Testimony for the
Committee on Government Reform's Subcommittee on Government Efficiency,
Financial Management and Intergovernmental Relations

Cyber Terrorism and Critical Infrastructure Protection

July 24th, 2002

Douglas Thomas
Associate Professor
Annenberg School for Communication
University of Southern California
Los Angeles, CA 90089-0281

douglast@usc.edu

Good morning and thank you for inviting me to speak before you today. My name is Douglas Thomas and I am currently an Associate Professor in the Annenberg School for Communication at the University of Southern California. My research focuses on the social and cultural impacts of new media and technology, with a particular emphasis on the subculture of the "computer underground." I have recently published one book, *Hacker Culture*, about the computer underground and co-edited another, *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*, which explores a broad range of security issues from an international and comparative perspective. I have spent the past 7 years studying computer hackers, in an effort to better understand who they are, what motivates them, and how their culture can be understood in relation to technological innovation. During that time, I have met with, spoken to, and interviewed hundreds of computer hackers. I have spent time immersed in their literature and their culture and I feel confident in saying that I believe I understand, for the most part, how hackers think.

I want to address the question of our vulnerability, but I wish to do so from a perspective that you may have not heard before.

I'd like to start off by answering the broad question: what are the risks that a terrorist organization might seek our hackers and employ them to carry out attacks on our information infrastructure? With the vast majority of hackers, I would say 99% of them, the risk is negligible for the simple reason that those hackers do not have the skill or ability to organize or execute an attack that would be anything more than a minor inconvenience. Granted, hackers often have an antagonistic (and often times juvenile) response to authority, often producing behaviors that appear to pose a troublesome threat. As Steven Levy pointed out in his discussion of the role that hackers played in the creation of the PC and the information revolution, a central tenet to the "Hacker Ethic" has always been a profound mistrust of authority. Accordingly, today's hackers break into NASA and the Department of Justice web servers and rearrange their web pages. Occasionally, they even engage in Denial of Service attacks that make web sites inaccessible for brief periods of time. In short, they engage in behaviors that are typical of adolescent boys, challenging adult authority and flexing their muscles (in this case via technology) in the ways that young men (and in a relatively few cases, women) have done since time immemorial. It is a kind of vandalism that is and should be illegal. And when laws are broken, hackers should be caught, prosecuted and punished. But in times such as these, it becomes critical to ask ourselves what exactly the impact of computer hackers' behaviors is. Are these things annoying? Yes. Are they juvenile and occasionally embarrassing? Often. But are they dangerous? I don't think so. Certainly not at the level that you want to be discussing here today. I do not believe that terrorists are likely to attack us by knocking E-Bay offline for a few hours or that such an attack would constitute an act of cyberterror.

Of the hackers that remain, my experience suggests that the most talented, who may be able to inflict serious damage, are neither inclined to do so nor likely to be tempted by financial incentives. They tend instead to be the most strongly motivated by an ethic which values security, which values information, and which puts innovation and learning at the top of their list of priorities. In other words, the idea of engaging in terrorism, of any sort, does not fit their profile.

Here, it also might be of some use for me to discuss the hacker psychology. The typical hacker, and of course there are exceptions, is motivated by a profound sense of curiosity. Hackers like to know how things work and they like to make things work better or in unexpected ways. And while it may be convenient to divide the hackers of yesterday, such as Steve Jobs, Richard Stallman, Steve Wozniak, and Linus Torvalds from the hackers of today, doing so misses an important commonality. Hackers like innovation. They like identifying and finding elegant solutions to complex problems. Like the hackers of yesterday, the hackers of today have a very clear ethic that shouldn't be overlooked by this committee: Above all else, they too believe in computer security. And, most important, they believe that without constant vigilance most software manufacturers will remain content to leave security as a secondary issue. They believe that in most computer software used today, *security has become an "add on" feature rather than a design principle and it is that, above all else, which puts us at risk.*

