FRONTLINE
20 YEARS ON PBS

WGBH
125 Western Avenue
Boston, Massachusetts 02134
617.300.3500
Fax: 617.300.1001
www.pbs.org/frontline

Major funding provided
by public television viewers

CYBER WAR!
PBS Airdate: Thursday, April 24, at 9 P.M., 60 minutes

In the aftermath of September 11, as most intelligence gathering shifted to finding Al Qaeda cells throughout the world, one group at the White House decided to investigate a new threat—attacks from cyberspace.

"In the past, you would count the number of bombers and the number of tanks your enemy had. In the case of cyberwar, you really can't tell whether the enemy has good weapons until the enemy uses them," says Richard Clarke, former chairman of the White House Critical Infrastructure Protection Board.

In "Cyber War!" airing Thursday, April 24, at 9 P.M. on PBS (check local listings), Clarke and other insiders talk about a new set of warriors who are fighting on a new American battlefield—cyberspace. In this one-hour report, FRONTLINE investigates how vulnerable the Internet is to both virtual and physical attack.

"The thing that keeps me awake at night is [the thought of] a physical attack on a U.S. infrastructure…combined with a cyberattack which disrupts the ability of first responders to access 911 systems," says Ron Dick, former head of the FBI's National Infrastructure Protection Center. The issue of cyberwar first began to command urgent White House attention after a distinguished group of scientists wrote an open letter to the president following the Al Qaeda attacks.

"The critical infrastructure of the United States, including electrical power, finance, telecommunications, health care, transportation, water, defense and the Internet, is highly vulnerable to cyberattack. Fast and resolute mitigating action is needed to avoid national disaster," wrote the authors of the letter, who included J.M. McConnell, a former head of the National Security Agency, Stephen J. Lukasik of the Defense Advanced Research Projects Agency, and Sami Saydjari of the Defense Research Center.

"Ultimately, it turned into about fifty-four scientists and leaders—former national leaders, intelligence community people as well—sending this letter that makes the case that says, 'We have a problem here,'" Saydjari tells FRONTLINE.

In "Cyber War!" FRONTLINE investigates a number of cyberattacks that have already occurred: "Slammer," which last January took down the Internet in South Korea and affected 911 systems and the banking system in the United States, and the "Nimda" virus that quietly attacked Wall Street in 2001.

"Nimda cost probably three billion dollars," says Clarke. "Had it not been for the fact that September eleventh was the week before, it would have been a big news story."

FRONTLINE also follows efforts by the United States to go on the offensive.

"You cannot defend yourself unless you understand how the offense works. And in so doing, you learn to wage offensives," says John Arquilla, associate professor of Defense Analysis at the Naval Postgraduate School in Monterey, California. Arquilla has helped the Department of Defense develop information warfare strategies utilized in the first Gulf War, Kosovo, Afghanistan, and in the most recent war with Iraq.

But many cyberwar experts believe the Internet could be used to launch a major attack on the nation's infrastructure.

"What we found on Al Qaeda computers was that members of Al Qaeda were from outside the United States doing reconnaissance in the United States on our critical infrastructure," says Clarke.

One target, experts say, could be the country's electric power grid. By exploiting vulnerabilities in the supervisory-control and data-acquisition (SCADA) systems that utility companies use to remotely monitor and control their operations, American cities could be left in the dark.

"You could take down significant pieces of it for let's say operationally useful periods of time. Penetrating a SCADA system that's running a Microsoft operating system takes less than two minutes," one cyberwarrior who spoke on the condition of anonymity tells FRONTLINE.

Joe Weiss, a control system engineer and executive consultant for KEMA Inc. reluctantly agrees that the power grid is vulnerable. "A very worst case could be loss of power for six months or more," says Weiss.

Clarke, scientists, and some inside the military have tried to convince Washington that cybersecurity needs to be a priority. They have had limited success.

"I think cyberterrorism is a theoretical possibility," says John Hamre, director of the Center for Strategic and International Studies, a prestigious military think tank. "Will cyberterrorism be like September eleventh? No, I don't think so, not right now."

"Terrorists are after the shock effect of their actions," Hamre adds. "And it's very hard to see the shock effect when you can't get your ATM machines to give you twenty dollars."

But Clarke—who as head of counterterrorism for the Clinton and Bush administrations was an early voice warning about Al Qaeda in the middle 1990s—says cyberattacks are imminent.

"When we have the experts telling us we have a big risk," says Clarke, "wouldn't it be nice, for once, to get ahead of the power curve, solve the problem, so there never is the big disaster?"

Following the broadcast, visit FRONTLINE's Web site, at www.pbs.org/frontline, for extended coverage of this story, including:

- Extended interviews with top-level experts on cyberspace security in private industry, the U.S. government, the intelligence community, and infrastructure networks;
- A forum with cybersecurity experts who will field questions from viewers;
- A discussion with a master hacker on how tools for computer hacking can help access systems such as SCADA controls, corporate databases, and secure government networks;
- Video streaming of "Cyber War!" in both WindowsMedia and Real Player, and much more.

"Cyber War!" is a FRONTLINE co-production with the Kirk Documentary Group. The writer, producer, and director is Michael Kirk. The co-producer and reporter is Jim Gilmore.

FRONTLINE is produced by WGBH Boston and is broadcast nationwide on PBS.

Funding for FRONTLINE is provided through the support of PBS viewers.

FRONTLINE is closed-captioned for deaf and hard-of-hearing viewers.

The executive producer for FRONTLINE is David Fanning.

Press contacts: (617) 300-3500
Erin Martin Kane [erin_martin_kane@wgbh.org]
Chris Kelly [chris_kelly@wgbh.org]

FRONTLINE XXI/April 2003