JOURNAL OF CIVIL DEFENSE

Volume 37, Issue #10 *October 2004*

Inside This Issue:

The Electromagnetic Pulse Commission Warns of an Old Threat with a New Face

By Jack Spencer, the Heritage Foundation
Backgrounder #1784

A nuclear-generated electromagnetic pulse (EMP) "is one of a small number of threats that has the potential to hold our society seriously at risk and might result in defeat of our military forces." The Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack announced this startling conclusion in a July 22 report to Congress [1]. This alarming report clears the way for Congress to debate more seriously the most effective measures to meet the threat of an EMP attack.

Protecting the United States against the evolving EMP threat will require a mix of active defenses, passive defenses, and policy changes. Specifically, the United States should:

• Develop a clear policy about how it will respond to an EMP attack;
• Assess which assets of the nation's power grid and telecommunications infrastructure are most critical to the overall system;
• Harden those critical assets against EMP;
• Retrofit at least a portion of U.S. military assets to protect against EMP;
• Engineer EMP protections into a greater percentage of future military capabilities; and
• Deploy an effective ballistic missile defense.

What Is Electromagnetic Pulse?
In addition to the ability to kill thousands of people instantly, nuclear weapons have another, equally crippling capability to destroy or disrupt power grids, electronic systems, and communications in an entire country, while sparing the lives of its people--at least initially. Specifically, a nuclear bomb detonated above the earth's atmosphere would create a split-second electromagnetic pulse, similar to an extremely high-energy radio wave. For example, a single nuclear weapon detonated at an altitude of 500 kilometers could produce an EMP that would blanket the entire continental United States, potentially damaging or destroying military forces and civilian communications, power, transportation, water, food, and other infrastructure essential to modern society. [2]

Although recent changes in homeland security policy would decrease the severity of such an attack, recovery could still take years. In a congressional hearing on the EMP threat, chaired by Representative Roscoe Bartlett (R-MD), Dr. Lowell Wood of the Lawrence Livermore National Laboratory described the effect of an EMP attack as instantly regressing a country dependent on 21st century technology by more than 100 years. [3]

Although the EMP threat has been the focus of significant government-funded research and testing over the past 30 years, most of those efforts were conducted during the Cold War and focused on hardening strategic systems against a massive nuclear attack by the Soviet Union. Far fewer resources have been dedicated to examining the potential vulnerability of the U.S. civilian and industrial infrastructure to an EMP attack. Moreover, since the end of the Cold War, U.S. military and civilian systems have become increasingly dependent on advanced electronics that are potentially more vulnerable than older electronics to EMP attack--a trend that will likely continue.

The EMP Commission

Recognizing the potential of this powerful nuclear phenomenon, Congress established the EMP Commission under the National Defense Authorization Act of 2001 in order to provide an independent assessment of this threat against the United States. The authorizing provision directed that the EMP Commission investigate and report to Congress its findings and recommendations for the United States concerning four aspects of the EMP threat:

1. The nature and magnitude of potential high-altitude EMP threats to the U.S. from all potentially hostile states and non-state actors that have or could acquire nuclear weapons and ballistic missiles enabling them to launch a high-altitude EMP attack against the U.S. within the next 15 years;
2. The vulnerability of U.S. military and civilian systems to an EMP attack, giving special attention to the vulnerability of the civilian infrastructure as a matter of emergency preparedness;
3. The capability of the U.S. to repair and recover from damage inflicted on the U.S. military and civilian systems by an EMP attack; and
4. The feasibility and cost of hardening select military and civilian systems against EMP attack. [4]

America's Vulnerability to EMP Attack

Little has been done to safeguard U.S. electrical systems from the EMP threat beyond simply protecting the nation's nuclear war-fighting infrastructure--and even that is not as secure as it once was. During the Cold War, only the Soviet Union--and to a lesser extent China--had the ability to mount an EMP attack against the United States. If one of those countries had launched an EMP attack, it would most likely have been the initial salvo of a larger nuclear attack. Therefore, it made little sense to separate an EMP attack from general nuclear war. Because most civilian and non-strategic military equipment would be destroyed or of no use during a full-scale nuclear exchange, there was no requirement to protect civil infrastructure from an EMP.