In our new age of corporate responsibility, it may be worth taking a few minutes to examine one of the primary reasons that hacker are seen as threatening and why we might be quick to make associations between hacker activity and terrorist activity. Most of what hackers do is write programs that *expose security flaws* in computer software, mainly in the operating systems produced by Microsoft and to a lesser degree by Sun Microsystems. That process of hacking has been responsible, particularly over the past decade, for alerting the public and security professionals to major security flaws in software. What hackers see as a public service, pointing out dangerous and troubling security risks, many people see as criminal activity. Many public releases of security holes came as a result of companies refusing to fix (or even acknowledge) security flaws in their products because *there is no regulation for security in software, and most important, there is no liability for software companies when their products create risks for consumers*. At one level, the work that hackers do is not entirely unlike the work of a watchdog organization or *Consumer Reports*. Admittedly, the outlook, style and demeanor are different, but the end results are the same. Hackers force computer software manufacturers to pay attention to security. They find security flaws, and when they point them out, we tend to associate hackers with the flaws, rather than placing responsibility with the corporations that write and sell bad software. We need to be careful to focus on the causes of such vulnerabilities and to not blame the messengers.

When facing a question as weighty as cyberterrorism, a very serious problem that you face is getting the facts. Almost everyone that you talk to has an investment in inflating the risks and the dangers that hackers pose. Everyone, hackers included, are invested in telling you that the threat is much worse that it is. Cyberterrorism is a term that is bandied about with increasing frequency, but it is also one that has almost no meaning. I have yet to hear anyone articulate a realistic scenario in which computer hackers would be able to effect significant economic or physical damage in order to be considered a "terrorist" threat. It is easy to imagine scenarios that sound like terrorism: For example, hacking into air traffic control and crashing planes, or hacking into the New York Stock

Exchange and undermining the Stock Market. These things make great Hollywood plots, but there is no evidence that any such scenario is possible, much less likely. In fact, most of the research I am familiar with in this topic concludes just the opposite.

Cyberterrorism is a lot more difficult than many people assume. Because a power plant has a website, for example, does not mean that one could access controls for that power plant online. In most cases, in order to control the operation of a power plant, you must be *physically* inside the power plant. You would need to enter the building and sit down at a computer terminal. Such power plants are not controlled or accessible through the Internet or dial up modems. One cannot "hack" that power plant and shut it down. It is technologically, physically, and in every other way *impossible*. Systems that are well designed should all have similar access barriers, such as independent, non-public networks, physical barriers and sophisticated authentication and encryption schemes. Such access barriers make it extremely difficult to even reach places where damage might occur and will protect our most critical information infrastructure assets.

Furthermore, even if you were to assume that a hacker had the ability to hack into one of our nation's critical infrastructure assets, he or she would also need expertise in some other area, such as power plant management, air traffic control, or banking. Absent the expertise to effect some significant and targeted attack, even access to these systems would be of limited threat potential.

Also, most of our critical infrastructures are monitored and require human control to function. People tend to notice when things look suspicious. We may feel as though computers have come to control every aspect of our lives, but the reality is that humans still exert primary control over all the most important aspects. For example, if you looked at your schedule for the day and saw the entry "12:30: Jump off a bridge," you are not likely to follow that instruction, even if it is in your Palm Pilot or Outlook calendar. On the face of it, there is something wrong with that information and you become suspicious.

For the foreseeable future, acts of cyberterrorism, such as the ones usually imagined, will be very difficult to perform, unreliable in their impact, and easy to respond to in relatively short periods of time. In point of fact, there has never been an act of cyberterrorism committed, nor has there ever been, to my knowledge, a computer hacking incident that has resulted in the loss of life.

