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]

1. 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.

2. 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. The following three tables highlight the sectors reviewed and the scope of the papers.

Table 1: Papers with a focus on cybersecurity in the power sector

#	Reference	Paper	Scope
1	IFRI Center of energy	Cybersecurity in the energy sector: a comparative analysis between Europe and the US	Presents policy recommendations based on reviewing literature and conducting fifteen interviews with experts in energy and cybersecurity in Europe and USA.
2	Heymann et al.	Cybersecurity and resilience in the swiss electricity sector: Status and policy options	This report analyzes the current status of cybersecurity in the Swiss electricity sector and compares it with that of neighboring European countries.
3	Kumar et al.	Cyber security threats in the power sector: neeed for a domain specific regulatory framework in India	The paper identifies key cybersecurity threats across India's power sector (generation, transmission, and distribution). The paper looks at the experience of regulators in other critical sectors in Inida (like banking and Telecom) alongside power sector regulations internationally.

4	Rajavuori and Huhta	Digitalization of security in the energy sector: evolution of EU law and policy	This paper analyzed the dynamics and implications of digitization of security in the energy sector by reviewing EU legal and policy instruments of the last 15 years.
5	Atlantic Council	Securing the energy transition against cyber threats	The paper covers the challenges of cybersecurity associated with energy transition, then talks about the federal cyber policy and gives recommendations regarding establishing bureaucratic roles and responsibilities and setting an effective investment framework for energy cybersecurity.
6	Zhang	Cybersecurity policy for the electricity sector: the first step to protecting our critical infrastructure from cyber threats	Identifies problems of predicting and identifying cyber threats. Proposes five components to comprehensive cybersecurity policies.
7	Leszczyna	A review of standards with cybersecurity requirements for smart grid	Brings in all the relevant standards of cybeersecurity for smart grids into one place (based on a systematic study), and overviews the cybersecurity requirements which they specify.
8	Sanders et al.	Critical energy infrastructure and the evolution of cybersecurity	Analyzes the cyber threat to critical energy infrastructre, how the energy sector can respond to said threats, and sociotechnical approaches to the threats.
9	Krause et al.	Cybersecurity in Power Grids: Challenges and Opportunities	Addresses security concerns that result from the increased interconnectivity of power grids. The paper gives an overview of the communications infrastructure and the challenges associated with it. It then identifies a set of attack scenarios to said challenges.
10	Jarmakiewicz et al.	Cybersecurity protection for power grid control infrastructures	A robust cybersecurity protection approach for power grid control systems
11	Ratnam et al.	Electricity system resilience in a world of increased climate change and cybersecurity risk	Explores electric system resiliency as climate change and cybersecurity threats increase. Discusses whether distributed and renewable systems be less resilient than centralized ones due to greater complexity; or would the system be more resilient due to multiple pathways.
12	Tolba and Al-Makhadmeh	A cybersecurity user authentication approach for securing smart grid communications	Technical approach regarding cybersecurity through user authentication was introduced for securing smart grid communication

