Testimony of

Mr. Dan Verton

February 24, 2004

Feb. 24, 2004

Statement for the Record of
Dan Verton
Author, Black Ice: The Invisible Threat of Cyber-Terrorism (McGraw-Hill/Osborne, 2003)

On
"Virtual Threat, Real Terror: Cyberterrorism in the 21st Century "

Before the
Subcommittee on Terrorism, Technology and Homeland Security
United States Senate Committee on The Judiciary
Washington, D.C.

Good afternoon Chairman Kyl, Ranking Member Feinstein and Members of the Subcommittee.

I want to thank you for the honor of appearing before you today to discuss what I believe is an urgent national security matter and I applaud your leadership in this area.

Although I do not consider myself a technical expert, I have a professional background in intelligence and information security, and I'm the author of a recently published book by McGraw-Hill titled Black Ice: The Invisible Threat of Cyber-Terrorism that goes into detail regarding the subject of today's hearing and has been endorsed by some of the nation's leading authorities in critical infrastructure protection, terrorism and information security, including the president's two former chief cyber security advisors, Richard Clarke and Howard Schmidt. My statement for the record, which I will summarize for you now, is based primarily on my research for Black Ice and some of my more recent work in this area.

I would like to address the following three questions:

1. What is the nation's current level of vulnerability to cyber-terrorism?

2. What is al-Qaeda's capability to conduct cyber-terrorism?

3. What are the potential implications of a combined physical and cyber-terrorist attack against U.S. critical infrastructures?

1. What is the nation's current level of vulnerability to cyber-terrorism?

Before any meaningful discussion can be conducted about the nation's vulnerability to cyber-terrorism, it is important to understand that there is no longer any separation between the physical, real world, and the cyber-world. Computers and computer networks control real things in the real world. And many of those "things" are critical infrastructures, such as electricity, drinking water and real-time financial transactions that have implications for both public safety and the national economy.

And this understanding must lead us to a new, more flexible definition of the term cyber-terrorism. We can no longer view cyber-terrorism with blinders on, choosing only to consider the acts of somebody sitting behind a computer and hacking or disrupting the operation of other computers or networks as cyber-terrorism. If we learned anything from 9/11 it was that traditional physical forms of terrorism can have massive cyber ramifications that can severely impair the functioning of the nation's economy - an economy that is almost wholly dependent on the uninterrupted operation of a fragile, privately owned and operated digital infrastructure.

Likewise, it is just as important for us to recognize that there is no longer such a thing as an insignificant vulnerability. When vulnerabilities exist, regardless of how minor we may think they are, they open the door to the unexpected and the unanticipated. This is particularly true in the realm of information technologies, where hidden interdependencies exist throughout the nation's critical infrastructures.

And it is an unprecedented level of interdependency that accounts for the nation's current level of vulnerability to cyber-terrorism, in both its physical and its electronic forms. Today every infrastructure or sector of the economy is potentially the Achilles heel of other infrastructures and economic sectors. For example, there is little question about the critical role of electric power in the operation of all sectors of the economy, the dependence of the electric industry on natural gas, the dependence of reliable telecommunications on electric power, the dependence of financial, government, and emergency services operations on both electric power and telecommunications, and the potential impact from prolonged failures of these infrastructures on drinking water and transportation systems. And the interdependence and potential for the type of cascading failure I am describing here stems from the confluence of the physical world and the cyber world.

Perhaps one of the most important areas where an unprecedented level of vulnerability has existed for years and still exists today is in the widespread adoption of wireless technologies. Although there are proven methods and security systems available for protecting wireless networks, they are not always understood and deployed properly, if at all. In my research I have found evidence of unprotected wireless networks in use at the following infrastructure settings: hospitals; airline baggage checking systems at some of the largest U.S. air carriers; railroad track heating switches; uranium mining operations; water and wastewater treatment facilities; security cameras; and oil wells and water flood operations.

