# *CYBERSECURITY PERSPECTIVES IN THE ENERGY AND POWER SECTOR: AN OVERVIEW*

[Ahmed Albalawi, KAPSARC, +966509716252, Ahmed.balawi@kapsarc.org]
[Khalid Alhadhrami, KAPSARC, khalid.hadhrami@kapsarc.org]
[Faris Aljamed, KAPSARC, faris.jamed@kapsarc.org]

## Overview

Cybersecurity in the power system is growing in importance with the transition to smart grids and electrification of other sectors. The power sector underpins all other sectors and consequences of cyber-attacks on energy infrastructure extend to other key infrastructures. Therefore, it is important to address all potential threats and risks that could face the power system. Cybersecurity is a critical issue across various fields, including the power sector, electric vehicle infrastructure, and critical infrastructure. Several studies have proposed recommendations, technologies and approaches to address the growing cybersecurity challenges related to the energy and infrastructure sectors. In Europe, there has been a shift from sectoral regulation to a cross-sectoral approach while in China, there has been an effort to establish a cybersecurity legal system.

## Methods

A comprehensive literature review was conducted to look at looks at the cybersecurity across three specific fields, namely the cybersecurity in the power sector, cybersecurity in the electric vehicle infrastructure, and cybersecurity in critical infrastructure. Papers were sourced from peer reviewed journals and well known research entities reports. The focus of the review is to identify potential threats affecting the power sector and critical infrastructure and how these risks can lead to a more serious damage whether digital or physical. It is noted that physical consequences of a cyber attack are becoming increasingly a concern with the increased connectivity in the communication infrastructure including industrial control systems. Over fifty papers were reviewed and synthesised to reach an overview of the emerging cybersecurity threats and policy responses in the electric power sector.

## Results

Research papers focusing on different countries policies were reviewed and analysed to uncover energy and cybersecurity policy differences across countries. The US strategy perspective looking with detailed regulations implemented by federal regulations, while the EU strategy is more reactive and covers a wider range of sectors. The papers propose numerous solutions such as setting an investment framework and identifying responsibilities, while in some countries there are currently no mandates or policies in place. In response to the 5G technology crisis, the EU's initial policies have changed to focus on cybersecurity. In Switzerland, a national self-assessment of the cybersecurity capabilities was performed and rudimentary protection of information and operation technology was found.

Several survey studies have been conducted on cybersecurity in the power sector, which have assessed a wide range of topics and technologies including standards, false data injection attacks, cyberattacks on operational technology, challenges in communication infrastructure, distributed and renewable electricity systems, critical energy infrastructure, protection systems for power grids, demand response aggregators, Cyber-Physical Power System testbeds, nano grids, local electricity markets, Edge computing-based security systems and distributed ledger technology. These studies aim to identify risks, develop protection mechanisms, provide security, and measure the severity of cyber-attacks.

Studies have been conducted on cyber threats to critical infrastructure. The potential solutions to the cyber threats include addressing the skilled workforce shortage, promoting cyber hygiene, developing informational resources, and standardizing engineering methods. There are also legal systems and training programs available to improve cybersecurity. Additionally, there are approaches proposed in literature to enhance cyber security in logistics and supply chain management, as well as detecting false data injection attacks. It is necessary for governments to collect, validate, and disseminate data and for strong connections between legislation and practice to be established.

For autonomous vehicles, attack and defense technologies related to autonomous vehicles. was mainly conducted on electronic control units (ECU) and controller area networks (CAN) prior to 2017. Recently, however, studies have

been extensively conducted on external communication attacks, such as on V2X. Research on defense was conducted on areas such as security of CAN, security of authentication protocols, and intrusion detection. Regarding attack detection methods, recent studies consider artificial intelligence techniques to improve specification of ECUs. Finally, vehicle security models were also studied ranging from traditional security models to combining security models with artificial intelligence and deep learning technologies.

## References

All information, data and references will be sufficiently presented and referenced.