

# Cyber Terrorism: Political and Economic Implications

## Book Questions

1. *What is cyber terrorism?*

Cyber terrorism is a premeditated, politically motivated criminal act by sub-national groups or clandestine agents against information and computer systems, computer programs, and data that result in violence where the intended purpose is to create fear in non-combatant targets.

2. *Are terrorists really that skilled?*

The new emerging form of terrorism uses asymmetric warfare. Threats to information systems are outside conventional warfare. Groups like al Qaeda are learning organizations that have shown their ability to use our own technology against us. They have also shown a long-term planning and preparation approach to their attacks. Many of their leadership are from middle class or higher families. These people are neither ignorant nor stupid. Remember, the leaders of the September 11<sup>th</sup> attacks went to Western universities and received masters degrees in a host of technical areas

3. *Just how serious is the threat of cyber terrorism?*

So much of our livelihoods now depend on the secure use of computers for communications, transportation, banking, medical, etc., and these systems have been penetrated by hackers, crackers and cyber criminals for quite some time. Imagine what would have happened if mobile phone service were disrupted just prior to a major chemical attack. Visualize having your blood type changed in a medical database before a major operation. Law enforcement is working to integrate their computer systems to provide better sharing of criminal and terrorist activities. In the past, people have demonstrated their ability to break into judicial and law enforcement systems and actually remove their criminal histories. Envision a cyber terrorist removing five people from a watch list hours before they board a jetliner. Imagine having your identity stolen and used to rent an apartment that was

used to make the bombs that blew up a subway system. Imagine how this one event could change your whole life.

4. *What is being done about cyber terrorism on a micro level?*

Security comes in three parts: protective systems such as the encryption of communications and data, mechanisms and supporting technologies; configuration and maintenance such as access controls, and proper and timely updates; and people involving policies and procedures for the proper use of systems, and general awareness and security reporting. All three must be considered to ensure your systems and networks are secured. This can be accomplished by establishing a strong security awareness program, establishing a comprehensive security policy, creating and implementing a comprehensive disaster recovery plan, implementing the latest security technologies, conducting regular security audits, and working with law enforcement when security breaches do occur.

5. *What can be done about cyber terrorism on a macro level?*

We now live in the information age. This means information is power, and whoever controls that information controls the power. In open, democratic societies, it is the individual citizen who must take back their ownership and assert their right to privacy. Legislative and judicial activities must reflect this orientation if we are to secure our livelihoods and daily activities. Abuses and poor security management must have penalties sufficient to discourage information mismanagement abuse. This in turn will limit the opportunities available to cyber terrorists.