**Terrorismo,** e o Ciberterrorismo (início da pesquisa)

Just how real is the threat that cyberterrorism poses? Because most critical infrastructure in Western societies is networked through computers, **the potential threat from cyberterrorism is, to be sure, very alarming. Hackers, although not motivated by the same goals that inspire terrorists, have demonstrated that individuals can gain access to sensitive information and to the operation of crucial services.** Terrorists, at least in theory, could thus follow the hackers’ lead and then, having broken into government and private computer systems, cripple or at least disable the military, financial, and service sectors of advanced economies. **The growing dependence of our societies on information technology has created a new form of vulnerability, giving terrorists the chance to approach targets that would otherwise be utterly unassailable, such as national defense systems and air traffic control systems.** **The more technologically developed a country is, the more vulnerable it becomes to cyberattacks against its infrastructure.**

**The roots of the notion of cyberterrorism can be traced back to the early 1990s, when the rapid growth in Internet use and the debate on the emerging “information society” sparked several studies on the potential risks faced by the highly networked**, high-techdependent United States. As early as 1990, the National Academy of Sciences began a report on computer security with the words, “We are at risk. Increasingly, America depends on computers. . . . **Tomorrow’s terrorist may be able to do more damage with a keyboard than with a bomb.”** At the same time, the prototypical term “electronic Pearl Harbor” was coined, linking the threat of a computer attack to an American historical trauma.

Most notably, Dorothy Denning, a professor of computer science, has put forward an admirably unambiguous definition in numerous articles and in her testimony on the subject before the House Armed Services Committee in May 2000:

**Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks 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. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear.** Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

Cyberterrorism is an attractive option for modern terrorists for several reasons.

• First, **it is cheaper than traditional terrorist methods**. All that the terrorist needs is a personal computer and an online connection. Terrorists do not need to buy weapons such as guns and explosives; instead, they can create and deliver computer viruses through a telephone line, a cable, or a wireless connection.

• Second, **cyberterrorism is more anonymous than traditional terrorist methods**. Like many Internet surfers, terrorists use online nicknames—”screen names”—or log on to a website as an unidentified “guest user,” making it very hard for security agencies and police forces to track down the terrorists’ real identity. And in cyberspace there are no physical barriers such as checkpoints to navigate, no borders to cross, and no customs agents to outsmart.

• Third, **the variety and number of targets are enormous**. The cyberterrorist could target the computers and computer networks of governments, individuals, public utilities, private airlines, and so forth. The sheer number and complexity of potential targets guarantee that terrorists can find weaknesses and vulnerabilities to exploit. Several studies have shown that critical infrastructures, such as electric power grids and emergency services, are vulnerable to a cyberterrorist attack because the infrastructures and the computer systems that run them are highly complex, making it effectively impossible to eliminate all weaknesses.

• Fourth, **cyberterrorism can be conducted remotely**, a feature that is especially appealing to terrorists. Cyberterrorism requires less physical training, psychological investment, risk of mortality, and travel than conventional forms of terrorism, making it easier for terrorist organizations to recruit and retain followers.

• Fifth, as the I LOVE YOU virus showed**, cyberterrorism has the potential to affect directly a larger number of people** than traditional terrorist methods, thereby generating greater media coverage, which is ultimately what terrorists want.