When these scenarios are proffered, I urge you to ask the tough questions about them. What additional security measures would have to fail for such an attack to take place? Scenarios that begin with the phrase, "First, a hacker breaks into an air traffic control center . . ." cannot serve as the basis for policy decisions about terrorism any more than "First, someone steals all the gold out of Fort Knox . . ." can serve as the basis for regulating decisions about banking. Before acting on these sorts of threats, we must be certain that these threats are grounded in some sense of reality. Take, for instance, the most frequently cited example of interference with air traffic control. Air traffic control systems are not readily accessible and, more to the point, they don't actually control anything. They provide radar data to controllers who use radios to direct pilots. Even if a terrorist were able to get access and cause interference the human control measures, air traffic controllers monitoring the flights, and pilots flying the planes, on board radar, etc. would detect and correct for problems immediately. In practice, such an attack would be exceedingly difficult to carry out, if not because of access difficulties, because of the human control elements which provide an additional layer of security that is difficult to circumvent. By extension, then *every critical system should have safeguards in place, so that if something suspicious happens, it can be monitored and corrected.*

It is imperative, in turn, to understand security as a multi-layered process. How specifically would such an attack happen? This is the single most important consideration. Idle speculation is easy. Detailing the plan for such an attack is much more challenging. Do not assume that anything of vital importance is connected to the Internet. Just because a system is "networked" does not make it accessible through the Internet or even accessible from the outside at all. What kind of access would be required to cause such a catastrophe? I assure you, the threat is not a 16-year-old, with a Dell laptop hacking from his bedroom. In most cases, you will find that an attack would require someone to physically invade a space and get control without anyone noticing as well as requiring a detailed knowledge of the location and organization being attacked. *Therefore, our focus, through projects such as that National Infrastructure Protection Center, should be on controlling, regulating, and safeguarding access to these points. There is no substitute for a well designed system that controls access to critical systems.*

One of the great challenges you face is getting accurate, reliable information, both with respect to hackers and with respect to the computer and security systems that may be targets for attack. Hackers tend to exaggerate their own abilities out of a sense of bravado. And while there are hackers who can do damage to systems, disrupt e-commerce, or even force web sites offline, the vast majority of them can't. The ones who can, generally, don't.

Hacking stories make good copy, but they are very rarely accurate, tending to exaggerate threats and downplay the realities of the event. There is a big difference between hacking into NASA's central control system (which has *not* happened) and hacking into the server that hosts their web page (which has happened repeatedly). Most media reports fail to distinguish between the two (or to explain that hacking a web page is essentially the same as spray painting a billboard, posing very little actual risk). The media, moreover, tends to exaggerate threats, particularly by reasoning from false analogies such as the following: "If a 16 year old could do this, then what could a well funded terrorist group do?" The reality is that there is very little that a well-funded terrorist group could do that a 16-year-old hacker couldn't. And neither of them threatens us in a way that can rightly be called "terrorism."

Law enforcement, security consultants, and even software corporations are all highly motivated to embrace similar outlooks. It is to their advantage to have you believe that the threat to our nation's security is severe. Almost no one has any investment in a more balanced, nuanced, and complete perspective. It is that perspective that I hope you will seek out as you work to assess vulnerabilities and identify solutions.

My last comment has to do with what we might think of as a worst case scenario. Should an extremely talented hacker, who violates the ethic of hacking, manage to get access to a critical system, bypass all security measures, and launch an attack unnoticed by those monitoring the situation, it should be noted that this country has some of the best resources available to it to deal with, diffuse and neutralize such a threat. The faculty and students at places like MIT, UC Berkeley, Stanford, Purdue and Carnegie Mellon as well as organizations such as CERT and the National Computer Security Association provide our best defense against such threats. But these groups only provide that advantage as long as the network is open and accessible. *Security only gets better through testing, design, and redesign. The real threat to security is closing off avenues of exploration and examination. The more we know about our networks, the better we are able to defend them.* The more we know about the network's flaws, the better able we are to redesign it to eliminate these flaws. Testing our networks, probing them and finding those flaws is the only way in which we can be sure that they remain safe and secure and maintaining their openness is the only way to assure that if the worst does happen, that we can respond immediately, directly, and effectively.