun Gong in China. There are also well-financed private cyberarmies mustering in Pakistan, India, and Germany.

In this form of warfare, both the generals and the soldiers are marked by extreme youth. The jargon reflects this. In addition to being called script kiddies, frontline attackers are known as "ankle biters" and "packet monkeys."

Some computer experts denigrate these more minor players. "They don't have to be very intelligent," says John Hale, a computer science professor who works with the Cyber Corps program at the University of Tulsa. "These hackers use scripts other people write."

The hacker community has other weaknesses. Its members are often their own worst enemy. "Hackers can expose and break into things, but they aren't necessarily good at making something work," says McIlroy, of Internal Network Services. "A person committing the crime of breaking in isn't always expert in defending. Besides, the question isn't how to defend a system, but how to make it unbreakable."

Though that question may have no answer, the strongest hope lies with pulling in all available minds. Cyberwar is not a game for the shortsighted. Some argue the long-term fallout from a potent assault would be even more devastating than the virtual battle itself. John Adams, a well-known defense expert and former Washington correspondent for the London *Sunday Times*, recently wrote that cyberwar technology "is capable of deciding the outcome of geopolitical crises without the firing of a single weapon."

And just as the effects of an atom bomb linger for generations, so a cyberwar could unleash a host of viruses, worms, and Trojan horses that defy the best defense efforts long after the fighting has ended. Already, there are some 30,000 hacker-oriented sites on the Internet, bringing the tools needed to wage cyberwar within the reach of even the technologically challenged. The array of weapons is vast and growing. According to ICSA Labs, more than 50,000 computer viruses have been created, and up to 400 are active at any one time, with over 10 new ones released every day.

In the end, the Department of Homeland Security may fail in its mission because it is reactive rather than proactive, seeking to influence events from on high rather than from the ground level, where effective control can determine the outcome of cyber-conflict. Left unprepared, New York—and the country—could find itself the victim not simply of a cyberattack, but of an utter failure of governing elites to see the writing on the wall.

-END-

Research Credit: JH

7/19/2002

High Priests of the Technocracy: The Information Awareness Office :.

Since the end of the Cold War, governments around the world have been increasingly viewing their own states' populations as threats to national security. What we are now witnessing is a struggle for control of ideas. The battlespace is the Internet.

In current national security parlance, terrorists, individuals, non-governmental organizations and other actors are considered asymmetric threats. When compared to state actors, asymmetric actors exhibit a marked lack of congruence in terms of military power. What the non-state actors lack in military muscle, they make up in speed, agility, intelligence and personal conviction. In the story of David and Goliath, David was an asymmetric threat to Goliath. Today, lots of individuals armed with information technology and brain power pose a similar threat to the established order.

Clearly, the U.S. government is frightened.

They're not just scared of terrorists. Think back to the circumstances that touched off the American Revolution. Now start thinking about the endless string of trillion dollar swindles that have been accelerating over the past twenty years. The degree of corruption and high level criminality under way today makes the circumstances of, "Taxation without representation" seem desirable in comparison. The fraudsters running the show realize this, and they also know that people are waking up, discussing issues, sending email, creating websites and reading websites, etc.

In order to keep such a large genie in the bottle, the U.S. government needs a new way to view the threat. Over the last twenty years or so, several states, lead by the U.S., implemented the ECHELON surveillance system. Today, those efforts have resulted in an overabundance of raw data; much more data than can be analyzed effectively. The government wants to be able to spot definite patterns in what looks like noise on top of noise. They want to unravel the structure of loosely organized networks of individuals. In other words, they want to use the Internet---the tool which has the potential to set us all free---to track some of us down and silence us when we become too much of a threat.

The Information Awareness Office is brand new and is lead by John Poindexter. Remember him? His **CV** states that, "He was directly involved in implementing The President's policies on a strong defense, freedom and democracy around the world, human rights, world hunger, economic and military assistance." However, it fails to mention his multiple felony convictions. Woops. I think **Wired** sums the situation up pretty well:

John Poindexter, head of the Pentagon's new data mining service, the Information Awareness Office.

Master of Delete: After serving as Reagan's national security adviser during the Iran-Contra scandal, Poindexter was found guilty of five felony counts (later overturned on a technicality), including obstructing Congress by erasing more than 5,000 incriminating emails.

Data Hunter: In January, Poindexter, 66, was tapped to lead the IAO. The office, funded by Darpa, works to counter "asymmetric threats" (such as terrorist cells) with IT solutions. It's building a prototype system for collating billions of previously unconnected data points - everything from the classified files of lone-wolf agencies like the FBI, CIA, and DEA to personal Internet communications and credit records.

Now, last, but definitely not least, if you thought the **logo for the Babylon project** was good (used to be **here**, but it has been removed, see **google cache**), wait until you see the logo for the Information Awareness Office. Yes, friends, that's the, "All Seeing Eye" of Illuminated Free Masonry's fame. Yes, the same one that's on the back of your one dollar bills. These guys are out of the closet now. They're in control, they know it and they're not afraid to show it. The Latin phrase below the symbol, "Scientia Est Potentia," means, "Knowledge is Power." Also, notice the part of the world that's indicated in the symbol, Central Asia, the region which has been targeted for imperial occupation because of its rich oil and natural gas deposits.

TR submitted this very interesting information:

Subject: Scientia est potentia

These guys at the Information Awareness Office either don't know their Latin very well, or they are being blantantly evil.

Potentia means power but it has the connotation of unconstitutional private power. Power attained by private means and used for personal ends. What they should say is "Potestas." This is power attained by and for the public good. As in this famous quote by Francis Bacon: Ipsa scientia potestas est. Knowledge itself is power.

In my copy of the "New College Latin and English Dictionary" potentia is defined as: "force, power; political power (esp. unconstitutional power)". Whereas potestas is defined as: "power, abililty, capacity; public authority, rule, magisterial power; possibility, opportunity, permission..."

So by saying "Scientia est potentia" they're just coming out and saying, "Knowledge is unconstitutional political power for a few private individuals." Sounds about right to me. Maybe they do know their Latin after all.

-END-