Today, the proliferation of nuclear technology and ballistic missiles has changed the nature of the EMP threat. A high-altitude EMP explosion over the continental United States or a battle space must be understood as a separate and unique threat that requires a unique response. Understanding both the effects of EMP, as well as America's vulnerability, is the first step in addressing the threat.

The scientific principles behind generating a high-altitude EMP are relatively simple. If a nuclear weapon is detonated between 25 miles and 300 miles above the earth's surface, the radiation from the explosion interacts with air molecules to produce high-energy electrons that speed across the earth's magnetic field as an instantaneous, invisible electromagnetic pulse. [5]

An EMP can have devastating consequences for developed countries because any metallic conductor in the affected area becomes a "receiver" for the powerful energy burst released by the blast. Such receivers include anything with electronic wiring--from airplanes and automobiles to computers, railroad tracks, and communication lines. If systems connected to these "receivers" are not protected, they will likely be damaged or disrupted by the intense energy pulse. Indeed, depending on the strength of the pulse and the vulnerability of the equipment, the effects could range from a passing interference to completely melting the electrical components.

An EMP attack damages all unprotected electronic equipment within the blast's "line of sight" (the EMP's "footprint" on the earth's surface). The size of the footprint is determined by the altitude of the explosion. The higher the altitude, the greater the land area affected. A Scud-type ballistic missile launched from a vessel in U.S. coastal waters and detonated at an altitude of 95 miles could degrade electronic systems across one-quarter of the United States. A more powerful missile launched from North Korea could probably deliver a warhead 300 miles above America--enough to degrade the electronic systems across the entire continental United States.

Furthermore, a nuclear weapon with only a low explosive yield could be designed to generate a strong EMP. In fact, crude weapons with low yields, such as those used against Japan in World War II, would have ample power to generate an EMP over the entire continental United States.

Likely EMP Scenarios

Under what circumstance would the United States be attacked with an EMP? Possible scenarios include a rogue state interested in demonstrating its ability to strike U.S. territory or a country that wants to give itself an advantage in a regional conflict by crippling U.S. military and other allied forces that are more dependent on advanced electronics.

Although the threat of a high-altitude EMP attack against America existed during the Cold War, the likelihood may be much greater today. [6] During the Cold War, an EMP attack was viewed as the first step in launching a nuclear war. However, it was never tried because the threat of massive nuclear retaliation, the central tenet of the mutual assured destruction doctrine, provided an effective deterrent. Although China and Russia both maintain the ability to launch major nuclear strikes against the United States, the Cold War dynamic that made the doctrine of mutual assured destruction relevant is largely gone from today's strategic calculations.

The proliferation of weapons of mass destruction (WMDs), the rise of powerful non-state actors, and the evolving strategic relationships with countries like China and Russia have made the threat more difficult to assess. In reality, the U.S. simply cannot rely on the old tools of deterrence to compel threatening regimes not to attack the United States or its interests. As demonstrated on September 11, 2001, the Cold War deterrent of massive retaliation does not work.

The emergence of nuclear rogue states results in a completely new strategic calculation. Since no rogue nation has the capacity to fight a general nuclear war, an EMP blast would not be a precursor of a full-scale nuclear war. Furthermore, since an EMP blast is unlikely to kill anyone directly or to be followed by a nuclear strike that would annihilate U.S. cities, the United States is less likely to retaliate and destroy an entire nation of innocent people as punishment for the decisions of a rogue leader. It is simply unclear how the U.S. would respond to such an attack.

The difficulty of developing a clear response to EMP is due primarily to the unique nature of the threat. It is unclear, for example, what would constitute a "proportional response" to an explosion that takes place in space without being seen or heard, yet instantaneously devastates society or a military force while resulting in no initial loss of life or physical destruction. Furthermore, there is a dearth of academic or legal analysis by which to guide such policies because, until very recently, few took the threat seriously. This is especially so in the context of rogue states or transnational groups.

