WORLD CONFERENCE ON SECURITY STUDIES

29 - 31 May 2026 Warsaw , Poland

Hybrid Threats and Cascading Failures in Energy-Centric Critical Infrastructure

Teodora Gjorgjievska , Nikola Manev

Institute for Security, Defense and Peace, Faculty of Philosophy, University of "Ss. Cyril and Methodius" in Skopje, Macedonia
Military academy "General Mihailo Apostolski" – Skopje, Goce Delcev University, Macedonia

Abstract

Modern societies depend on highly interconnected critical infrastructure, with the energy sector serving as a foundational enabler for all other sectors. This interdependency increases vulnerability to hybrid threats, which exploit systemic weaknesses through cyberattacks, physical sabotage, supply-chain disruptions, and disinformation campaigns. Disruptions in one sector can propagate across dependent systems, producing cascading failures that compromise public services, urban mobility, healthcare, water supply, and communications. This paper develops an analytical framework for understanding how hybrid threats targeting energy infrastructure can induce multi-sector cascading failures. The framework combines interdependency mapping, dependency-graph modeling, and scenario-based reasoning to identify the most critical pathways for failure propagation. The research findings show that the complexity and interconnectedness of modern critical infrastructure magnify the systemic impact of hybrid threats, demonstrating that resilience cannot be achieved through single sector approaches alone. The paper concludes with recommendations for enhancing critical infrastructure resilience through cross-sector coordination, redundancy planning, interdependency-aware risk assessments, and the integration of cascading-failure modeling into national hybrid-threat mitigation strategies.

Keywords: Dependency analysis; interdependency; modeling; resilience; risk assessment