13	Dedrick et al.	Assessing cyber attacks on local electricity markets using simulation analysis: Impacts and possible mitigations	Development of local electricity markets (LEMs) creates new vulnerabilities to cyber attacks. The study uses simulation techniques to measure the severity of these risks and offer recommendations to deal with them.
14	Hueros-Barrios et al.	Addressing the cybersecurity vulnerabilities of advanced nanogrids: A practical framework	Development of a framework to identify risks and implement protection mechanisms in future nanogrid developments using experimental testbed of an advanced nanogrid based on a PV system and controllable loads.
15	Yohanandhan et al.	A holistic review on Cyber-Physical Power System (CPPS) testbeds for secure and sustainable electric power grid – Part – I: Background on CPPS and necessity of CPPS testbeds	Used testbeds to review various CPPS research areas such as modelling of CPPS, software tools for modelling and simulation, cybersecurity and privacy in CPPS, cascading failure analysis, resilience and reliability analysis, physical power infrastructure of CPPS, communication networking and CPPS Protocols, and cloud computing & data analytics.
16	Yohanandhan et al.	A holistic review on Cyber-Physical Power System (CPPS) testbeds for secure and sustainable electric power grid – Part – II: Classification, overview and assessment of CPPS testbeds	Reviews the CPPS testbeds in the view of the testbed type, targeted research area, CPPS domain, and communication infrastructure with the fusion of physical and cyber systems.
17	Yohanandhan et al.	A specialized review on outlook of future Cyber-Physical Power System (CPPS) testbeds for securing electric power grid	This study aims to provide an outlook on future CPPS testbeds for long-term cybersecurity research in all aspects
18	Venkatachary et al.	Cybersecurity challenges in energy sector (virtual power plants) - can edge computing principles be applied to enhance security?	Provides an assessment and a way of adopting Edge computing-based security systems in virtual power plants.
19	Gourisetti et al.	Standardization of the Distributed Ledger Technology cybersecurity stack for power and energy applications	The paper talks about the potential of distributed ledger technology (DLTs) in helping with the worldwide trend of integrating distributed energy sources. The paper presents a DLT cybersecurity stack and demonstrates its potential through several power use cases.
20	Kolosok and Korkina	Applying the principles of cyber-physical management to enhance cybersecurity of the Demand Response Aggregator structure	The article proposes a technical approach to increase the cybersecurity of the DR-Aggregator structure using cyber-physical management, in which an intelligent feedback loop is created at the lowest level of the structure.

21	Rodriguez et al.	A systematic approach to analysis for assessing the security level of cyber-physical systems in the electricity sector	Analyzes the main incidents that have affected the energy sector. A general study is conducted using standards that affect it in order to develop a simple and practical methodology to assess the level of security of the cyber-physical systems.
22	Reda et al.	Comprehensive survey and taxonomies of false data injection attacks in smart grids: attack models, targets, and impacts	This paper has put together a number of publications related to false data injection attacks (FDI) by three classes: attack model, attack target, and impact of attack.

Table 2: Papers with a focus on cybersecurity in critical infrastructure

#	Reference	Paper	Scope
1	Chowdhury and Gkioulos	Cyber security training for critical infrastructure protection: A literature review	This paper performs a systemic literature review of training solutions, methodologies, target groups, and focus areas in cybersecurity training. The paper establishes the current cybersecurity training offerings for critical infrastructure and KPIs to evaluate their effectiveness.
2	Alladi et al.	Industrial Control Systems: Cyberattack trends and countermeasures	The paper covers major cyber attacks on industrial control systems (ICSs) with major economic damage, the potential for physical equipment damage, and human casualties over the past 20 years. The paper covers each attack's methodology and possible solutions to prevent them.
3	Jimada-Ojuolape and The	Surveys on the reliability impacts of power system cyber–physical layers	This paper reviews studies that evaluate the impact of infromation and communication tchnology (ICT) on the system reliability while at the same time considering the effects of malfunctions of the cyber system.
4	Guo	China’s cybersecurity legislation, it’s relevance to critical infrastructures and the challenges it faces	Examines the legislation history of Cybersecurity laws, analyzes the problems of current cybersecurity legislation, and presents ideas on establishing a cybersecurity legal system with reference to the relevant legislation of developed countries, such as the United States and Japan.
5	Quigley et al.	‘Cyber Gurus’: A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection	A rhetorical analysis of ten recent cybersecurity publications ranging from popular media to academic and technical articles.
6	Asghar et al.	Cybersecurity in industrial control systems: Issues, technologies, and challenges	Reviews possible cyber attacks on ICSs, identify typical threats and vulnerabilities, and discuss unresolved security issues with existing ICS cybersecurity solutions.
7	Gao et al.	Fast economic dispatch with false data injection attack in electricity-gas cyber–physical system: A data-driven approach	Proposes a data-driven approach to improve cybersecurity and computational efficiency in fast economic dispatch. The data driven approach also serves exact location detection of false data injection attacks (FDIA).