The simple motivation for a rogue state to use its limited nuclear arsenal in an EMP strike against the United States is that an EMP attack maximizes the impact of a few warheads while minimizing the risk of retaliation. This profound decrease in risk for rogue leaders could impel them to use EMP to offset overwhelming U.S. conventional power on the battlefield. While EMP may not precede general nuclear war, it could be used as an opening salvo in a conventional war. Nations with small numbers of nuclear missiles, such as North Korea or Iran, may consider an EMP attack against U.S. forces in a region, to degrade the U.S. military's technological advantage, or against the United States' national electronic infrastructure.

Furthermore, an EMP attack using a few nuclear weapons could theoretically damage the entire continental United States, far exceeding the impact of using those same warheads against specific U.S. cities or installations. Likewise, an EMP attack could degrade the U.S. armed forces throughout an entire region. Because America's response to an EMP attack by a rogue state is unclear and because EMP attacks are less risky for rogue states, such attacks are far more likely in this era of nuclear weapons proliferation than during the Cold War.

Protecting America Against EMP

Unfortunately, hardening systems is difficult and expensive. To protect electronics infrastructure, entire systems must be encased in a metallic shield to prevent any external electromagnetic pulse from entering. Moreover, antennas and power connections must be equipped with surge protectors, windows must be coated with wire mesh or conductive coating, and doors must be sealed with conductive gaskets. Fiber optic cable is not vulnerable to EMP, but the switches and controls that use microelectronics in conjunction with the fiber optic cable need to be protected. Continuing efforts to replace copper communications cable with fiber optic cable will significantly reduce overall EMP vulnerability. To ensure that the protection lasts for the lifetime of the equipment, system maintenance and testing should be performed regularly. If a system is modified, repaired, or serviced, its EMP vulnerability should be reassessed.

All of these steps can be affordable. Assuming these protections are engineered into a product or structure from the outset, these protections would add as little as 1 percent to 5 percent to overall costs. (Retrofitting systems, however, could add substantial costs.) EMP surge protectors have become very inexpensive. According to George Ullrich, former Deputy Director of

the now abolished Defense Special Weapons Agency, such hardening is needed:

"Systems, such as commercial power grids [and] telecommunications networks remain vulnerable to widespread outages and upsets due to high altitude EMP. While DOD hardens assets it deems vital, no comparable civil program exists." [7]

Protecting the United States against the evolving EMP threat will require a mix of active defenses, passive defenses, and policy changes. Specifically the United States should:

• Develop a clear policy about how it would respond to an EMP attack. An adversary may be emboldened to use EMP because the U.S. has no clear retaliation policy. As the commission's report makes clear, an EMP attack could devastate both civilian and military assets without harming humans--in the short term. An adversary could therefore calculate that the United States would respond less severely to an EMP strike than it would to a more traditional strike that results in physical destruction and casualties. That makes EMP very attractive. It could carry decreased risk but promise great reward.

By itself, a policy guaranteeing significant retaliation may not deter all hostile groups from using EMP, but it may deter some. Better yet, a policy to retaliate combined with other actions--such as installing active defenses, increased passive defenses, and assuring military survivability--would decrease the likelihood of an EMP attack against the United States because such measures would make a strike less likely to succeed. If it did succeed, the consequences for the United States would be minimal. Thus, the value of an EMP strike would be greatly reduced, but the risk of launching an attack would be greatly increased because the U.S. would not only have a policy to retaliate, but also the capability.

• Protect the vital nodes of America's power grid and telecommunications systems. Much of America's power grid and telecommunications systems is vulnerable to EMP attack. In the near term, hardening America's entire critical infrastructure is not feasible. However, protecting those elements of U.S. infrastructure that would be key to any post-EMP recovery (e.g., large turbines, generators, high-voltage transformers, and electronic telecommunications switching systems) is possible. These major nodes are not only critical to the nation's power-grid and telecommunications capability, but would be extremely difficult and time consuming to rebuild or repair. Protecting these critical infrastructure nodes may be expensive in the near term, but it could save the nation significantly in both money and lives in the future.

