

Cyberthreats not to be dismissed, warns Clarke

By DAN VERTON
JANUARY 03, 2003

The U.S. has ignored warning signs before: two attempts by al-Qaeda in 1994 to use airplanes as weapons, as well as public statements in 2000 about terrorists being trained as pilots.





Now Richard Clarke, chairman of the President's Critical Infrastructure Protection Board, is trying to prevent new warning signs from being ignored -- signs that al-Qaeda's brand of terrorism has a growing cyberelement and that the nation's economy is at risk.

Before taking his current post in October 2001 (see story), Clarke advised two presidents on cybersecurity and served as the country's first counterterrorism coordinator. Most of his time now is spent raising awareness of the changing nature of terrorism and the increasing relevance of cyberterrorism to the stated goals of groups such as al-Qaeda.

"Cyberspace still is underappreciated as a threat, and the solutions aren't as obvious as they are with physical security," said Clarke during an exclusive interview with *Computerworld* late last month. "We have no clue as a country how to protect our cyberspace. It is a totally different kind of issue."

Clarke said vulnerabilities in the nation's critical infrastructure stem mainly from unknown security holes in widely deployed software and from the constant influx of

new technologies that often have unintended consequences for security.

One of his biggest concerns is the growing use of wireless technologies, he said. There have already been cases in Spain and Japan in which PC-based worms have infected hundreds of next-generation cell phones, tricking them into dialing local 911 emergency systems, Clarke added.

"Now, if you're a terrorist, the first thing you might want to do before an attack is take down the 911 system," he said.

According to Clarke, the Sept. 11 terrorist attacks were a turning point for the national effort to protect cyberspace.

"Before Sept. 11, [al-Qaeda] was interested in killing as many people as possible," he said. "After Sept. 11, [Osama bin Laden] starts talking about destroying the American economy. And he starts to talk about going after the economic infrastructure of the United States. You could drive around a lot of truck bombs and really not do a lot of damage to the economic infrastructure because it's so diverse and dispersed. But if you do it in cyberspace, you might have the ability to hit the entire financial services network simultaneously."

Clarke said he's aware that many people doubt the willingness and ability of terrorist organizations to carry out strategic cyberattacks against the U.S. But he said it's his job to think differently about the future -- and to do what some officials failed to do in the months leading up to Sept. 11.

"There are a lot of different people who can conduct cyberwarfare," Clarke said. "There are countries that are creating cyberwarfare units. There are criminal groups engaging in cybercrime. There are also some terrorist groups we know are looking at using cyberattack tools. But I don't spend a lot of time trying to figure out who's going to be the next attacker."

Eliminating al-Qaeda, for example, "won't end the threat to us from cyberspace," he said.

And therein lies the challenge, according to Clarke. The U.S. needs to take the target of cyberspace away from its enemies by eliminating vulnerabilities, he said.

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.