8	Cassotta and Sidortsov	Sustainable cybersecurity? Rethinking approaches to protecting energy infrastructure in the European High North	Looks at the impact of exceptionally critical infrastructure conditions (ECICs), like remoteness, seasonal darkness, and severe climate, on energy critical infrastructure (CI). The paper argues for a new approach to address cyber threats to energy infrastructure under ECIC.
9	Gur	Cybersecurity, European digital sovereignty and the 5G rollout crisis	This article analyses the European Union's (EU) regulatory response to the 5G roll-out crisis in the context of its digital sovereignty policies with a specific focus on whether it complies with its international law commitments.
10	Dimitrov et al.	Complexity Assessment of Research Space for Smart City Cybersecurity	Aims to draw a space for cybersecurity challenges for smart cities from a systematic perspective. Proposed a method to reveal the scope of cybersecurity challenges concerning the current state and sustainable development of a smart city with the incorporation of state-of-the-art technologies
11	Cheung et al.	Cybersecurity in logistics and supply chain management: An overview and future research directions	Reviews studies on measures that enhance cybersecurity in logistics and supply chain management

Table 3: Papers with a focus on cybersecurity in transportation

#	Reference	Paper	Scope
1	Moghadasi et al.	Trust and security of electric vehicle-to-grid systems and hardware supply chains	Proposes a framework to address possible future scenarios or conditions that might threaten the security of EV charger embedded systems and their networks.
2	Kim et al.	Cybersecurity for autonomous vehicles: Review of attacks and defense	Reviews 151 studies about attack and defense technologies related to autonomous vehicles.
3	Taeihagh and Lim	Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks	Examines autonomous vehicles (AVs) and different categories associated with their technological risks. Furthermore, strategies that can address these risks alongside government responses are explored.
4	Khan et al.	A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles	Aims to develop a conceptual System Dynamics (SD) model to analyse cybersecurity in the complex, uncertain deployment of emerging connected and autonomous vehicles (CAV)
5	Benyahya et al.	Automated city shuttles: Mapping the key challenges in cybersecurity, privacy and standards to future developments	Proposes a comprehensive state of the art with farsighted analyses addressing security threats and data privacy concerns from both technical and legal perspectives to thwart potential attacks for the automated city shuttles (ACSs)

6	Zhang et al.	Challenges of future high power wireless power transfer for light-duty electric vehicles -technology and risk management	Discusses the future challenges and risks for high power wireless charging for light-duty electric vehicles. Aiming at 200 kW or higher wireless power transfer, the paper discusses technology and risk management challenges in the area of electromagnetic safety, resonant frequency determination, and cybersecurity risks in detail.
7	Argyropoulosa et al.	Addressing Cybersecurity in the Next Generation Mobility Ecosystem with CARAMEL	CARAMEL project will bring 15 partners from Europe to develop cybersecurity solutions for: autonomous cars, connected vehicles, and electromobility. The paper presents CARMEL's anti-hacking detection/prevention solution, which it implements using AI and ML techniques.
8	Sayed et al.	Electric vehicle attack impact on power grid operation	The study investigates EV charging ecosystem and identify vulnerabilities in EV charging systems and how they can be exploited to launch attacks on the power grid.
9	Channon and Marson	THE liability for cybersecurity breaches of connected and autonomous vehicles	Reevaluates how to assign responsiblility for damages and losses caused by mass hackings of connected and auonomous vehicles (CAV). The study examines challenges with hackings CAVs and it explores current reguatory regime and issues with apportioning responsibility.
10	Pizzi	Cybersecurity and its integration with safety for transport systems: not a formal fulfillment but an actual commitment	The paper propose an attack-fault tree for a case study using a real incident (of a regional Italian railway line incident) as an example of integrated risk analysis.

3. Literature review

Several previous studies have proposed recommendations for updating policies to keep pace with technological development and improve cybersecurity. The IFRI Center of Energy (2018) conducted a comprehensive analysis of energy cybersecurity policies in the United States and Europe. The study, which was based on a review of the literature and interviews with experts, found that the United States has a more prescriptive approach, with detailed regulations implemented by federal agencies. The European Union, on the other hand, has a more flexible approach that allows countries to implement their own standards. The study found that both models have strengths and weaknesses, and that each could learn from the other. Another study, by the Atlantic Council (2022), examined the cybersecurity challenges posed by new technologies needed for the energy transition in the United States. The report made recommendations for improving federal cybersecurity policy, including establishing clear roles and responsibilities for government agencies and creating an effective investment framework.

