The Potential Threat of Cyber-Terrorism on National Security of Saudi Arabia

Abdulrahman Alqahtani
Department of Politics and International Studies, The University of Hull, UK
qahtaniasa@hotmail.com

Abstract: Throughout history, there have been many events and dangers that threaten state security, causing heavy loss of life, disease, injuries, destruction of property, displacement of large numbers of people and heavy economic losses. Political unrest on international and local levels and recent technological developments increase the seriousness of threats against national security. The concept of security has evolved gradually, especially since the disintegration of the Soviet Union, and end of the Cold War. The lingering impact of the policy of the bipolar world has blurred the image of relations between states. However, it provides an opportunity to understand and identify new threats and emerging conflicts, in addition to many unsolved problems. Simultaneously, globalisation has changed international rules and norms, in order to facilitate the rapid flow of capital and technology, with a weakening of national barriers. Non-governmental actors now play key roles in international politics, some as a threat, and others bridging the gap between communities and nations. In these circumstances, the role of the state began to suffer and the accepted traditional concept of power was challenged. Today, a major issue of such concern worldwide, arousing heated debate at both national and international levels, is terrorism. The threat of terrorism has never been as prominent as it seems to be at the present time. Terrorism is an old phenomenon that has existed since the emergence of human societies, but the threat of terrorism has increased steadily over the past 30 years. With technological and technical progress, the actions of terrorists have become more dangerous and destructive, while the perpetrators of such acts are becoming more elusive. There are few parts of the world that have escaped terrorism since late 1960s (Mythen and Walklate 2006). The phenomenon of terrorism is changing, while the motives of terrorism remain the same. The world today faces new and unfamiliar kinds of weapons. The international system, intelligence systems, security procedures and tactics which are expected to protect people, nations and governments, are not able to meet this new and devastating enemy. The methods and strategies developed to combat terrorism over the years are providing ineffective, as the enemy no longer attacks only with hijacked plans, truck bombs or suicide bombers. Terrorists may engage in cyber-terrorism, the use of cyberspace to launch attacks. The integration of the virtual and physical worlds, is a weakness confronting security agents (Collin 1996). This paper outlines a PhD proposal, which seeks to design an effective framework for the potential threat of cyber-terrorism on national security, compared with conventional terrorism by addressing three main themes: awareness - vulnerabilities – response, important in assessment of any security threat. According to Denning (2000) to understand the potential threat of cyber-terrorism, we should consider two factors: first, whether there are targets that are vulnerable to attack, and, secondly, whether actors have the ability and motivation to attack them. In this proposal a preliminary review of relevant literature will be introduced, followed by the research questions to be addressed and the proposed methods to address them. Then the expected time frame will be considered.

Keywords: terrorism, cyber-terrorism, national security, Saudi Arabia

1. Introduction: Research title

The proposed thesis will focus on cyber-terrorism and assess its potential threat to national security, as compared to conventional terrorism in Saudi Arabia. So, therefore a suggested title is, "The Potential Threat of Cyber-terrorism on National Security of Saudi Arabia".

2. Literature review

> "If you ask 10 people what 'Cyber-terrorism' is, you will get at least nine different answers! When those 10 people are computer security experts, whose task it is to create various forms of protection against 'Cyber-terrorism'" (Gordon and Ford 2003).

Gordon and Ford (2003) highlight the inconsistency of understandings of cyber-terrorism even among people representing government agencies charged with protecting critical infrastructure components and assets. However, they say this is not surprising because of the lack of documented scientific support to integrate the various aspects of computer-related crimes.

The term "Cyber-terrorism" was first coined by Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California, in the 1980s (Collin 1997). No single definition of the term has yet gained global acceptance. Tagging a computer attack as "Cyber-terrorism" is problematic because of the difficulty of determining the intention, identity, or political motivations of an attacker with certainty.