GEORGE C. MARSHALL
EUROPEAN CENTER FOR SECURITY STUDIES™

O'Sullivan, Arieh. "Virtual Terror: Threat of a New World Disorder."
The Jerusalem Post, 27 March 1998, pp. 1-5.
Reprinted by permission of The Jerusalem Post.

Virtual Terror: Threat of a New World Disorder

Arieh O'Sullivan

In today's computer age terrorists are searching for ways to cause havoc by remote control - but Israel has only just woken up to the threat. Arieh O'Sullivan talks to the cyber-terrorism experts.

Ever lie awake at night wondering if legions of mercenary hackers, in league with terrorist organizations or *rogue states*, are working to bring down banks and stock exchanges and cripple vital infrastructures with computer viruses and other malevolent software?

Naw, it's just a dream. This James-Bond type of nightmare is too far off to be real.

And then you wake up to reports that an Israeli teenage master hacker has been caught after mounting a sophisticated cyber-assault on the Pentagon computer systems.

And then you start wondering: Was that crash of the Hong Kong stock market last fall perhaps some plot of a mad terror group?

According to experts in terrorism and *Information Warfare* specialists, we are on the verge, if not already in the midst, of the "cyber-terrorism" age. Add to this the threat of unaccounted-for nuclear bombs - some that can fit into a suitcase - and biological weapons, and you've got "super-terrorism."

"This is a new form of warfare. It isn't conventional, and we have to think about the unthinkable," says terrorism expert Prof. Yonah Alexander.

Thinking about the unthinkable was exactly what a gathering of experts did in Israel last week. They came from around the world to discuss the phenomenon at an international conference called Threats of the Technological Age, co-sponsored by the Terrorism Studies Program at George Washington University, the Inter- University Center for Terrorism Studies in Holon and Tel Aviv University's Curiel Center for International Studies. Not surprisingly, perhaps, participants came up with more questions than answers.

Conference organizer Alexander believes that the globalization of cultures, economies and security opens us up to a "new world disorder" and a globalization of crime and terrorism.

Technology has created an interconnected world. But the benefits of this contain a great flaw, with each connection creating new exposures and risks, making us more vulnerable.

IN OTHER words, today's problem is that there are too many "doors," and you can never be sure who will drop by for a visit via the Internet.

"We are moving toward a new age of Internet or 'click' terrorism, Alexander says."Like Kodak used to say: 'Push the button, and we'll do the rest.' This is the new face of terrorism in the future."

According to Alexander, author of numerous books on terrorism, today's terror groups, including Hizbullah and Hamas, use the Internet for propaganda and psychological warfare purposes. (If you want a taste, check out Almanar.com.)

But, says Alexander, the Internet is also being used by terror groups to recruit members and transfer orders. In some ways, he notes, the Internet has replaced military training camps by putting recipes for bombs on line.

"Today there is basically no need for training camps, because you can get information on the Internet on how to make both conventional and non-conventional weapons," Alexander says. But that's just the mild stuff.

Alexander notes that in today's computer age you don't need tanks and infantry to disrupt a country's infrastructure. It can be done by someone sitting in front of a computer screen tens of thousands of miles away.

Examples of cyber-terrorism made their rounds at the conference. One was the idea that terrorists could alter the formula at a food-company plant, poisoning its product.

Terrorists can and do use the Internet to put out disinformation, search for targets, steal information and work to alter opinions through chat groups.

"You have a clear-cut proof of agent coordination," says Dr. Joseph Hershko, a lecturer and scientist at the Center for Technological Education in Holon. Hershko has developed a program to send 20,000 e-mail messages an hour.

"This is sabotage," he notes grimly. "If I sent you 20,000 e-mails an hour your server would crash."

There was general agreement at the conference not to say too much - "because I don't want to give anyone any ideas," as one participant put it.

What else could cyber-terrorists do?

ONE US scenario goes something like this: Using hacked information, a list of employees at a highly classified military installation could be put together. By manipulating computer records, a designated person's credit rating could be demolished, thus removing him from sensitive positions.

With the right timing and frequency, the move could be done just before the onset of hostilities, thus confounding the installation's capabilities.

Sounds complicated and confusing? In fact, much of cyber-terrorism is intangible. One of the most problematic aspects of the phenomenon is knowing if, and when, you are under attack.

There's another difficulty. Once you recognize you are under cyber-terrorist attack, it's hard to figure out who it is that is attacking you. This of course makes retaliation even more complicated and diminishes the effect of deterrence.

Thus, should the water system fail, knocked out by a bug in the electric company, the only thing a government can do is... fix it.

No revenge. No air strike on a hidden guerrilla camp. Nothing but hire a slew of computer experts to set up what are called "firewalls" to prevent it happening again.

MARVIN Leibstone, an *Information Warfare* analyst and former army colonel, believes cyber-terrorism isn't a full reality... yet.

"The tactical inventory of political terror groups is rapidly declining," says Leibstone, a former member of the US Marines Green Berets unit. Leibstone says that improvements in security have made it much more difficult to take hostages, stage guerrilla attacks and launch bombs than in the past.

"Terrorists are looking for remote means of causing havoc," Leibstone says, citing possible ways groups could use the Internet overtly to push forward their cause.

They could negotiate on line, and by breaking into a computer could, for example, demonstrate certain scenarios their group intended to carry off. They could control resources, and let the world know they were doing it.

