FISA EURADWASTE 2025

SNETP Forum

Analysis of Terrorist Threats to Nuclear Infrastructure: Case Studies and Security Implications

Wojskowa Akademia Techniczna | Regionalna Inicjatywa Doskonałości | Ministerstwo Nauki i Szkolnictwa Wyższego

Klaudia Rzadkowska[1], Barbara Wiaderek[1] and Patrycja Bryczek-Wróbel[1]

[1]Military University of Technology, gen. Sylwestra Kaliskiego 2, 00 – 908 Warsaw, Poland

1. Introduction

Nuclear infrastructure plays a crucial role in ensuring a country's energy and strategic security. In recent decades, the number of threats to nuclear facilities has significantly increased. These threats encompass both traditional forms of attacks, such as sabotage, terrorist acts, and attempts to seize radioactive materials, as well as modern cyber methods that can lead to the takeover of management and security systems. Terrorist organizations and criminal groups are increasingly interested in acquiring nuclear materials or disrupting critical infrastructure to achieve political or military objectives.

2. Research Methodology

To conduct a comprehensive analysis of terrorist threats, including attacks and incidents targeting nuclear infrastructure, and to assess the effectiveness of current protective measures, a multi-faceted approach was adopted in this study, consisting of the following stages:

a) Analysis of real-world attacks and incidents documented in the database of terrorist attacks involving hazardous materials, compiled as part of the RID Project;
b) Review of data from the International Atomic Energy Agency (IAEA);
c) Assessment of the effectiveness of current security measures;
d) Comparative study and inference.

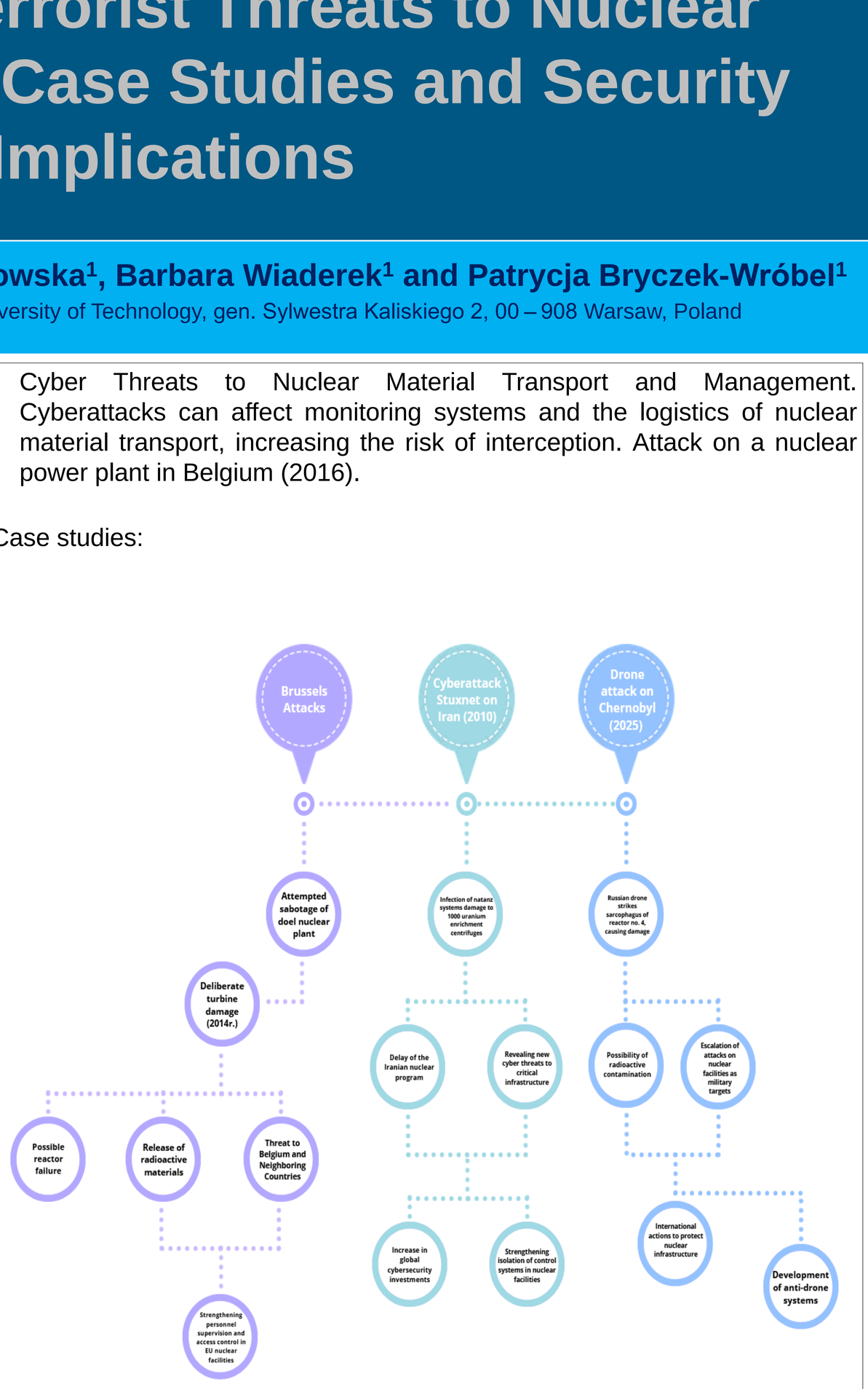
3. Trends and Threats Emerging from Incident Analysis

