

COMPUTERWORLD

[Home](#) [News](#) [Topics](#) [Departments](#) [Services](#) [Subscriptions](#) [Events](#)

You may retrieve this story by entering QuickLink# 34495

[Return to story](#)

Experts: Don't dismiss cyberattack warning

By [DAN VERTON](#)
NOVEMBER 18, 2002

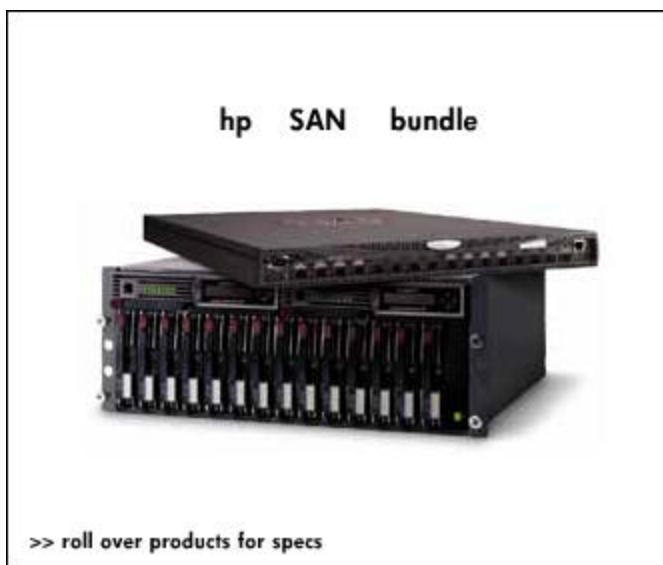
Security experts and two former CIA officials said today that warnings of cyberattacks by al-Qaeda against western economic targets should not be taken lightly.

Vince Cannistraro, the former chief of counterterrorism at the CIA, said that a number of Islamists, some of them close to al-Qaeda, have developed expertise in computer science.

"And some are well schooled in how to carry out cyberattacks," he said. "We know from material retrieved from [al-Qaeda] camps in Afghanistan that this is true. But their expertise seems mostly dedicated to communicating securely among al-Qaeda cells. Cyberattacks would probably render them less secure by focusing attention on their location."

In an exclusive interview with *Computerworld* on Monday, Sheikh Omar Bakri Muhammad, a London-based fundamentalist Islamic cleric with known ties to Osama bin Laden, said al-Qaeda and various other fundamentalist Muslim groups around the world are actively planning to use the Internet as a weapon in their "defensive" jihad, or holy war, against the West.

Bakri, founder of the London-based group Jama'at Al-Muhajirun and the spokesman for Osama bin Laden's International Islamic Front for Jihad Against



Jews and Crusaders ([see story](#)), said all types of technology, including the Internet, are being studied for use against the West.

"In a matter of time you will see attacks on the stock market," he said, referring specifically to the markets in New York, London and Tokyo.

His comments represent the first time that a high-profile radical Muslim cleric with known links to bin Laden has spoken publicly about the use of cybertactics for offensive purposes.

Cyberterrorism experts offered mixed views of whether such attacks could, or would, be carried out. Cannistraro, for example, called Bakri a "fire breather" with no special insight into al-Qaeda operations or plans.

But they stressed that the threat should not be dismissed out of hand.



Sheikh Omar Bakri
Muhammad, founder of the
London-based group Jama'at
Al-Muhajirun
Credit: The Associated Press

According to Bakri, a Syrian-born Muslim cleric whom the FBI and British intelligence have tied to some of the Sept. 11 hijackers and others seeking flight training in the U.S., Islam justifies the use of "all types of technologies" in the defense of Muslim lands, including psychological and economic weapons "or a weapon of mass destruction."

Jihad groups around the world are very active on the Internet, Bakri said, speaking from a cell phone near his north London office. And while his group, Jama'at Al-Muhajirun, is primarily focused on supporting the political goals of Al-Qaeda and other radical Islamic groups, Bakri said the military wings of these various groups are also using and studying the Internet for their own operations.

"That is what al-Qaeda is skillful with," said Bakri. "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," he said, referring to an ongoing threat of an attack.

Michael Caloyannides, a senior fellow at Mitretek Systems Inc., in Falls Church, Va., and a former CIA scientist, said the skills required to launch a strategic cyberattack with devastating economic consequences are far different from what terrorist groups have focused on in the past. However, the Internet remains "very vulnerable" to serious disruptions, including those focusing on domain name servers, border gateway protocol routers and various single points of failure, said Caloyannides.

"While the Internet was originally designed and configured to be survivable, its transformation to a commercial entity has caused it to become economically efficient at the expense of no longer being anywhere near as survivable," said Caloyannides.

He said any such attack launched by al-Qaeda or in direct support of al-Qaeda

could have a significant impact on the Bush administration's war on terrorism. In particular, Caloyannides warned of potentially dire consequences for any nation that knowingly allows such an attack to be launched from systems and networks within its borders. "Any country that allows its territory to be used for a massive Internet attack on the U.S. may want to think twice of the likely consequences," he said.