Another paper from the United States (Zhang, 2013) discussed the first step in protecting critical infrastructure from cyberattacks. The paper outlined the specific challenges of predicting and identifying cyber threats, and proposed five components of a comprehensive cybersecurity policy: recognition of responsibility by government and industry, information sharing of cyber threats and vulnerabilities, procurement rules for vendors, federal agency emergency powers, and international cooperation. In Europe, digitalization has only recently penetrated the energy sector's security paradigm. Countries are moving from sectoral regulation in the energy sector to a cross-sectoral approach to digitalized security. However, there is a significant disconnect in conceptualizing the risks and opportunities associated with digitization. Gur (2022) investigated the EU's response to the 5G roll-out crisis. The author analyzed the EU's digital sovereignty policies and how they comply with international law commitments. In response to the crisis, the study found that the EU's initial 5G policies have shifted from being market and competition-driven to being more focused on cybersecurity.

In Switzerland, a study by Heymann et al. (2022) analyzed the status of cybersecurity in the electricity sector and compared it with that of neighboring European countries. The study performed a national self-assessment of the cybersecurity capabilities of Swiss electricity companies by implementing the NIST cybersecurity assessment framework. The results showed that the Swiss electricity sector has rudimentary protection of information and operation technology. Another study in India by Kumar et al. (2014) identified key cybersecurity threats across India's power sector. The study found that there are no mandates or policies regarding cybersecurity in the power sector specifically in India. The authors looked at the experience of regulators in other critical sectors in India, such as banking and telecom, as well as power sector regulations internationally. They believe that regulations and specifications from other sectors in India and global power sectors can be applied to the Indian power sector.

Several survey studies have been conducted on cybersecurity in the power sector. Leszczyna (2018) reviewed cybersecurity standards and requirements specified for smart grids, identifying 17 standards. The aim of this study was to present all relevant standards and their cybersecurity requirements. Some of these documents are dedicated to specific smart grid components, such as substations, power plants, advanced metering infrastructure (AMI), industrial control and automation systems (IACS), intelligent electronic devices (IEDs), and plug-in electric vehicles (PEVs). Reda et al. (2022) presented a comprehensive survey research of false data injection (FDI) attacks and their advancements. The authors studied FDI with respect to adversarial models, attack targets, and impacts on smart grid infrastructure. They found that most articles researched adversarial models that require full or partial network resources, while some studied models that use a data-driven approach. They also found that energy management systems are the most affected target in power infrastructure. Rodríguez et al. (2021) analyzed previous cyberattacks on the energy sector, after which they conducted a study on the standards that affect it. The IEE 1686 and IEC 62,351 standards were used to develop a methodology that evaluates the security of cyber-physical systems and electrical installation equipment.

A couple of studies in literature have focused on identifying the cybersecurity challenges that the power sector might face. For example, Krause et al. (2021) looked into challenges in the communication infrastructure to address security concerns that arose due to the interconnectivity of the power grid. The authors identified attack scenarios based on the challenges and approaches to provide security against them. Some of the approaches identified include intrusion detection systems, software-defined networking, and awareness training. Another study was conducted by Ratnam et al. (2020), which investigated whether distributed and renewable electricity (DRE) systems are more resilient than conventional ones due to their multiple pathways, or whether they are less resilient due to having greater cybersecurity risks. The authors identified vulnerabilities in distributed energy systems and from consumer devices. For example, technologies such as rooftop solar, battery storage, and demand response are connected behind the meter outside the reach of utilities, which presents more vulnerable points.

Several studies have proposed approaches to certain cyber threats to the power sector. Sanders et al. (2022) analyzed threats to critical energy infrastructure (CEI) and presented sociotechnical approaches to address these threats. They identified three main areas where recommended approaches are needed: operation technology cyber security, information sharing, and strengthened grid management. Jarmakiewicz et al. (2017) described an approach that can be utilized to protect the control infrastructure for power grids. The authors' analysis indicates that limited knowledge is available regarding cybersecurity solutions for power grid control systems, as no standards exist for developing robust solutions. The paper describes a cybersecurity protection system that is used by transmission and distribution service operators for attack detection and controlled information dissemination. Kolosok and Korkina (2022) proposed a technical approach to improve the cybersecurity of demand response (DR) aggregator structure using cyber-physical management. To increase the mobility of decision making of the DR-aggregator, a feedback loop is created at the lowest structure level, which protects the upper levels from cyber threats.