• Conduct a national vulnerability assessment and prepare a national recovery plan. Although protecting the nation's entire electronic and telecommunications systems against EMP strike is unreasonable, protecting some of those assets is possible. The Department of Homeland Security (DHS) should work with the private sector to identify which parts of the nation's power grid and telecommunications infrastructure are critical to preserving the nation's core capabilities. These assets would also be the most essential to recovery efforts in a post-EMP environment. By protecting these nodes, the United States could significantly reduce the time needed to recover from an attack. Additionally, DHS should develop a contingency plan for recovery from an EMP attack that would minimize confusion.

• Retrofit portions of the U.S. armed forces to ensure EMP survivability. The United States' military must end its nearly complete vulnerability to an EMP strike. This glaring hole in U.S. defenses is a liability that America's adversaries will surely exploit if it is not corrected. As with civilian infrastructure, hardening America's entire military apparatus against EMP is prohibitively expensive. However, the nation should invest the resources to retrofit enough of the military's land, sea, and air assets to guarantee any potential adversary that the U.S. will be able to respond comprehensively to any kind of attack. Hardening military equipment against EMP costs approximately 10 percent of the original cost of the equipment. While this is high, it is a necessary expense given the risk.

• Begin building military systems that are engineered with EMP protections. Although retrofitting against EMP is extremely expensive, engineering EMP resistance into a system from the beginning adds only about 1 percent to the system cost. Given that so much of military equipment is already old and that force transformation will result in many new systems and platforms, now is an opportune time to begin dealing with this problem. In addition to saving money by incorporating EMP resistance into new systems instead of retrofitting existing equipment, America's transformed military will increasingly rely on many sophisticated electronic networks and systems. A successful EMP strike against U.S. forces that disrupted or destroyed these systems would effectively turn America's technological advantage into a distinct liability.

• Deploy ballistic missile defense. The surest way to protect the United States from a high-altitude EMP is by deploying a ballistic missile defense system that can intercept and destroy a warhead before it could be

detonated above the U.S. This would prevent an EMP attack and eliminate any potential harm to U.S. systems, and it could even deter rogue leaders from considering the use of EMP. Deploying a missile defense architecture that can intercept a missile early in flight (during the ascent phase) would render rogue missiles ineffective, thereby undermining the rationale to use them. Moreover, because protecting America's entire civilian electronic infrastructure is not fiscally feasible and because a ballistic missile is the most likely delivery vehicle for an EMP attack, the most prudent method to protect America is a missile defense system that could destroy a ballistic missile before it reaches U.S. airspace.

Conclusion

As the EMP Commission reported, an EMP attack on America is a serious possibility and one for which the United States is unprepared. While the world focuses on WMDs and ballistic missiles, it is imperative that an EMP attack be considered with equal weight. The profound impact that an EMP attack would have on a developed, modern, electronically oriented country forces nations in similar positions to reassess their own protection against such attack.

Looking toward the future, America should consider its options for protecting its infrastructure against such a debilitating attack. Those options are limited, but include deploying an effective missile defense system and hardening electronic systems against EMP. As the commission indicated, the implications of an EMP attack need to be assessed further with greater severity and inevitability as America considers possible protective actions against this threat.

Jack Spencer is Senior Policy Analyst for Defense and National Security in the Kathryn and Shelby Cullom Davis Institute for International Studies at The Heritage Foundation.

1. Dr. John Foster, Jr., et al., Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Volume 1: Executive Report, report to Congress, 2004.

2. "Title XIV--Commission to Assess the Threat to the United States From Electromagnetic Pulse (EMP) Attack: Overview," in National Defense Authorization Act for Fiscal Year 2001, Public Law 106-398, June 2003.

3. Lisa Wright, press secretary to Representative Roscoe Bartlett, e-mail broadcast, June 21, 2004.

4. Public Law 106-398, Title XIV, Section 1402.

5. For a scientific description of the physics of high-altitude electromagnetic pulses, see Gary Smith, "Electromagnetic Pulse Threats," testimony before the Subcommittee on Military Research and Development, Committee on National Security, U.S. House of Representatives, July 16, 1997.

