Experts say electromagnetic pulse devices threaten U.S.

BY DANIEL VERTON
Oct. 18, 1999

Experts this month warned Congress that terrorists and foreign countries may have a new cyberweapon at their disposal to counter U.S. military might—electromagnetic pulse devices.

When "detonated," an EMP weapon produces a pulse of energy that creates a powerful electromagnetic field capable of short-circuiting a wide range of electronic equipment, particularly computers, satellites, radios, radar receivers and even civilian traffic lights. An EMP shock wave can be produced by a device small enough to fit in a briefcase or by exploding a small nuclear weapon high in the atmosphere.

Regardless of the method of delivery, experts agree that EMPs can be powerful enough to cripple electronic wiring and circuitry over a geographic area as large as several square miles, posing a real threat to the nation's critical infrastructure. In addition, the Defense Department's reliance on satellites and commercial computer equipment to conduct real-time command and control of forces around the world also puts military operations at risk, experts say.

Speaking this month at a hearing of the House Armed Services Committee's Research and Development Subcommittee, subcommittee chairman Rep. Curt Weldon (R-Pa.) said the United States' evolution into a technologically dependent society has made its infrastructure vulnerable to the effects of EMPs.

"The widespread paralysis of electronic computer systems, communications, power grids and transportation systems would not merely be an inconvenience," Weldon said. "Our modern way of life, and life itself, depends upon the functioning of our electronic society."

However, Stanley Jakubiak, senior civilian official for nuclear command, control, communications and EMP policy for DOD, said that while the EMP phenomenon has been studied for many years, the impact of such an attack is unclear.

"We know it will impact electronic equipment, but due to the variation of tolerances built into commercial equipment and the different system configurations, we can't accurately predict how widespread any damage or disruption will be," Jakubiak said.

Still, military systems are becoming increasingly reliant on commercial off-the-shelf components, which are not designed to withstand the effects of an EMP attack, he said.

"These devices provide terrorists the equivalent of a surgical strike by an airplane," said Winn Schwartau, president of security consulting company Interpact Inc. "If you're a victim of one of these attacks, you are not going to know what hit you."

First developed in 1870 by scientist Heinrich Hertz, EMP technology can be harnessed by terrorists who have only basic engineering and technical skills, Schwartau said. In addition, EMP devices are highly portable, can be operated from a distance and provide remote security that hackers do not have when they are connected to the system they are hacking, he said.

Martin Libicki, a defense and national security analyst with Rand Corp., said he is skeptical of the extent to which terrorists would want to use EMP devices to carry out attacks against critical infrastructure. "I have yet to see [a terrorist group, such as] Islamic Jihad, take credit for anything like a cyberattack," Libicki said. He questioned the notion that terrorists are interested in nonlethal weapons. "Terrorists like to see blood and gore," he said.

A weapon similar to an EMP device involving graphite particles recently was used during the war in Kosovo to short-circuit the electric grid in Yugoslavia without using deadly explosives. During Operation Allied Force, NATO aircraft dropped strips of graphite on electric power lines throughout Yugoslavia, which resulted in cascading power failures.