Supervisory Control and Data Acquisition systems, or SCADA systems, are in many ways the crown jewels of some of the nation's most important industrial control settings, such as the electric power grid. But they are not - as their name might imply - built upon secret, proprietary technology. To the contrary, modern design specifications for SCADA systems, which I have documented through both personal interviews with experts and through open-source research on the Internet, presents us with the frightening reality that the SCADA systems being used in our nation's critical infrastructures are nothing more than high-end commercial PCs and Servers running Microsoft Corp. operating systems. In other words, the genie is out of the bottle and has been for years in terms of understanding how to disrupt or corrupt the operations of SCADA systems. Today, it's simply a matter of gaining access. And as I have also documented in my research, gaining access to SCADA systems for the purpose of causing widespread chaos, confusion and economic damage is increasingly becoming a mere formality for professional hackers, virus and worm writers, and terrorist-sponsored saboteurs.

The energy industry has acknowledged the existence of these linkages and the imperative of protecting SCADA systems from unauthorized access. In December 2001, for example, the American Gas Association and the Gas Technology Institute met in Washington, D.C., to discuss the need for improved encryption to protect SCADA communications between key nodes in the natural gas grid. One of the slides used during the two days of presentations highlights the threats posed to SCADA communications from the use of commercial computer equipment, open communication protocols that are widely published and available to anybody, linkages and reliance on the public switched telephone network, and the ability to steal the hardware.

In addition, a recent network architecture plan released by a major company in the water and wastewater industry included the following requirements for its SCADA systems: Peer-to-peer networking over TCP/IP (Transmission Control Protocol/ Internet Protocol--in other words, the Internet); software changes that can be downloaded from any node on the network; dial-in capabilities to all software functions; and a link to the existing pump station.

Consider the following additional examples, which I document in my book, Black Ice; The Invisible Threat of Cyber-Terrorism:

The U.S. railroad system's increasing use of wireless technologies may present one of the most immediate dangers to both national security and local safety. Given the system's long, winding network of radio, telephone, and computer assets, voice and data communications networks provide vital links between train crews, trackside monitoring and repair staff, and rail control centers. Total control of the massive network is accomplished through a communication system that integrates trackside maintenance telephones, trackside transponders, security cameras and monitors, passenger information displays, public announcements, the public telephone network, radio bases, and control center consoles. However, wireless SCADA systems are increasingly providing the management glue that keeps all of these systems running together. In the colder regions of the country, underground heaters keep the rails from freezing in winter. These operations are also being controlled and monitored by wireless SCADA computers. The use of modern technology in this case means that in the case of a failure, railroads no longer have to dispatch technicians in the dead of winter to remote locations where heating switches are usually located. However, it also means that the security of these switching operations may now have a new series of security challenges to deal with. This is of particular concern given the dangerous nature of some train cargo.

The City of Brighton, Michigan, is one example. Brighton is a city of only 6,500. But that population skyrockets to more than 70,000 each day due to a thriving business district and a boom in hotel space. However, beneath the streets of Brighton is a water and wastewater system that is controlled in part by wireless technology. The remote terminals monitor pump run time, pump failures, flood sensors, high water level alarms, and power, as well as site intrusion alarms and manually activated panic buttons. The utility also planned to equip work vehicles with a controller connected to a laptop computer. "With critical data now available at just the click of a mouse, the laborious, time-consuming, and often hazardous, need for utility workers to make daily rounds to check pump status at each of the lift stations is a thing of the past," claimed marketing material from one of the contractors responsible for installing the equipment. The mobile controller would then allow utility engineers to monitor the waste water system while they're driving around the city.

Uranium mining operations in Wyoming extract uranium from the soil through a process by which water is injected into the ground. Because of the contamination, remote terminals are necessary to control and manage the pumps that move the water and extract the uranium. Commercial PC-based remote workstations now support critical monitoring functions, such as pump failure, pump status, temperature, speed, and even the pump's on/off condition. But the security implications are enormous. When pumps lose power, water pressure starts building up in the plant. Software has been programmed to automatically reset certain pumps to get the pressure out as fast as possible. And it's all being done in the name of cost-effectiveness.