6. For an analysis of the fear concerning an EMP attack during the Cold War, see David Burnham, "U.S. Fears One Bomb Could Cripple the Nation," The New York Times, June 28, 1983, p. 1.

7. Dr. George W. Ullrich, statement in Hearing, Threat Posed by Electromagnetic Pulse (EMP) to U.S. Military Systems and Civil Infrastructure, Subcommittee on Military Research and Development, Committee on National Security, U.S. House of Representatives, 105th Cong., 1st Sess., July 16, 1997, p. 23, at: www.commdocs.house.gov/committees/security/has197 010.000/ has197010_0f.htm (July 30, 2004).

Source: www.heritage.org

The Threat of Nuclear Terror

The prevailing assessment in the United States is that Al-Qaeda and other large terror organizations are individually making efforts to obtain fissionable nuclear materials that will enable them in the future to produce atomic weapons. It is no wonder that important American strategists are saying that the greatest security threat to the United States today is a nuclear terror attack, which will surprise and cause the U.S. a mortal blow. They believe that if preventative measures against atomic terror are not taken, then an "American Hiroshima," as they call it, is almost inevitable.

One of the leading experts who holds this view is Professor Graham Allison of Harvard University, a former senior Pentagon official who has participated in numerous conferences dealing with the nuclear issue. Allison sets forth his firm opinions in his new book, "Nuclear Terrorism: The Ultimate Preventable Catastrophe" (Times Books), which was published in August and is receiving a great deal of attention.

In it he also expresses astonishment at the possibility that nuclear terror is not of concern to Israel, even though it could well serve as a target for an organization like Al-Qaeda. According to Allison, it is known that in

the past Al-Qaeda conducted experiments with chemical and biological weapons as well as with radioactive materials, the main danger of which is the creation of mass panic.

Another expert, Professor Paul Bracken of Yale University, who recently visited Israel, also believes that the danger of atomic terror is real. That danger is increasing because of the wild proliferation of nuclear materials and know-how, as exemplified by the case of "the father of the Pakistani atomic bomb," Abdul Qadeer Khan, who sold nuclear know-how to various rogue countries like Iran, Libya and North Korea. This affair - in which a country that is considered a friend of the United States becomes the largest disseminator of nuclear know-how - takes up considerable space in Allison's book.

Other sources for the spread of know-how and materials could be Iran and the Confederation of Independent States. There are those who believe that a pre-nuclear Iran constitutes a danger. Brenda Shaffer, an expert from Harvard, says that there is a danger of the loss of control over nuclear materials that have been produced in Iran and are liable to be sold to various elements.

During the Cold War period, the United States was also under a nuclear threat from a rival power. However, this danger - as opposed to the danger of nuclear terror - had an address. Today there is not even a phone number by which it is possible to negotiate with nuclear terrorists, and of course there is no target for a response to a terrible act.

The powers of yesterday, which had at their disposal no fewer than 22,000 tactical nuclear bombs but also had at least an address, could lose their safe hold on them. Criminal elements are liable to sell the small atomic bomb to terrorists, and the smuggling of such a bomb into the United States would also not be difficult, according to commentators.

Israel's name often comes up in chapters in Allison's book that deal with ways to prevent the spread of atomic weapons. Allison notes three main aims that are essential to any strategy of prevention, goals that necessitate above all an umbrella of close international cooperation.

The first aim is to prevent at any price new member countries from joining the existing nuclear club, whose members are, according to Allison, the United States, Russia, England, France, China, India, Pakistan and Israel.

The second aim is to prohibit additional countries from enriching uranium or extracting plutonium on their own. Instead, an international bank of enriched uranium will be established, and countries that need it for peaceful purposes will be able to apply to the bank.

The realization of this aim will make it easier to achieve the third aim - getting rid of the fissionable materials that already exist. With Iran, for example, there will be a need to negotiate the way in which it will get enriched uranium for peaceful purposes. This is after it will agree to stop producing it on its own. Thus far there has been no real international awakening on this issue, and the truth is that in light of what is happening in the world, Allison's proposals seem like an ideal vision, though it is doubtful that it can be realized.