In April, the CIA sent an analysis paper to the Senate Select Committee on Intelligence outlining the cyberthreat posed by international terrorist groups, particularly al-Qaeda.

"Cyberwarfare attacks against our critical infrastructure systems will become an increasingly viable option for terrorists as they become more familiar with these targets and the technologies required to attack them," the CIA paper stated. "Various terrorist groups, including al-Qa'ida [sic] and Hizballah, are becoming more adept at using the Internet and computer technologies. These groups have both the intentions and the desire to develop some of the cyberskills necessary to forge an effective cyber attack modus operandi."

To date, al-Qaeda's cybercapabilities have been the subject of much debate. Most Internet security professionals have doubted such groups' interest in cyber tactics on the grounds that physical bombings and other forms of attack provide the fear and bloodshed that al-Qaeda is looking for. However, in recent statements made by bin Laden, the terror leader has shown a clear desire to inflict catastrophic damage on the U.S. economy as a way to force the U.S. to withdraw its military forces from Afghanistan and to curtail its support for Israel.

"There are millions of Muslims around the world involved in hacking the Pentagon and Israeli government sites," said Bakri. "The struggle will continue," he said, referring to the millions of young bin Laden supporters who are now studying computer science as a way to support the cause.

"I believe that Osama bin Laden has earned his leadership and most [Muslim students] who are graduating in computer science and computer programming and IT technology are supporting Osama bin Laden," Bakri said.

"I would advise those who doubt al-Qaeda's interest in cyberweapons to take Osama bin Laden very seriously," he said. "The third letter from Osama bin Laden a few months ago was clearly addressing using the technology in order to destroy the economy of the capitalist states.

"This is a matter that is very clear, and Osama bin Laden must be taken very seriously."

Just last week, an intelligence threat assessment by Chantilly, Va.-based iDefense Inc. of pro-Islamic, pro-al-Qaeda hacking activity raised concerns about the ongoing development of malicious code by hackers, particularly those based in Malaysia, who are sympathetic to the cause of radical Islamic terrorist groups.

One hacker who goes by the handle "Melhacker" is thought to be responsible for

the Nedal worm ("Laden" spelled backwards). Analysis of the worm conducted by iDefense found that it contained encrypted code and numerous Muslim names whose significance is unclear, as well as at least one and possibly two references to al-Qaeda.

"While this does not prove a direct link to al-Qaeda, it certainly shows empathy to the terrorist organization and an apparent willingness to act on their behalf," the iDefense study concludes.

Melhacker is also reportedly working on a new mega-worm that has been referred to as a "3-in-one." According to iDefense's director of threat intelligence, Jim Melnick, the worm will supposedly combine features of SirCam, Klez and Nimda and will be named Schezda.

"This should be viewed as a major threat," wrote Melnick in the iDefense study. "The continuing development of malicious code from pro-Islamic and pro-al-Qaeda hackers, especially in Malaysia, is of great concern, and one that needs to be closely watched."

The public threat from Bakri may be part of the attack. Steven Aftergood, a defense and intelligence analyst at the Federation of American Scientists in Washington, said statements such as Bakri's are "themselves a crude form of information warfare," intended to incite, alarm and confuse. "They need to be viewed dispassionately in that light," said Aftergood.

"There is always room for improvement in information systems security," he said. "And it would be prudent to take the existence of an adversarial threat seriously."

Officials at the White House said Richard Clarke, chairman of the President's Critical Infrastructure Protection Board, and his vice chairman, Howard Schmidt, are unavailable for comment.

[Join an online discussion on this article in our Security Knowledge Center.](#)

Source: Computerworld

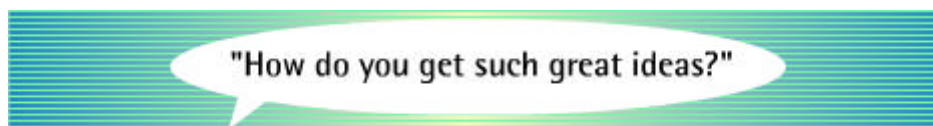
Sponsored Links

Prove the Business Value of IT! Attend Computerworld's Premier 100 IT Leaders Conference, Feb 23-25 in Scottsdale!

Free Trial The Advisory Council, practical peer advice for solving IT problems

Learn how to receive a Cisco router valued at \$3,500

[About Us](#) [Contacts](#) [Editorial Calendar](#) [Help Desk](#) [Advertise](#) [Privacy Policy](#)



Copyright © 2003 Computerworld Inc. All rights reserved. Reproduction in whole or in part in any form or medium without express [written permission](#) of Computerworld Inc. is prohibited. Computerworld and Computerworld.com and the respective logos are trademarks of International Data Group Inc.