Chapter XVII
Cybercafés and Prevention of Terrorist Activities

Esharenana E. Adomi
Delta State University, Nigeria

Williams P. Akpochafo
Delta State University, Nigeria

ABSTRACT

The purpose of this chapter is to describe the use of the Internet by terrorists in cybercafés and explore measures intended to stem the use of cybercafés for terrorist activities. Specifically, the reasons terrorists use of the Internet, how they use the Net, their motivations for utilization of cybercafés, various measures adopted in different countries for combating terrorists' use of cafés for their acts, impediment to prevention of terrorism via cybercafés, and future trends are set forth.

INTRODUCTION

Propaganda has traditionally been disseminated by word of month or printed pamphlets distributed through a known network of members and sympathizers. However, the Internet has made information widely available to a more diverse audience than ever before and offers many advantages over the traditional method of publishing—it is relatively cheap in terms of presentation, set up and distribution, in addition to its ability to by pass national laws (Crilley, 2001). When the Internet first appeared, it was hailed as an integrator of cultures and a medium for businesses, consumers, and governments to communicate with one another. It appeared to offer unequalleled opportunities for the creation of a "global village." Today the Internet still offers that promise, but it has also proven in some respects to be a digital menace. It has provided a *virtual battlefield* for peacetime

hostilities between Taiwan and China, Israel and Palestine, Pakistan and India, and China and the United States (during both the war over Kosovo and in the aftermath of the collision between the Navy EP-3 aircraft and Chinese MiG). In times of real *conflict*, the Internet was used as a *virtual battleground* between NATO's coalition forces and elements of the Serbian population. These real tensions from a virtual interface involved not only nation-states but also non-state individuals and groups either aligned with one side or the other, or acting independently. The Internet is being used as a "cyberplanning" tool for terrorists. It provides terrorists with anonymity, command and control resources, and a host of other measures to coordinate and integrate attack options (Thomas, 2003).

Essentially, the national security consequences of the potential use of the Internet by terrorist organizations are now a concern of governments, police, and intelligence agencies (Crilley, 2001).

The story of the presence of terrorist groups on the Net has barely begun to be told. In 1998 about half of the 30 organizations designated as "foreign terrorist organizations" under the United States Antiterrorism and Effective Death Penalty Act of 1996 maintained Web sites; by 2000, virtually all terrorist groups had established their presence on the Internet (Weimann, 2004). A scan of the Internet by staff of the U.S. Institute of Peace in 2003-2004 revealed hundred of Web sites serving terrorists and their supporters. And yet, in spite of this growing terrorist presence, when policy makers, journalists, and academics have discussed the combination of terrorism and the Internet, they have focused on the overrated threat posed by *cyber terrorism* or *cyber warfare* (that is, attacks on computer networks including those on the Net) and grossly ignored the numerous uses that terrorists make of the Internet daily (Weimann, 2004).

Though cyber terrorism or cyber warfare is very important, there is need for policy makers, journalists, academics, and professionals to also focus on the use of the Net by terrorists with a view to exploring ways to prevent/control their activities.

The Internet has expanded the terrorists' theater of operation by allowing them full control over their communications through the use of the developed world's *cyberspace* infrastructure. The terrorists do not mention their own violent activities but highlight what they claim is the righteousness of their cause and the ill treatment of their supporters (Weimann, 2006).

Though terrorists can perpetuate their activities on the Internet from any location, cybercafés provide veritable base for their operations. Besides serving tourists or others without home Internet access, some cybercafés could be attractive to terrorists (Eng, 2002). This chapter sets out to describe the use of the Internet in cybercafés by terrorists and explores measures that have been adopted to stem the use of cybercafés for terrorism.

BACKGROUND

Terrorism has to do with the use of threat of violence to create fear and alarm, usually for political purpose (The World Book Encyclopedia, 2004). It is coercive and violent behaviour taken to accomplish or promote a particular political objective or cause often involving the overthrow of established order (The Cambridge Encyclopedia, 1997). Terrorists can act individually, in small groups, through organized networks, or from within a government (The World Book Encyclopedia, 2004).

Terrorist acts are committed for various reasons. While some individuals and groups use terrorism to support particular political philosophies or religious beliefs, others represent groups seeking a change in government or liberation from a governing power. Most terrorist groups believe the threat or use of violence to create fear is the most effective way to gain publicity and support