Source: www.haaretz.com/hasen/spages/482591.html

U.S. Tries To Penetrate Al-Qaeda 'Cyber Sanctuaries'

CLIFTON, New Jersey From the main street here, you can see the Manhattan skyline, off in the distance. The flags that sprouted after the Sept. 11 attacks still flap on lawns and flutter on poles outside well-tended homes.

Looming above them is a concrete tower that houses a real estate firm, an office supplies company - and, investigators fear, an outpost of Al-Qaeda. On the second floor, an Internet company called Fortress ITX unwittingly provided access until recently for an Arabic-language Web site where postings in recent weeks urged attacks against American and Israeli targets. "The Art of Kidnapping" was explained in electronic pamphlets, along with "Military Instructions to the Mujahedeen," and "War Inside the Cities."

Visitors could read instructions on using a cellular phone for remote detonation of a bomb or for asking for help in manufacturing small missiles.

"How can this be?" asked Cathy Vasilenko, who lives a few doors away from the Fortress ITX office. "How can this be going on in my neighborhood?"

Federal investigators, with the help of a small army of private contractors monitoring sites round the clock and across the world, are trying to find out. Ever since U.S.-led forces smashed Al-Qaeda's training grounds in Afghanistan, cyber substitutes, which recruit terrorists and raise money, have proliferated.

While Al-Qaeda operatives have employed an arsenal of technical tools to communicate - from e-mail encryption and computer war games to grisly videotapes like the recent ones showing beheadings - investigators say they worry most about the Internet because extremists can reach a broad audience with relatively little chance of detection.

By examining sites like those stored inside the Clifton business, investigators are hoping to identify who is behind them, what links they might have with terror groups, and what threat, if any, they might pose.

And, in a step that has raised alarms about infringing on civil liberties and so far proved unpersuasive in the courtroom, prosecutors are charging that those administering these sites should be held criminally responsible for what is posted.

Attempting to apply broad new powers established by the Patriot Act, the U.S. government wants to punish those who it charges provide "expert advice or assistance." Those that do, the government says, play an integral part of a global terror campaign that increasingly relies on the Internet.

Deputy Secretary of Defense Paul Wolfowitz has called such Web sites "cyber sanctuaries."

"These networks are wonderful things that enable all kinds of good things in the world," Wolfowitz said of the Internet. "But they're also a tool that the terrorists use to conceal their identities, to move money, to encrypt messages, even to plan and conduct operations remotely."

Many question the government's strategy of trying to combat terrorism by prosecuting Web site operators. "I think it is an impossible task," said Thomas Hegghammer, who helps monitor the use of the Internet by Al-Qaeda. "You can maybe catch some people. But you will never ever be able to stem the flow of radical Islamic propaganda."

The government faces many hurdles in pursuing virtual terrorists. While many militant Islamic message boards and Web pages reside on computer servers owned by Internet companies in North America, concerns like Fortress ITX say it would be impossible - and unethical - for them to keep track of the content stored within their equipment.

"It is hideous, loathsome," said Robert Ellis, executive vice president of Fortress, after viewing postings from the Arabic-language Web site for which his company was host, that of Abu al Bukhary. "It is the part of this business that is deeply disturbing." His company shut down the site last month after learning of it from a reporter.

The intense focus on Muslim-related sites like Abu al Bukhary has provoked charges that the effort against cyber sanctuaries is really a misguided anti-Muslim campaign that is compromising important rights guaranteed by the U.S. Constitution.

Arsalan Iftikhar, legal director for the Council on American-Islamic Relations, said that the effort "opens the floodgates to really marginalizing a lot of the free speech that has been a hallmark of the American legal and political system."

"Globally," he added, "it really does nothing but worsen the image of America in the rest of the world."

A self-proclaimed terrorist hunter, Rita Katz, engages in such detective work. She is an Iraqi-born Jew whose father was executed in Baghdad in 1969, shortly after Saddam Hussein's Baath Party came to power.