Testbeds allow researchers to perform security experimentation in realistic environments using a wide variety of technologies that are common in control systems, as well as in the protection or security analysis of networks. The goal of this testbed is to measure the performance of the system when instrumented with cybersecurity protections in

accordance with practices prescribed by prevailing standards and guidelines. Yohanandhan et al. (2021) and Zhao et al. (2021) provide a holistic review of Cyber-Physical Power System (CPPS) testbeds for secure and sustainable electric power grids. These papers reviewed various CPPS research areas, such as: Modelling of CPPS, software tools for modeling and simulation of CPPS, Cyberattacks in CPPS, Cybersecurity and privacy in CPPS, Cascading failure analysis of CPPS, Resilience and reliability analysis of CPPS, Physical power infrastructure of CPPS, Communication networking in CPPS, CPPS Protocols, and Cloud computing and data analytics. The papers highlighted the need for a CPPS testbed for cyberattacks and a long-term cybersecurity analysis of various cyberattacks in the power and energy sectors around the world.

Regarding nano grids, Hueros-Barrios et al. (2022) developed a framework to identify risks and implement protection mechanisms in future nano grid developments. They used an experimental testbed of an advanced nano grid based on a PV system and controllable loads. The study found that the higher the energy price, the higher the security level that should be implemented to minimize the total cost. Another study (Dedrick et al. 2023) used simulation techniques to measure the severity of cyber-attacks under the development of local electricity markets and offer recommendations to deal with them. The local electricity market can change how information flows, increasing the security risks caused by these changes.

Venkatachary et al. (2021) present an assessment of Edge computing-based security systems in virtual power plants (VPPs) and propose a way to adopt them. The paper defines an Edge-centric architecture and proposes solutions to address key protection of VPP devices, including a comprehensive cybersecurity architecture, the application of Edge-based firewalls and intrusion detection systems, and Edge-based authentication and authorization. Another study (Gourisetti et al. 2021) mentions the potential of distributed ledger technology (DLTs) in helping with the worldwide trend of integrating distributed energy sources. The paper presents a DLT cybersecurity stack and demonstrates its potential through several power use cases. The cybersecurity benefits of DLT include providing integrity and immutability for grid communication. The paper also discusses attack vectors and risks associated with DLTs.

In the infrastructure sector, Alladi et al. (2020) and Asghar et al. (2019) reviewed major cyberattacks on industrial control systems (ICSs), including the methodology used in each attack and possible solutions to prevent them. The case studies showed that most ICS attacks were caused by malware injection, hacking outdated networks or systems, or exploiting vulnerabilities. The most common ways in which malware was injected were through phishing emails, insecure connections to the internet, and unsanitized USB drives. Sanders et al. (2022) presented recommendations based on an analysis of the cyber threat to critical infrastructure (CI). These recommendations include addressing the skilled workforce shortage, promoting cyber hygiene and information-sharing practices, developing rich informational resources, standardizing cyber-informed engineering methods, and prioritizing infrastructure needs between current and future infrastructure.

Quigley et al. (2015) highlighted that understanding risk perception can help to understand and predict people's behavior. Awareness of how perceptions are constructed can also improve communication between technical experts and laypersons. Governments have a role to play in this. They can collect, validate, and disseminate more data among owners and operators of critical infrastructure (CI). They can also adopt institutional arrangements to moderate exaggerated claims, and encourage education programs to stimulate a more informed debate over the long term. For instance, China will gradually establish and improve the cybersecurity legal system and establish a strong connection between legislation and practice. Guo (2018) presents ideas for establishing a cybersecurity legal system focusing on China regarding the relevant legislation of developed countries, such as the United States and Japan.

