The Information Society and the Danger of Cyberterrorism

Giampiero Giacomello
Università di Bologna, Italy

INTRODUCTION

Computers have always caused psychological uneasiness in the human brain. That a computer is the closet thing to a thinking machine can be discomforting. That average users have little understanding of the complexity and intricacies of how computers and software operate only add to the distress. Networked computers further increased the puzzlement of human beings. The media (suffering from the same poverty of information as the public) have picked up catchwords like *cyberwar, netwars, cyberterrorism*, and *cybercrime.* Speaking of Electronic Pearl Harbors and comparing modems to bombs have only contributed to increasing the level of media hysteria and confusion in public opinion. Schwartau (1994) is a classic example. Imagine that poorly informed journalists start telling the general public that ruthless hackers (hired by terrorists) could take over the power grid and shut it down, or cause patients' death after their medical records have been compromised. The mere suspicion that terrorists could perform such acts would be enough to fueling the fear factor, which regularly happens as a result of this crying wolf.

Under these circumstances, cyberterrorism seems like a nightmare come true. As Embar-Seddon (2002) noted, the word terrorism brings together two significant modern fears: the fear of technology and the fear of terrorism. Both technology and terrorism are significant unknowns and unknown threats are generally perceived as more threatening than known threats. To some extent, cyberterrorism does not need to be manifested itself in any significant way because many already believe it to be real. This article will try to dispel some of the myths of cyberterrorism, such as the contention that terrorists could remotely take control of critical infrastructure and thus bring a country to its knees. In fact, today, cybercrime and economic damage caused by hackers are far more real and serious threats than terrorists. Misdeeds are more likely to be committed by disgruntled insiders than skilled outsiders (Randazzo et al., 2004).

There is no commonly accepted definition of terrorism, hence cyberterrorism has been variously interpreted. For example, Sofaer et al. (2000) defines it as "intentional use or threat of use, without legally recognized authority, of violence, disruption or interference against cyber systems" (p. 26), resulting in death or injury of people, damage to physical property, civil disorder, or economic harm. The probability, however, that cyberattacks may actually cause victims is extremely low. Furthermore, Sofaer et al. tends to exclude states from committing terrorist acts, which is also debatable. Hughes (2004) observes cyberterrorism as a diverse set of technologies whose purpose is to scare people, but scaring people without getting anything in return is simply useless. Paraphrasing a working definition of terrorism, I would identify cyberterrorism as the use of digital means to threat or undertake acts of organized violence against civilians to achieve political advantages. Perpetrators then could be nonstate groups or sovereign states. Terrorists spreading scary stories to terrify the populace via the Internet would also qualify.

Finally, because of cost efficiency, information and communication technologies have blurred the distinction that long existed between the noncombatant and the combatant spheres. The technology on which the military now rely is exactly the same commercial off-the-shelf hardware and software products that civilians have in their homes and offices (Department of the Army, 2003). Military and civilians alike use largely the same computer networks, which were designed for ease of use and not for hardened communications. During the Cold War, dual use technology (civilian hardware and software) was considered "dangerous" because it could help the Soviets close the gap with the West. Paradoxically, dual-use technologies are now "good." One of the many downsides of such a situation is that if terrorists hit computer networks, in theory, they could hit multiple targets: the economy, law enforcement agencies, emergency services, and (albeit to a lesser extent) even the military. For terrorists this scenario would be a dream come true. Reality, however, is substantially different.

BACKGROUND

The first report to highlight vulnerabilities and risks for societies highly dependent on computer networks was the Tengelin report, in the 1980s (Tengelin, 1981). Soon

Table 1. National critical infrastructures (Source: personal elaboration based on Randazzo et al., 2004, Wenger, Metzger, and Dunn, 2002, Commission of the European Communities, 2004)

E.U.	United States	Australia	Canada
Finance	Banking and finance	Banking and finance	Financial services
Communications and information technologies	Information and telecommunications	Communications	(Tele) Communications and Information services
Energy, oil, gas	Food, energy, water	Energy and utilities	Energy and utilities
Transport	Transportation and shipping	Transport and distribution	Transport
Government	Postal, emergency services, defense industrial base, continuity of government	Other critical government services (e.g., defense and emergency)	Safety
Food and water	Agriculture		Safety
Healthcare	Public health		Safety

sociologists began to explore "the world of high-risk technologies" (Perrow, 1999), where "normal accidents" might occur in risky enterprises, like nuclear power plants or air traffic control, resulting in the deaths of hundreds and crippling the lives of thousands or even millions. After the publication of the Tengelin report, more governments, in primis the U.S. federal government, became sensible to the issues. The issue of computer-dependent societies skyrocketed in the 1990s with the diffusion of the Internet.

In 1998, U.S. President Clinton signed the Presidential Decision Directive 63 (White House, 1998), the first official document to identify "critical" sectors (information and communications, electric power, transportation, oil & gas, banking & finance, water, and emergency services) for protection. Disruption in one or more of these sectors would seriously compromise the survival of the United States as a sovereign country. The U.S. government has revised and refined the list of critical infrastructures several times since 1998 (the Patriot Act of October 2001 also mentioned the necessity to protect the country's critical infrastructures). The most recent modifications were included in the *National Strategy to Secure Cyberspace* in 2003 (White House, 2003). More recently, the E.U. has also come up with a list of critical infrastructures. The items on the E.U. list resemble very closely those sectors identified by the United States government and those of other advanced countries (see Table 1).

The U.S. military first considered "information operations" in the early 1990s. The Gulf War was actually the first information war (Campen, 1992; Libicki, 1995). Information operations involve "actions taken to affect adversary information and information systems while defending ones own information and information systems" (Joint Forces Staff College, 2003, p. 1). Adversaries could be hackers, criminals, vandals, terrorists, transnational groups and nation states. Computer Network Operations are a subset of information operations and may include psychological operations, open source intelligence, *hacktivism* (Denning, 1999), and so on. Perception management (the old propaganda), via selecting bits of information may demoralize the adversary and even obtain that victory without fighting, which Chinese strategist Sun Tzu (400 B.C.) portrayed as superior to other forms of winning.

More worrisome for the United States and other advanced countries is that even non-state actors like terrorist groups could become skilled enough to launch cyberattacks. Alberts (1996) noted that such acts would entail serious consequences for information infrastructures. Among the first to explore this eventuality were RAND researchers Arquilla and Ronfeldt, (1997, 2001), who investigated "cyberwars" and "netwars." Netwars, involving "nonstate, paramilitary, and other irregular forces," would be located "increasingly at the societal end," where "military operations other than war" were (Arquilla & Ronsfeld, 1997, p. 275).

At the end of the 1990s, Nelson et al. (1999) of the Center for the Study of Terrorism noted that "the majority of literature dealing with cyberterrorism has focused principally on the vulnerabilities of critical infrastructures" (p. 3). Exercises like Black Ice or Blue Cascade (Verton, 2003) focused on disruption of critical infrastructures and penetration of supervisory control and data