Chapter 12

The Future of High-Technology Crime

Chapter Outline

I. Introduction

A. Three future high-technology criminal issues:

1. The intersection of technology and terrorism.
2. The modification of the legal system to respond to high-technology crimes.
3. The globalization of cybercrime and how the worldwide nature of many high-technology crimes has affected the international response to the problem.

II. Cyberterrorism

A. Terrorism—Politically motivated attacks that are preplanned and staged in such a manner as to instill fear into the general population.

B. Perpetrators are extremely dedicated to their mission and are often willing to sacrifice their own lives in order to complete their mission.

C. The Computer Fraud and Abuse Act was modified by the USA PATRIOT Act to include a definition related to cyberterrorism: Any conduct that causes (or, in the case of an attempted offense, would, if completed, have caused)— (i) loss to one or more persons during any one-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting one or more other protected computers) aggregating at least $5,000 in value; (ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals; (iii) physical injury to any person;(iv) a threat to public health or safety; or (v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security.

1. One problem with the above definition of cyberterrorism is that for an individual to be charged with an act of cyberterrorism it must be shown that the individual could have committed the act in question.
2. There is debate whether each of the above acts is worthy of being termed "terrorism."

D. Representatives Dorothy Denning defined cyberterrorism as "unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political and social objectives."

1. Prevents the confusion of the earlier definition and continues to address cyberterrorism in light of potential threats to society at large.

E. What Acts Qualify as Acts of Cyberterrorism?

1. There have been numerous reported instances of cyberterrorism over the last 10 years.
   a. Many of these examples range from not being representative of cyberterrorism to being examples of outrageous uses of technology.
2. Because there is great potential for future terrorist attacks, the National Security Agency (NSA) hired 35 hackers to conduct a controlled experiment of the nation's critical infrastructure in 1997, in what was called Operation "Eligible Receiver."

      a. Hackers gained access to more than 36 of the Department of Defense’s computer networks, the power grids of four major cities, simulated a plane crash as the result of accessing an air traffic controller, and more.
   3. Over the last few years there have been some reported instances of cyber-related terrorism abroad, but there has been no major discussion concerning the activity.

F. What Acts Are Not Cyberterrorism?
   1. There have been several crimes to be inappropriately termed cyberterrorism.
   2. To be considered cyberterrorism, the behavior must fall into one of the following categories:
      a. Serious financial loss of $5,000 against a protected computer.
      b. Physical injury to any person.
      c. Threat to public health or safety.
      d. Damage inflicted upon a computer system used by a government entity in furtherance of the administration of justice, national defense, or national security.
   3. It is important to note that only those crimes with serious potential for physical harm are labeled cyberterrorist acts.

G. Evolution of the Legal System
   1. It is necessary for the legal system to develop clearer guidelines associated with high-technology crime.
      a. By this it is meant that there must be:
         i. Adequate criminal structure addressing the various high-technology crimes and their punishments.
         ii. Consistent rulings from the courts as to how the law can be applied to investigations of high-technology crime.
   2. Adequate criminal structure addressing the various high-technology crimes and their punishment.
      a. State and federal governments have consistently improved in this area.
      b. There are debates as to whether the penalties associated with these crimes are sufficient.
   3. Consistent rulings from the courts as to how the law applies to investigations of high-technology crimes.
      a. There are some doubts that the legal system can handle the problem of high-technology crimes, and many believe that technology continues to evolve faster than the legal system.
         i. Some argue that as quickly as legislation is passed or court decisions come down, the technology may change and the ruling and/or statutes become obsolete or inapplicable to the particular behavior in question.
      b. At one point, legal scholars argued that the answer to the problem involved the use of code-based regulation.
         i. Software designed to regulate and prevent unlawful use.
         ii. The problem with this solution is that so many cybercrimes involve the use of technology that has been either created for or modified for use in criminal activity.
      c. A second possibility involves the continued development of high-technology crime investigation teams.

i. In recent years, a growing number of organizations have arisen to develop training programs for law enforcement personnel.

ii. There has also been an increase in cybercrime-related investigations and computer forensics courses at universities.

iii. There may still be a disconnect between the desire to maintain such a team and having the resources to staff and train such a team.

4. Given the situation of the legal system, there has been a movement whereby the control of high-technology crime is believed to be associated with target hardening of victims, which involves educating potential victims of the dangers associated with technology-related behavior.

I. The Globalization of Cybercrime

A. Cybercrime is considered to be a global problem.

B. The problem is that while crimes may be legal in one area of the world, they may not be illegal in all areas of the law.

C. Because cybercrimes do not always require a physical presence, there are situations in which an offender will operate from another part of the world.

D. Globalization—The sharing of cultural, capital, or technological ideas.

E. With the vast number of potential sites of cybercrime-related activity, the question has become one of how the world's legal systems should respond to the high-technology crime problem.

1. One solution suggested was the creation of an international law enforcement task force designed to investigate cyber-related crimes, but there has been little support for such a task force.

2. There is a movement being developed that would allow for greater standardization of cybercrime legislation.

a. The Convention on Cybercrime was initiated in 2001.

i. The Convention attempts to get member states (countries) to pass legislation that criminalizes high-technology crimes such as: intellectual property theft (file sharing), hacking and computer intrusion, forgery and fraud, and the manufacture and distribution of child pornography.

ii. It also allows for greater cooperation between law enforcement agencies and Internet Service Providers (ISPs) by clarifying the situations in which government agents can request information from ISPs.

iii. Only 20 countries have ratified the document.

II. Conclusion

Key Terms

Code-based regulation: Software designed to regulate and prevent unlawful use.

Cyberterrorism: Unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.

Deterrence theory: The belief that punishment is used to ensure that a person does not engage in future criminal behavior.

Globalization: The sharing of cultural, capital, or technological ideas.

Target hardening: Ensuring through education that potential victims are more cautious, thereby reducing the number of victims.

Terrorism: Politically motivated attacks that are preplanned and staged in such a manner as to instill fear in the general population.