Cybersecurity training programs are available across educational types and levels, but there is no consensus on the best measures and methods for training. Chowdhury et al. (2020) reviewed training solutions, methodologies, target groups, and focus areas for cybersecurity training. They established the current cybersecurity training offerings for critical infrastructure and identified key performance indicators (KPIs) to evaluate their effectiveness. Cheung et al. (2021) reviewed studies on measures that enhance cybersecurity in logistics and supply chain management. They found that there are few studies focusing on cybersecurity in logistics, despite the importance of logistics in supply chains.

We gathered proposed approaches from literature on cybersecurity related to infrastructure. Gao et al. (2022) studied the increasing threat of false data injection attacks (FDIA) towards electricity-gas cyber-physical systems (EGCPS). They proposed a data-driven approach to improve cybersecurity and computational efficiency in fast economic dispatch, while also finding the location of FDIA. The results showed that the approach can achieve detection of FDIA, tampered data recovery, and data-driven fast economic dispatch. Another study by Cassotta and

Sidortsov (2019) looked at the impact of exceptionally critical infrastructure conditions (ECICs), such as remoteness, seasonal darkness, and severe climate, on energy critical infrastructure. They proposed an approach that links cybersecurity and environmental governance through sustainable development and the precautionary and polluter-pays principles of environmental law. The authors proposed three guiding principles: If ECICs are present, then digitization must ensure economic and social development. If the effects of cyberattacks are not known in ECICs, then redundancy, analogue controls, and zero-option alternatives should be used. Actors responsible for cyberattacks are also responsible for all economic, social, and environmental damages and the cost of missed opportunity.

Some papers have identified the cybersecurity challenges that target infrastructure. For example, Moghadasi et al. (2022) proposed a framework to identify possible future scenarios that are most disruptive to electric vehicle (EV) charger embedded systems. Two key vulnerabilities are hardware device vulnerabilities and supply chain issues. The authors developed the framework by conducting interview surveys with experts and stakeholders. Experts were asked about the effectiveness of different criteria on the success of EV charging fleets and how different initiatives would affect the different criteria. On the other hand, Dimitrov et al. (2022) viewed smart cities from a systematic perspective in order to highlight cybersecurity challenges. They proposed a method to reveal the scope of cybersecurity challenges regarding the current state and sustainable development of smart cities by using state-of-the-art technologies. The authors researched three system areas of cybersecurity: regulation, technologies, and subsystems.

Regarding cybersecurity in the transportation sector, Kim et al. (2021) reviewed 151 studies about attack and defense technologies related to autonomous vehicles. They found that research on attacks was mainly conducted on electronic control units (ECUs) and controller area networks (CAN) prior to 2017. However, recent studies have been extensively conducted on external communication attacks, such as on V2X. Research on defense was conducted on areas such as the security of CAN, the security of authentication protocols, and intrusion detection. Regarding attack detection methods, recent studies have considered artificial intelligence techniques to improve the specification of ECUs. Finally, vehicle security models have also been studied, ranging from traditional security models to combining security models with artificial intelligence and deep learning technologies.

Taeihagh and Lim (2019) examined the technological risks associated with autonomous vehicles (AVs) and government responses to address these risks. They found that AVs' data storage and transmission capabilities make them vulnerable to third-party access to users' personal information. Additionally, AV communication networks can be maliciously attacked, compromising cyber and physical security. Regarding privacy risks, the European Union and most governments have implemented new regulations to control access and use of personal data, not specific to AVs. However, the UK and Australia have presented recommendations on how to deal with privacy risks. When it comes to cyberattacks, each country has its own response to manage these issues. These responses range from introducing new non-AV specific solutions, creating groups to explore cybersecurity, funding research in the private sector, and providing cybersecurity principles to manufacturers. The US, China, and Singapore have presented non-AV specific cybersecurity laws. The UK and Singapore show intent to explore cybersecurity risks to improve their adaptability.

Going over the cybersecurity challenges in transportation, Khan et al. (2022) developed a conceptual system dynamics (SD) model to analyze cybersecurity in the complex and uncertain deployment of connected and autonomous vehicles (CAV). The model described various system archetypes to find leverage avenues in intelligent transport systems (ITS) for CAV cybersecurity. Another study by Benyahya et al. (2022) investigated security threats and data privacy concerns regarding automated city shuttles (ACSs) from a technical and legal perspective. They identified two main attack vectors: in-vehicle attacks, which target the internals of ACSs; and external communication threats, which include different communication types that may influence mini-bus operations.

