Title: Cybersecurity and Cyber Terrorism – in Energy Sector – A Review

Authors: Sampath Kumar Venkatachary, Jagdish Prasad, Ravi Samikannu

Year:2018

Journal:Journal of Cyber Security Technology

1. Introduction

The paper highlights the increasing digitization of the energy sector, which enhances efficiency but also expands vulnerabilities to cyber threats. With growing reliance on ICT, energy systems face rising risks from sophisticated cyberattacks. Since energy infrastructure is critical to national operations, cyber disruptions can cause severe economic and social consequences.

2. Problem Statement

The energy sector is highly exposed to cyber threats due to interconnected digital systems. Existing security frameworks are insufficient for modern cyberattacks. There is no unified understanding of threats specific to energy infrastructure, making the sector inadequately prepared for cyber terrorism and advanced attacks.

3. Objectives

- To review cybersecurity threats unique to the energy sector.

- To analyze impacts of cyberattacks on operations, safety, and national security.

- To summarize existing cybersecurity frameworks applicable to energy systems.

- To identify challenges faced by the sector in addressing cyber risks.

- To provide a comprehensive, sector-specific overview linking cybersecurity and cyber terrorism.

4. Research Gap

- Limited sector-specific studies on cybersecurity in the energy industry.

- Lack of integrated research combining cybersecurity and cyber terrorism.

- Insufficient analysis connecting technical vulnerabilities with economic and operational impacts.

- No consolidated evaluation of current defense mechanisms for energy systems.

- Underexplored vulnerabilities in SCADA and smart grid systems.