In states throughout the Midwest, one can find oil wells arranged in a twelve-mile-diameter circle. They are part of what's known in the vernacular of the oil industry as a "water flood" operation. However, with such a large number of pumps and holding tanks to manage, drilling companies are increasingly turning their attention to wireless SCADA systems to monitor critical functions of the operation, including emergency systems that are designed to ensure environmental safety. For example, wireless SCADA systems are used to monitor pressure and flow rates in both oil and water pipelines. When flow rates drop below normal levels, the system is designed to turn on additional pumps. In addition, if pipeline pressure or tank levels exceed normal operating limits the system will turn various pumps off. They are also used to monitor tank levels and overflow pit levels --a critical safety indicator that could have environmental consequences if it fails. And as in the case of the 911 emergency systems, oil well managers and technicians also have remote dial-in connection capabilities.

For the most part, these dire warnings have gone unheeded by the private- sector companies that own and operate these infrastructure systems. Senior executives view such scenarios as something akin to a Hollywood movie script. However, throughout the entire post-September 11-security review process, a process that continues to this day, administration experts and other senior members of the U.S. intelligence community were quietly coming to the conclusion that they were witnessing the birth of a new era of terrorism. Cyberspace, with its vast invisible linkages and critical role in keeping America's vital infrastructures and economy functioning, was fast becoming a primary target and a weapon of terror.

Mr. Chairman, my fear is that the next time we have a massive power failure, such as we experienced on Aug. 14, 2003 it will not be a self-inflicted wound, but potentially a terroristinduced failure that is quickly exploited by suicide bombings, rampaging gunmen or chemical and biological attacks against those stranded in the subway systems.

The Genie Is Out of the Bottle

Figure 1.

This is a photo taken from a publicly available Web site that depicts the most sensitive natural gas pipeline interconnection point in the U.S. What's interesting about this Web page is that it is completely interactive, not only allowing the user to zoom into great detail, but also providing latitude and longitude coordinates and detailed terrain/man-made landmarks.

Figure 2

Detailed, street-level maps of metropolitan area fiber networks are also available online, and include building and company names through which these high-speed interconnections pass.

Other Sensitive Data Available on Government & Corporate Web Sites

1. Detailed maps depicting the termination points along the entire Eastern Seaboard for all long-haul undersea fiber lines.
2. Maps depicting the storage locations of all spent nuclear fuel waste in the U.S.
3. Telecommunications network maps from which the location of current and planned critical facilities and nodes can be derived.
4. One telecom company offered location information for all of the company's five data centers, as well as a virtual tour inside a "typical" center, including a description of all security systems used to protect the facility.
5. Detailed descriptions by IT companies of deployment case studies involving SCADA systems.
6. Load-bearing capacities of elevators in large office buildings as well as location of ventilation and air conditioning systems.
7. Number of people employed at certain office buildings as well as maps and interactive photos of building and facility layout.

2. What is al-Qaeda's capability to conduct cyber-terrorism?

My goal in answering this question is to convince you and others in government to think differently about the future, and particularly, about the future of international terrorism. The high-tech future of terrorism is inevitable. And like the events leading up to the Sept. 11, 2001 terrorist attacks (events that dated back 8 years), we are beginning now to see the indications and warnings that international terrorism is evolving its tactics to meet the new operational realities it faces around the world and to better achieve its strategic goals.

Before we can tackle the question of al-Qaeda's capabilities in terms of conducting cyber-terrorism, it is imperative that we as a nation come to terms with the fact that terrorism is in a constant state of evolution. Terrorist tactics and modes of operation change and adapt over time, albeit very slowly and often imperceptibly. It is also imperative that we accept that terrorism has never only been about terror. There have always been and will always be socio-political and economic warfare aspects to international terrorism that speak directly to the potential employment of cyber-terrorist tactics.

Al-Qaeda's view of cyber-terrorism and its history in using information technologies is a case in point. But here, again, we face a significant perception problem. The picture that most Americans form in their minds when they think of al-Qaeda or of terrorists in general is a picture of a mindless horde of thugs living a hand-to-mouth existence in caves in Afghanistan. But this picture says nothing of the educated elite that forms the inner circle of the group's command and control, it says nothing of the technical support available on the open market in the form of out of work intelligence experts from a host of nations, and it says nothing of the threat posed by the continued radicalization of young people all over the world - young people who are studying computer science and mathematics and who may find it more advantageous to strike out directly at the U.S. economy than to strap explosives around their waste and walk into a crowded café.