The analysis of nuclear attack and incident data allows for the identification of several significant trends and threats:

• Increase in incidents related to the illegal trade of nuclear materials – Since 2010, the number of cases involving attempts to sell illegal nuclear materials has increased by 20%.
• New smuggling techniques – In recent years, more advanced methods of concealing radioactive materials have emerged, including their placement in transport containers and industrial cargo.
• Increased risk of using radioactive materials in terrorist attacks – Terrorist groups have shown interest in radiological devices that could be used to create "dirty bombs."

• Cyber Threats to Nuclear Material Transport and Management. Cyberattacks can affect monitoring systems and the logistics of nuclear material transport, increasing the risk of interception. Attack on a nuclear power plant in Belgium (2016).

Case studies:



4. Conclusions

Based on the conducted analyses, several key priorities for the protection of nuclear infrastructure can be formulated:

1. Modernization of physical security measures at nuclear power plants – Increasing the number of control points, implementing AI-based monitoring, and deploying new threat detection systems.
2. Strengthening cybersecurity – Isolating control systems, developing artificial intelligence for detecting cyberattacks, and implementing advanced data encryption systems.
3. Enhancing control over nuclear material transport – Introducing advanced tracking technologies and comprehensive escort procedures for nuclear shipments.
4. Expanding international cooperation in threat monitoring – Strengthening collaboration between countries within the IAEA and other nuclear security organizations.
5. Training and development of personnel responsible for nuclear infrastructure security – Improving staff preparedness for identifying and countering terrorist threats.

Literature:

• Iinternational Atomic Energy Agency (IAEA), Incident and Trafficking Database (ITDB), 1993–2023. Reports on cases of illicit trafficking of nuclear and radioactive materials.
• International Atomic Energy Agency (IAEA), Nuclear Security Series. Guidelines on nuclear infrastructure protection against terrorist and cyber threats.
• World Institute for Nuclear Security (WINS), Best Practice Guides on Physical Protection and Cybersecurity for Nuclear Facilities, 2021.
• Terrorist Attacks Involving Hazardous Materials – RID Project Database, No. RID/SP/0042/2024/01, (2025). Warsaw: Military University of Technology (WAT).

This work was supported by the Polish Ministry of Science and Higher Education under project No. RID/SP/0042/2024/01, Increasing Competences in identifying threats related to hazardous materials, from program Regional Excellence Initiative, 2024-2027.