Finding terrorists has become the major goal for Katz, who began going to pro-Palestinian rallies and fund-raisers disguised as a Muslim woman in the late 1990s, then presenting information to the U.S. government in an attempt to prove there were ties between Islamic fundamentalist groups in the United States and terror organizations.

While agencies like the National Security Agency, the FBI and the Department of Homeland Security monitor terror sites on the Internet and sometimes track users, they have also turned for help to groups like Katz's, the Search for International Terrorist Entities Institute. Katz's group, which has government contracts and corporate clients, may be the most influential of those organizations.

While some experts praise her research as solid, several targets view her as a vigilante. Several Islamic groups and charities, for example, sued for defamation after she asserted that they were terrorist fronts, even though they were not charged with crimes.

Knocking militant groups off the Internet for a day or two by urging individual Web host companies to shut the sites down did not accomplish much, Katz believed. So the government, in an unusual alliance with Katz, has been testing a different strategy.

Sami Omar al-Hussayen was their first target.

He had arrived at the University of Idaho in 1999 to pursue a doctorate in computer science.

Hussayen established a series of Muslim-related Internet sites and served as the regional leader of Islamic Assembly of North America, a group that described itself as a charitable organization, but which prosecutors said recruited members and instigated "acts of violence and terrorism."

Along with news from the Middle East and interviews with scholars, the sites included more disturbing information.

Videos displayed the bodies of dead suicide attackers as a narrator declared that "we had brethren who achieved what they sought, and that is martyrdom in the cause of Allah." Requests were posted for donations to Chechen groups that were trying to "show the truth about Russian terrorism." Clerical edicts appeared on topics including "suicide operations against the Jews."

The Justice Department did not charge that Hussayen had created the material for the militant site. Instead, by registering the Web sites, paying for them and posting the material, he was accused of aiding an extremist cause.

Hussayen's lawyers countered that their client was doing little more than expressing his free-speech rights. David Neven, one of the lawyers, said of Katz and the Justice Department: "They were wildly too zealous. This was not within a country mile of the kind of behavior that this nation has any business trying to criminalize." The jury was unconvinced by the government's case and acquitted Hussayen. The setback has not stopped the government. In July, a warrant was issued in Connecticut for Babar Ahmad, resulting in his arrest in London on Aug. 5. Ahmad, a computer technician at a London college, is accused of setting up Internet sites from 1997 to 2003 to recruit terrorists and raise money for them.

"If you're going to use cyberspace, we're there and we're paying attention," Kevin O'Connor, the U.S. prosecutor for Connecticut, said after Ahmad's arrest.

The United States is trying to persuade Britain to extradite him, drawing protests from Muslim groups and civil libertarians in Britain. In a letter from his prison cell that was posted on the Internet, Ahmad asserted that he was imprisoned "to strike terror and fear into the hearts of the docile, sleeping Muslim community."

Katz said she was not discouraged by the criticism of the prosecutions. "When you call for the death of people and then it results in actions - that is beyond the First Amendment," she said. "You are organizing a crime."

Source: www.iht.com/articles/540326.html

BGU Web Scanner Can Detect Terror Content

Engineering faculty researchers at Ben-Gurion University of the Negev reported recently that they have developed a system that can identify 95 percent of Internet pages with terrorism-related content.

The experimental system, which is being developed to detect information regarding terror activity automatically, was designed by Dr. Mark Last of the Department of Systems Information Engineering at BGU, and Prof. Abraham Kandel of the National Institute for Systems Test and Productivity, in the United States.

The system is based on the recognition of patterns in texts with terror content, based on examples from existing Internet sites. It uses these patterns to identify "hits" by surfers on other sites with similar characteristics, in order to locate users affiliated with terror organizations and new sites set up by terrorist elements, among other things.

According to Last, the development has great importance in view of the considerable use of the Internet in coordinating and orchestrating terror acts.

"The lack of ability to enforce limitations on Internet users allows terror organizations to set up Internet sites that spread incitement, raise money in support of terror and find new supporters for their causes," Last said.

Source: www.haaretz.com/hasen/spages/465047.html