Chapter 1
The Development of Internet-Enabled Terror

INTRODUCTION

Internet is a battlefield for jihad, a place for missionary work, a field of confronting the enemies of God. It is upon any individual to consider himself as a media-mujahid, dedicating himself, his wealth and his time for God (Prucha, 2011, Pg. 46).

Digital technologies are assisting in the coordination, communication and sustainability of contemporary movements, for better or for worse. Much of the existing literature focuses on the optimistic and democratic potential of digital technologies as well as the internet (Castells, 1996, 1999, 2012; Gerbaudo, 2012; Hussain & Howard, 2011). Yet the imminent threat of cyber war, infiltration of sensitive databases, disruption of the global financial markets, and the preparedness of governments around the world to respond...
The Development of Internet-Enabled Terror has become a major question in the 21st century. Richard Clarke, former National Coordinator for Security, Infrastructure, and Counterterrorism noted, 

*The U.S. military is no more capable of operating without the Internet than Amazon.com would be. Logistics, command and control, fleet positioning, everything down to targeting, all rely on software and other Internet-related technologies. And all of it is just as insecure as your home computer, because it is all based on the same flawed underlying technologies and uses the same insecure software and hardware (Clarke & Knake, 2010, Pg. 31).*

Most pressing is the utilization of digital technologies, social media, and the internet to aid in the facilitation of regimes, organizations, and groups that threaten the lives of humans (in the short-term) and global democratic governance (in the long-term). While the idea of terrorist groups or extremists using the internet for their own (oft not mainstream) agendas is not new, as organizations such as Al Qaeda, Hamas, Hezbollah, and more recently, the Islamic State, it is highly salient as more ruthless and pervasive groups are using digital tools more effectively to mobilize participants as well as support for their cause. This book addresses the evolving complexity of social media and internet use in contemporary terrorist organizations and the responses of the State (formal) and non-state actors (informal), such as Anonymous.

The co-dependent relationship between terrorist organizations and the media has been evident for a long time, as terrorists have relied on the traditional media (print, radio, television) to distribute their messages of ideology and destruction. Terrorists in the broadcast age had to plan very elaborate and strategic attacks on large-scale targets in Western countries or on Western-affiliated targets (Lockerbie bombing, various embassy bombings) in order to receive enough media attention to garner global recognition (Nacos et al., 2007). Terrorism by definition seeks to foster fear through attacks or threat of attack in societies that force governments and officials to pass legislation or take emergency measures that alter the function of a free (often democratic) society. The earliest example of methodical terrorist manipulation of the traditional media occurred in 1972, during the Munich Olympic games, when members of the Palestinian Black September group attacked Israeli athletes. This by no coincidence was the first Olympic games to be televised live and the first to be the location of a terror attack (Cosgrove & Bhownikck, 2013). Throughout the following decades, and the development of satellite and cable television, terrorist attacks and violence became a staple of news
Related Content

Cyber Terrorism Attacks
Kevin Curran, Kevin Concannon and Sean McKeever (2007). Cyber Warfare and Cyber Terrorism (pp. 1-6).
www.igi-global.com/chapter/cyber-terrorism-attacks/7433?camid=4v1a

Applicability of Jus in Bello in Cyber Space: Dilemmas and Challenges
www.igi-global.com/article/applicability-of-jus-in-bello-in-cyber-space/124131?camid=4v1a

Detecting Individual-Level Deception in the Digital Age: The DETECT Model
©
www.igi-global.com/chapter/detecting-individual-level-deception-in-the-digital-age/141050?camid=4v1a