Chapter 1
The Mirror Has Two Faces:
Terrorist Use of the Internet and the Challenges of Governing Cyberspace

Shefali Virkar
University of Oxford, UK

ABSTRACT

The Information Revolution has greatly impacted how nation-states and societies relate to one another; particularly wherein new, or hitherto less powerful, actors have emerged to bypass and influence established channels of power, altering the manner in which nation-states define their interests, power bases, security, and increasingly, their innate ability to govern and control flows of information. This book chapter investigates the 'winner-takes-all' hypothesis relative to how the Internet, its associated platforms, and technologies have been harnessed to enhance the activities of both transnational terrorist networks and the organisations, clusters, and individuals dedicated to researching and combating them. The issues covered by this research raise important questions about the nature and the use of technology by state and non-state actors in an asymmetric 'information war'; of how ideas of terrorism, surveillance, and censorship are conceptualised, and manner in which the role of the nation-state in countering and pre-empting threats to national security has been redefined.

DOI: 10.4018/978-1-4666-9661-7.ch001

INTRODUCTION

The Information Revolution and the advent of the new Information and Communication Technologies has significantly impacted how nation-states and societies relate to one another, and has underlined several challenges to international governance and security. These include the creation of global electronic platforms where new, or hitherto less powerful, actors have emerged to influence policy agendas; bypassing established channels of participation, changing the conception of how nation-states define their interests, their power bases, and their security, and increasingly challenging states' ability to govern and control the dissemination of information.

Ten years since its emergence as a mainstream global medium, the Internet plays an active role in both contentious political debates and the dissemination of alternative visions for a new order in world politics. Today, therefore, the issue is no longer *whether* the Internet and the World Wide Web have altered the world we live in, but instead *how* the study of them thereof might enhance our understanding of the political changes they bring. Unlike print or other broadcast media, which have largely remained the clearly designated territory of communications scholars, the study of the Internet and its associated new Information and Communications Technologies has attracted researchers from various scholarly backgrounds and disciplines to explore its implications for political, social, and economic change from the unique perspective of their own particular field of expertise.

With social scientists starting recently to examine the political impact of the new digital technologies on everyday living, concepts such as power and governance and their relationship to networks of communication, conflict, and excellence have become increasingly important and have entered common parlance when examined within the context of digital communications technology. When considered in this regard, the world has also seen the rise of a new type of conflict, *the Information War*, which involves the disruption of information networks through the proliferation of aggressive software and the use the Internet and its associated applications by loosely organised groups of dissidents to communicate and to co-ordinate attacks. Recent investigations spurred on by the global *War on Terror* have further thrown into sharp focus international terrorist networks' usage of the Internet, not only as a communications platform and as a vehicle for the dissemination of propaganda, but also as an active element in their recruitment strategies and as a tool for delivering remote instruction and training.

BACKGROUND

This book chapter investigates the 'winner-takes-all' hypothesis in relation to how the Internet and its associated platforms and technologies have been harnessed to enhance the activities of both transnational terrorist networks and the organisations, clusters, and individuals dedicated to researching and combating them. The attacks of September 11, 2001 on the United States of America, followed closely by numerous instances of terrorist-related activity around the world, demonstrated that modern-day terrorist networks are widely interconnected and connected to each other, and are able to harness effectively the flexibility afforded by the Internet and its associated technologies in order to achieve key aims, goals, and objectives.

Transnational terrorism has always been a security issue of great sovereign concern, and dissident groups have consistently taken advantage of the potentialities of the new digital communications media in direct opposition to the fundamental constitution of the nation-state. With scholars, practitioners, and