That said, there is already ample evidence to suggest that the current generation of al-Qaeda terrorists understand the usefulness of attacking the U.S. cyber infrastructure.

For example, L'Houssaine Kherchtou, a 36-year-old Moroccan, was one of al-Qaeda's early trainees in high-tech methods of surveillance during the early to mid 1990s. He attended electronics training conducted in a guesthouse owned by Osama bin Laden on Fey Street in Peshawar, Pakistan. The electronics Lab was run by Abu al-Alkali and Salem the Iraqi. When he arrived, however, he informed his superiors that he did not have any background in electronics. A short time later, a more senior instructor arrived and informed Kherchtou that a degree in engineering was required to attend electronics training. This is not the picture of a mindless horde of thugs. This is the picture of a thinking enemy that values formal training and education. In November 2002, I interviewed Sheikh Omar Bakri Muhammad, the leader of a London-based organization known as al-Muhajirun. Prior to the September 11, 2001 terrorist attacks, an FBI memo written by agent Kenneth Williams and e-mailed to the FBI's Washington headquarters on July 10, 2001, noted a connection between Middle Eastern men enrolled in Phoenix-area flight schools and Bakri's organization in London. This should have been no surprise since Bakri, a Syrian-born Muslim cleric, refers to
al-Muhajirun as "the mouth, eyes, and ears" of bin Laden and claims to speak on behalf of bin Laden's International Islamic Front for Jihad Against Jews and Crusaders. Furthermore, Bakri was one of several individuals in 1998 to receive a letter faxed from Afghanistan from bin Laden that outlined four objectives for a jihad against the U.S., including the hijacking of airliners. Also included in the fax was a statement urging Muslims to "force the closure of their companies and banks."

But my interview with Bakri in 2002 was the first example of a high profile, radical Islamic cleric speaking about the usefulness of cyber attacks in support of bins Laden's global Jihad. According to Bakri:

? "In a matter of time, you will see attacks on the stock market."
? "I would not be surprised if tomorrow I hear of a big economic collapse because of somebody attacking the main technical systems in big companies."
? "The third letter from Osama bin Laden...was clearly addressing using the technology in order to destroy the economy of the capitalist states. This is a matter that is very clear."

Osama bin Laden has also spoken in these terms. According to Hamid Mir, editor of the Ausaf newspaper, "Hundreds of young men had pledged to him that they were ready to die and that hundreds of Muslim scientists were with him and who would use their knowledge in chemistry, biology and ranging [sic] from computers to electronics against the infidels."

Bin Laden has also instructed his followers that "It is important to hit the economy of the United States, which is the base of its military power. If the economy is hit they will become preoccupied."

Since the start of the U.S. War on Terrorism, a significant amount of evidence has been unearthed throughout Afghanistan and various other al-Qaeda hideouts around the world that indicates terrorism may be evolving toward a more high-tech future at a faster rate than previously believed.

In January 2002, for example, U.S. forces in Kabul discovered a computer at an al-Qaeda office that contained models of a dam, made with structural architecture and engineering software. The software would have enabled al-Qaeda to study the best way to attack the dam and to simulate the dam's catastrophic failure. In addition, al-Qaeda operatives apprehended around the world acknowledged receiving training in how to attack key infrastructures. Among the data terrorists were studying was information on SCADA systems.

Despite all of the mounting evidence that suggests al-Qaeda is evolving toward the use of cyber-weapons, the terrorist group that started us down this path and that has posed the greatest threat of all terrorist groups to U.S. national security remains somewhat of a mystery. But the War on Terrorism has helped uncover some of the hidden trends. Al-Qaeda cells now operate with the assistance of large databases containing details of potential targets in the U.S. They use the Internet to collect intelligence on those targets, especially critical economic nodes, and modern software enables them to study structural
weaknesses in facilities as well as predict the cascading failure effect of attacking certain systems. But the future may hold something quite different.

