Chapter 9
Attribution:
Challenges in Cyber Terrorism and Cyber Security Preparedness

Aishwarya Majumdar
https://orcid.org/0009-0001-3495-4414
Delhi High Court, India

Pranjal Chaturvedi
https://orcid.org/0009-0007-0993-9005
Allahabad High Court, India

Bhupinder Singh
https://orcid.org/0009-0006-4779-2553
Sharda University, India

ABSTRACT

Amidst the evolving technological landscape and readily available tools and high speed internet, there exists a remarkable propensity for technology to be employed with wisdom, misused with malevolence, or catastrophically unleashed. The stark illustration of such catastrophic misuse is the realm of 'Cyber Terrorism. The very mode through which terror is sown is undergoing a profound transformation in the present era, one that is destined to further evolve in the future. Acknowledging technology is neutral, and the use of technology depends on the person using it, serious challenges are standing tall, which need significant notice and venturing. This chapter explores the evolving threat of cyber terrorism, and examines the cyber security preparedness to combat cyber terrorism. Through the exploration in real world incidents and attribution techniques it explores the intricate landscape of attributing cyber terrorism; it accentuates the crucial role of attribution in context of national and international cyber security.

DOI: 10.4018/979-8-3693-3522-2.ch009

INTRODUCTION

The terror landscape is changing from being foot on ground the terror actions are going online. It has turned more severe due to it being face and figure less. The future of inflicting terror is inextricably tied to the cyber domain, and cyber terrorist activities will happen in cyber space, a boundless space where territorial constraints or national borders do not apply (Cheng et al., 2021). Even the Intelligence agencies or the agencies in business of providing cyber security can't claim to be completely secured and past real world experiences of cyber terrorism (Muhlhoff, 2021) (Saltz et al., 2019). Even they are susceptible to crafty cyber-attacks and one of such system of communication is internet (Hoijtink & Planque-van Hardeveld, 2022) (Dean, 2024). The unprecedented proliferation of the internet, exemplified by rapidly enhancing and advancing Information and Communication Technology, has connected the world through an invisible chain (Utami et al., 2022). The dependence on Information and Communication Technology has increased many folds. Today we place reliance on Technology for our daily chorus (Zhang et al., 2022). This technology plays role in regulating Stock Market, Supreme Court Rosters, Water or Food Distribution System, Electronic Governance, Cashless Economy, Integrated Banking System, etc. (Baker & Robinson, 2020). The technology fostering interconnected system facilitates economic efficiency in governance and affects all social, political and economic dimensions of life. This chapter also examines the cyber security alacrity and preparedness by state and non-state actors (Aziz & Andriansyah, 2023).

Figure 1. shares the Landscapes of Introduction Split Section (Source- Original)