Channon et al. (2021) highlighted the need to reevaluate how to assign responsibility for damages and losses caused by the mass hacking of connected and autonomous vehicles (CAV). They examined the challenges of hacking CAVs and explored the current regulatory regime and issues with apportioning responsibility. Zhang et al. (2019) discussed the cybersecurity of wireless charging for electric vehicles (EVs) and recommended solutions to mitigate vulnerabilities and risks to public safety. Some of the solutions they proposed include encryption, control system monitoring, use of multiple data inputs, and the utilization of CIE methodology. Sayed et al. (2022) investigated the EV charging ecosystem and identified vulnerabilities in EV charging systems that could be exploited to launch attacks on the power grid. Once control of the grid is compromised, it can be attacked by

inducing mass charging and discharging. The authors highlighted that EV charging loads can have a bigger impact on the grid than residential loads.

To address the cybersecurity challenges of the next-generation mobility ecosystem, Argyropoulos et al. (2021) presented the CARAMEL project. The project will bring together 15 partners from Europe to develop cybersecurity solutions for autonomous cars, connected vehicles, and electromobility. Advanced artificial intelligence (AI) and machine learning (ML) techniques will be used to identify anomalies and classify incoming signals that indicate a cyberattack or risk.

Results

Cybersecurity threats to the three sectors numerous and vary depending on intentions and actors. The electric power sector is facing a growing number of cybersecurity threats. These threats can come from a variety of sources, including nation-states, terrorist groups, and organized crime. The nature of these threats is evolving as the electric power sector becomes more reliant on digital technologies, the potential for cyberattacks is increasing. Figure 1 illustrates some the common threats in the papers reviewed by category. It can be seen that the transition to smart grids represents a big challenge to the power sector, along with the importance of data governance and protection. To add to the challenge, several papers referred to the inadequate standards and policies to keep up with the increased digitalization. In critical infrastructure papers, several common threats were identified, and it is usually broad since it covers multiple sectors. One threat to note is the lack in training and expertise. The challenge in training is not only in developing the training materials but also in engaging the end users in these training because every point of access is a point of vulnerability, and it is not enough to have cyber specialists to fully protect the critical infrastructure. In transportation, the EV charging stations is a major concern in addition to communications safety against all attacks that could affect the operation of the EV fleet.

