Chapter 21

Cyber–Terrorism and Ethical Journalism: A Need for Rationalism

Mahmoud Eid
University of Ottawa, Canada

ABSTRACT

Terrorism has been a constant threat in traditional and contemporary societies. Recently, it has been converged with new media technology and cyberspace, resulting in the modern tactic, cyber-terrorism, which has become most effective in achieving terrorist goals. Among the countless cyber-terrorism cases and scenarios of only this last decade, the paper discusses four cyber-terrorism cases that represent the most recent severe cyber-terrorism attacks on infrastructure and network systems—Internet Black Tigers, MafiaBoy, Solo, and Irhabi 007. Regardless of the nature of actors and their motivations, cyber-terrorists hit very aggressively causing serious damages. Cyber-terrorists are rational actors who use the most advanced technology; hence, the critical need for the use of counter-threat swords by actors on the other side. Given that terrorist goals are mostly dependent on the media’s reactions, journalistic practices are significant and need to be most effective. A major tool that can help journalists in their anti- and counter-terrorist strategies with cyber-terrorists is rationalism, merged with the expected socially responsible conduct. Rational behaviour, founded in game theory, along with major journalistic ethical principles are fundamental components of effective media decision-making during times of terrorism.

A THREAT: TERRORISM

Threats to global citizens emanating from various terrorist groups around the world are increasingly widespread. No country is excluded from terrorists’ potential plans, and both transnational and internal terrorist attacks are possible everywhere as long as the roots of terrorism cannot be effectively expunged. Most noticeable in the late 20th and early 21st centuries are those threats that come from Al-Qaeda, exemplified by bombings and multiple deaths in Dar es Salaam and Nairobi (1998), New York (2001), Bali (2002), Istanbul (2003), Madrid (2004), London (2005), and
Sharm Al-Sheikh (2005). Al-Qaeda first emerged to challenge the incumbency and authority of rulers in various Middle Eastern countries, and then its attention shifted from the domestic to the global: a war against the West with a wider goal of having a global balance of power between the West and the world of Islam. America’s recent “war on terrorism” has made the West in general and North America in particular a major target of terrorist attacks. Even countries with strong foreign relationships and international reputations of peacekeeping, which might possibly reduce potential external or transnational terrorist attacks, still cannot guarantee that they will have any bearing in the face of potential national or internal terrorism.

The convergence of both national and transnational terrorism becomes a very dangerous threat. Transnational terrorism is a “type of non-state actor that is becoming more important” (Nye, 2005, p. 229). If external threats of terrorism are dangerous and require a rational response from policy decision-makers, it is also true that internal extremist groups can become more dangerous if policy decision-makers do not seriously address the issues with which these groups are concerned. Some argue, for instance, that “most terrorist attacks start from a racially, ethnically, or religiously motivated conviction that certain categories of human beings are not worthy of moral standing or consideration” (Ignatieff, 2004, p. 94). If it is conventional for counter-terrorism policymakers to regard terrorists as either mad or wicked, terrorists may, for example, see themselves as “freedom fighters, or fighters in a holy war or whatever. Thus, to execute a captured terrorist might have the very opposite effect from that which the authorities desired in that it creates a martyr and brings new people into the movement” (Nicholson, 1996, p. 169).

From another viewpoint, terrorism is sometimes described as the absolute last weapon of the oppressed.1 The argument that the internal terrorism in United Kingdom has occurred as a result of the country’s policies towards some Muslim countries in the Middle East may be partially correct, but it does not tell the whole story. September 11, 2001 (9/11) showed that the global villagers entertain profound misperceptions about, and abhorrence for, each other: “Living in a largely mediated world, they are hostage to the images of ‘the other’ received through the mass media. A growing global apartheid is tearing them apart into opposing camps” (Tehranian, 2002, p. 59). Hence, such apartheid seems to be one of the key factors behind global terrorism.

**TERRORISM AND NEW TECHNOLOGIES: THE BIRTH OF CYBER-TERRORISM**

The concept of cyber-terrorism was born in the mid-1980s, when Barry Collin, a senior research fellow at the Institute for Security and Intelligence in Palo Alto, California, USA, coined this hyped-up, techno-phrase by referring to the convergence of cyberspace and terrorism (Berner, 2003; Denning, 2000; Matusitz & Minei, 2009; Matusitz, 2009, 2005; Mitliaga, 2001). Although there are many different concepts of terrorism and no one agreed-upon definition of the term to date, most would acknowledge the existence of cyber-terrorism, i.e., the use of information and communications technologies to facilitate any or all forms of terrorism. Cyber-terrorism is the intentional use of threatening and disruptive actions, or attacks waged through computers, the Internet, and technology-based networks or systems against information and data, infrastructures supported by computer systems, programs, and networks in order to cause harm or to further ideological, political, or similar objectives, influence an audience, or cause a government to change its policies (Corzine & Cañas, 2008; Denning, 2000; Matusitz, 2005, 2008, 2009).

Terrorists have always been pioneers in embracing the newest communication technologies