TERRORISM
RESEARCH CENTER

The Terrorism Research Center
TRC Analysis - June 27, 2002
www.terrorism.com

Taking Cyberterrorism Seriously

Failing to Adapt to Emerging Threats Could Have Dire Consequences

Matthew G. Devost and Neal A. Pollard

The ability to identify and adapt to emerging threats is a critical component of the U.S. homeland security strategy. An article in today's Washington Post highlights several key pieces of evidence that support the notion that terrorists are looking to acquire a cyberterrorism capability. What this would portend is a major shift in operations, not only of al Qaeda, but of the terrorist threat in general. This is important to identify: counterterrorism strategies depend on an understanding of how terrorists are likely to attack, what targets they will attack, what weapons they will use, and what tactics and methods they will use to deliver their attacks. When terrorists take us by surprise, as they did on 9/11, it is because we did not identify or understand the change in these areas, and adjust our strategies accordingly. Terrorists take advantage of this fact, not only to increase the immediate damage of their attacks, but to increase the longer-term psychological impact.

As pioneering terrorist groups demonstrate the operational effectiveness of certain weapons, tactics, or targeting, other terrorist groups pursue similar lines. This is the area it is most important for our intelligence community to track, to avoid being taken by surprise when terrorists change their tactics, weapons, or targets. It is easy to understand when terrorists change on the strategic level - their communiqués and media statements usually are straightforward in their goals and desires. At the tactical level of specific attacks, it is almost impossible to design systematic strategies for identifying the immediate threat to the finer details of exactly where, when, and how. But at the operational level, how terrorists plan to use weapons, plan to deliver them, and plan to identify targets, one can observe and try to predict major changes in these areas that would imply a need for different, adaptive counterterrorist strategies. A change in al Qaeda operations - from truck bombs on embassies, to suicide planes against skyscrapers, to a "combined arms" attack on infrastructures with physical and information weapons - would demand a change in a US counterterrorism strategy that is already struggling to keep up with the last attack.

It is unlikely that a terrorist organization like al Qaeda currently posses the capability to launch a sustained cyberterrorism attack against critical infrastructures. The ability to launch a sustained attack with national strategic implications requires extensive planning and expertise that would take years to acquire.

However, it is possible that an isolated cyberterrorism attack would be used in one of the following scenarios:

In Parallel with a Physical or WMD Attack

It is likely that terrorist organizations will seek to enhance the impacts of conventional attacks through the use of cyberterrorism attacks. The objective of the attack would be to reduce our response capability thus increasing the impact of the physical attack. For example, a terrorist organization might seek to disrupt emergency response communications or in the event of a chem/bio, nuclear or radiological attack, they might seek to disrupt key weather data that would be used to calculate the dispersion of harmful material for the creation of evacuation areas and/or evacuation routes.

To Decrease Confidence in Critical Infrastructures/ Psychological operations
Isolated attacks against critical infrastructures could be used to create panic and decrease public confidence in critical infrastructures. Attacks against financial, transportation or vital human services would cause significant panic and impact our economic security.

To Cause Physical Damage and/or Loss of Human Life
Cyberterrorism attacks against select infrastructures could be used as an alternative to conventional physical attacks to facilitate the accomplishment of traditional terrorist goals such as the loss of human life and destruction of property.

Insights into emerging threats provide opportunities to creatively adapt our homeland security posture to help deter, prevent and respond to cyberterrorism attacks. Our current security posture, within both the private and public sectors, has left us increasingly vulnerable and we must act now to enhance our ability to deal with the cyberterrorism threat. The threat as outlined in today's Washington Post is hopefully still immature, but al Qaeda has always sent us clear signals on what they are interested in. We ignore these signals at our peril. Al Qaeda is not the last terrorist threat the US will confront, and indeed it may not be the first to successfully use information terrorism on a massive scale. However, we are not yet prepared – in strategy, policy, or organization – to deal with this threat. Several strategic directions must be followed before we are prepared, to include:

- Integrating, from the bottom up, policies, strategies and organizations to protect infrastructures from both physical *and* cyber attack, across the full range of critical infrastructures
- Engaging the private sector, with realistic incentives, as the first line of detection and defense against cyber attack
- Identifying and hardening critical infrastructure nodes and links – cyber and physical – that support our ability to respond to physical terrorist attacks
- Actively conducting red teaming and vulnerability assessments against critical infrastructures to identify and mitigate critical vulnerabilities and to detail infrastructure interdependencies
- Refocusing private-public sector information sharing initiatives to develop common protocols for reporting and cross-infrastructure information sharing
- Keep the military's computer network attack and computer network defense operations together as an activity, located at the recently announced merged command of Strategic Command and Space Command, rather than at Northern Command or a civilian Department, and develop this activity into a cyber equivalent of North American Aerospace Defense Command (NORAD).

Building on these and other bases of policy and strategy will prepare us for the inevitable day when terrorism successfully and irreversibly crosses into cyberspace.

Matthew G. Devost is the President and CEO of the Terrorism Research Center, Inc.

Neal A. Pollard is the Senior Director for Emerging Threats and Capabilities at Hicks and Associates, Inc. and is a Founding Director of the Terrorism Research Center, Inc.

About the Terrorism Research Center, Inc.

Founded in 1996, the Terrorism Research Center, Inc. (TRC) is an independent institute dedicated to the research of terrorism, information warfare and security, critical infrastructure protection and other issues of low-intensity political violence and gray-area phenomena. The TRC represents a new generation of terrorism and security analysis, combining expertise with technology to maximize the scope, depth and impact of our research for practical implementation.

The TRC provides core expertise in terrorism, counterterrorism, critical infrastructure protection, homeland security, information warfare and security (including design review, technical assessments, policy development and review, and training), vulnerability and threat assessment (red teaming), systems engineering, encryption, intelligence analysis, and national security and defense policy.

For more information:

Terrorism Research Center, Inc.
5765-F Burke Centre Parkway
PMB 331
Burke, VA 22015
www.terrorism.com
trc@terrorism.com

Media Relations:

Michelle Gabelmann
Lincoln Park Public Relations
michelle@terrorism.com
703-465-0276