Other examples, says Leibstone, include holding a referendum on line - the results of which could be used to show that their group had more popular support than previously thought, thus forcing governments to alter their policies.

According to Alexander, cyber-terrorist attacks could come from other sources too.

A disgruntled employee, an irresponsible computer hacker, an organized crime syndicate or a hostile foreign *Nation* - all of these could unleash cybernetic sabotage.

Targets could include telecommunications, electric *Power* systems, transportation and oil and gas distribution, as well as banking and finance, water supply systems, government services and even such emergency services as medical, fire, police and rescue.

In many cases,damage in one area will have a domino effect.

This begs the question of whether *Defense* against this kind of threat to a nation's vital interests is the responsibility of the military or the government. (And there are those who say that what we are up against isn't cyber-terrorism at all, just plain old crime with a new twist.)

Leibstone believes that in the US the free market will come up with a solution to the cat-and-mouse game with hackers and terrorists. But in Israel, Alexander says, we are in a heap of trouble.

He states it as fact that Israel's traditional terrorist enemies - Hamas, Hizbullah and the PLO - have sent students abroad specifically to study computer science and nuclear physics.

"Israel is just beginning to wake up to this threat," Alexander says, adding that, "in general, all societies are vulnerable. We are in the same boat as other technological societies. Potentially anyone with a computer can break into systems."

But Dr. Ariel Sobelman of the Jaffee Center for Strategic Studies at Tel Aviv University points out that most break-ins are carried out by smart kids who aren't terrorists. Clearly, the fight against this cannot be conducted in the same way as a country would fight terrorism.

"The reason virtual or cyber-terrorism has not yet appealed to terrorist organizations is psychological," Sobelman says. "The terrorist mind needs immediate gratification from an action; I'm not sure virtual fear translates very well."

Sobelman also believes that terror groups are not yet sophisticated enough to cause "cataclysmic" damage to the world with computers. This, he surmises, could be accomplished only on a state level, manifesting itself during an all-out conflict.

KEVIN STEVENS makes his living helping companies and governments protect their computer systems. He belongs to a whole coterie of *Defense* analysts and security consultants who gleefully spread doom-and-gloom stories.

Stevens notes that only 5 percent of America's $7.5 trillion economy is actually in hard currency. The rest is electronic. Scary.

He suggests confounding cyber-assault with "biometrics": the use of palm prints, iris and voice patterns and DNA characteristics in gaining access to computer systems.

But for the moment, Stevens admits, hackers have the upper hand.

"With the dismemberment of the Soviet Union sophisticated computer operators in their intelligence apparatus found themselves needing to make money. Many headed to the Mafia crime organizations. They are the biggest exporters of cyber-terrorism," Stevens says.

In the US, President *Bill* Clinton is reportedly expected to sign a historic directive to protect the US from what is being dubbed an "electronic Pearl Harbor." The directive is to include a series of far-reaching initiatives to bolster America's protection against computer attacks and focus on cyber-security and infrastructure protection.

According to Jane's *Defense* Weekly, the Pentagon suffered over 250,000 break-ins last year.

One particularly "heavy duty" information attack on a Pentagon computer came during the recent crisis with Iraq, but Pentagon officials claim it was unrelated.

Soon afterwards FBI agents came here to investigate the serious break-in; and almost immediately after that police detained Ehud Tannenbaum, the 18-year-old Israeli hacker known as "Analyzer." Could Tannenbaum - or someone like him - have been the perpetrator?

Experts say that even if Tannenbaum was responsible, that means he's smart - but, despite the media hype, not that sophisticated an operator.

ONE FEAR is that freelance hackers will offer their services to terror groups, or even countries, for a profit.

According to recent reports, a Dutch hacker ring called High Tech for Peace allegedly went to the Iraqi embassy in Paris during the US Gulf *War* buildup and offered to foul up the network handling logistics messages between bases in the US and the American military units in Saudi Arabia. According to John Fialka's book, *War* By Other Means: Economic Espionage in America, Saddam Hussein turned down the offer.

Hussein and scientifically-challenged terror groups are reportedly more interested in less sophisticated doomsday toys - biological weapons.

The running *Theory* holds that traditional terrorists want a lot of people watching, and not a lot of people dead. The exception to the rule are religious extremists.

"Biological weapons kill people but leave buildings standing, so they are the preferred weapons of religious fundamentalists who want to keep shrines intact," says David Siegrist, a researcher at the Potomac Institute for *Policy* Studies.

Earlier this month, the US Department of *Defense* acknowledged publicly that the military has ultra-secret, covert-action teams to combat cyber-terrorism. Called Special Mission Units, according to the *Defense* News weekly, the teams are also designated to fight the proliferation of weapons of mass destruction.

It cannot be confirmed, but the assumption is that the IDF is also moving in this sphere. According to top IDF scientists, there is a growing computer proliferation in the Middle East. But Arab nations are "pretty primitive.

"The asymmetry is that Israel is more vulnerable to cyber-attack then they are," says one top IDF scientist, who did not take part in the conference and spoke on condition of anonymity.

As Alexander sees it, it is just a question of time until the attack comes.

"In the 1960s, 1970s and 1980s terrorism was manifested by the physical actions of attacks, hostage- taking, hijackings and bombings. The 1990s and the next decade will be seen as the decade of super-terrorism.

"The impending doomsday scenario is not a question of if," warns Alexander. "It's a question of when."

"The Jerusalem Post" March 27, 1998, Friday FEATURES; Pg. 15