The three driving factors behind al-Qaeda's operations--intent, resources, and opportunity--all point to the future use of cyber-tactics.

First, the intent of Osama bin Laden is clear. He wants to cripple the economy of the U.S. as a means to force the withdrawal of U.S. military personnel from Saudi Arabia and curtail economic and military support for Israel. The targeting of corporate America and the digital economy is clear in this regard.

Second, the growing number of technologically sophisticated sympathizers, especially among Muslim youth, is providing al-Qaeda with a steady stream of new talent in the use of offensive cyber-weapons. In addition to the younger generations of hackers and virus writers, al-Qaeda and other radical Islamist movements can count on the intelligence services of various rogue nations who now and in the future will find themselves in the crosshairs of the U.S. military.

Finally, America continues to present al-Qaeda and other radical Islamist groups with ample economic targets in cyberspace, thus driving these groups toward the increased use of cyber-tactics. Unless current trends are reversed and America's digital economy is no longer a target of opportunity, terrorist groups around the world will continue to dedicate time and resources to studying ways to integrate cyber-weapons into their operations.

3. What are the potential implications of a combined physical and cyber-terrorist attack against U.S. critical infrastructures?

The blackout of August 14, 2003 notwithstanding, the danger stemming from this unprecedented level of infrastructure interdependency was proven during the first major infrastructure interdependency exercise, which took place in November 2000 in preparation for the 2002 Winter Olympics in Utah. Known by its code name, Black Ice, the simulation was sponsored by the U.S. Department of Energy and the Utah Olympic Public Safety Command. The goal was to prepare federal, state, local, and private-sector officials for the unexpected consequences of a major terrorist attack or a series of attacks throughout the region, where tens of thousands of athletes and spectators from around the
world would gather. When it was over, Black Ice demonstrated in frightening detail how the effects of a major terrorist attack or natural disaster could be made significantly worse by a simultaneous cyber-attack against the computers that manage the region's critical infrastructures.

Without going into the details of the exercise, the conclusions drawn by the exercise participants are startling. Estimates showed the loss of electric power throughout a five-state region and three provinces in Canada for at least one month. Other estimates went as far as several months.

The important lesson is that Black Ice showed the growing number of critical interdependencies that exist throughout the various infrastructure systems and how devastating combined cyber-attacks and physical attacks can be. It proved for the first time that the terrorist's mode of attack is irrelevant when it comes to cyber-terrorism. Terrorist groups that want to amplify the chaos and confusion of physical attacks or directly target the economy can succeed by launching traditional-style terrorist assaults against the nation's cyber-infrastructure.

According to the final report on the lessons learned from exercise Black Ice and a follow on exercise code-named Blue Cascades, government and private-sector participants "demonstrated at best a surface-level understanding of interdependencies and little knowledge of the critical assets of other infrastructures, vulnerabilities and operational dynamics of these regional interconnections, particularly during longer-term disruptions." Moreover, most companies and government officials failed to recognize their own "overwhelming dependency upon IT-related resources to continue business operations and execute recovery plans," according to the report.

As is evident from the following paragraph, the detailed findings of the Hart-Rudman task force confirmed the findings of the Black Ice and Blue Cascades exercises.

Sixty percent of the Northeast's refined oil products are piped from refineries in Texas and Louisiana. A coordinated attack on several key pumping stations--most of which are in remote areas, are not staffed, and possess no intrusion detection devices--could cause mass disruption to these flows. Nearly fifty percent of California's electrical supply comes from natural gas power plants and thirty percent of California's natural gas comes from Canada. Compressor stations to maintain pressure cost up to $40 million each and are located every sixty miles on a pipeline. If these compressor stations were targeted, the pipeline would be shut down for an extended period of time. A coordinated attack on a selected set of key points in the electrical power system could result in multi-state blackouts. While power might be restored in parts of the region within a matter of days or weeks, acute shortages could mandate rolling blackouts for as long as several years. Spare parts for critical components of the power grid are in short supply; in many cases they must be shipped from overseas sources.