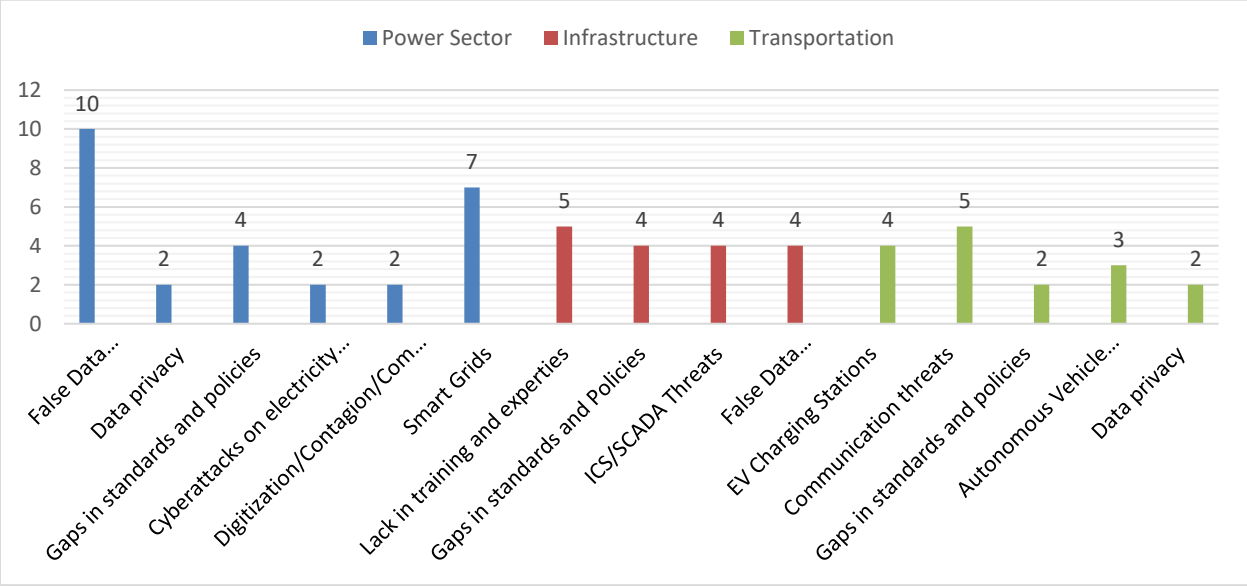

Figure 1: Cybersecurity threats categories per sector

Research papers focusing on different countries policies were reviewed and analysed to uncover energy and cybersecurity policy differences across countries. 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. Governments and industry are taking steps to address these threats. The following points are some general solutions and recommendations for cybersecurity in the power sector, critical infrastructure, and transportation.

- Invest in new cybersecurity technologies. This includes intrusion detection systems, software-defined networking, and blockchain.
- Train employees on cybersecurity best practices. This includes how to identify and report suspicious activity.
- Develop incident response plans. This will help to minimize the impact of a cyberattack.
- Share information and coordinate with other organizations. This will help to identify and respond to threats more quickly.
- Adopt a cross-sectoral approach to cybersecurity. This recognizes that cybersecurity is an issue that affects all sectors of the economy, not just the energy sector.
- Develop cybersecurity standards that are specific to the sector. This will help to ensure that all organizations in the sector are following the same best practices.
- Monitor the cybersecurity landscape and adapt as needed. The threat landscape is constantly evolving, so it is important to be able to adapt to new threats.

In addition to these general solutions, there are also some specific recommendations for cybersecurity in the power sector, critical infrastructure, and transportation: For the power sector, it is important to focus on protecting the critical infrastructure that is essential for keeping the lights on. This includes things like power plants, substations, and transmission lines. For critical infrastructure, it is important to consider the unique risks that each sector faces. For example, the transportation sector is vulnerable to cyberattacks that could disrupt transportation networks. For transportation, it is important to focus on protecting the systems that are used to control vehicles and infrastructure. This includes things like traffic lights, train control systems, and autonomous vehicles.

Conclusion

Cybersecurity is a growing issue for critical infrastructure, and the electric power sector is a high-value target for cyberattacks. There are a variety of cybersecurity solutions for ICSs, including IDS, risk assessment and metrics, and security simulation tools. However, more research is needed in this area, and more work needs to be done to understand the potential vulnerabilities and develop effective mitigation strategies. One of the most important cybersecurity risks is the increasing use of IoT devices in the power grid. IoT devices are creating new cybersecurity vulnerabilities, and they are also making it easier for attackers to gain access to the power grid. In addition to the cybersecurity risks posed by ICSs, the transportation sector is also facing a growing number of threats. Autonomous vehicles (AV), electric vehicles, and other new technologies are introducing new cybersecurity risks. Transportation sector is increasingly connected to the power sector, which creates additional vulnerabilities.

Governments and industry need to work together to develop effective cybersecurity solutions for the electric power and transportation sectors. This includes investing in new technologies, training employees, and developing incident response plans. The electric power sector is critical to the global economy, and it is essential that this sector is protected from cyberattacks. Overall, the research papers provide a valuable overview of the cybersecurity challenges facing the electric power and transportation sectors. These challenges are complex and evolving, but they are essential to address in order to protect critical infrastructure from cyberattacks.

References

[1] Alladi, Tejasvi, Vinay Chamola, and Sherali Zeadally. "Industrial control systems: Cyberattack trends and countermeasures." *Computer Communications* 155 (2020): 1-8.

[2] Argyropoulos, Nikolaos, Pouria Sayyad Khodashenas, Orestis Mavropoulos, Eirini Karapistoli, Anastasios Lytos, Paris Alexandros Karypidis, and Klaus-Peter Hofmann. "Addressing cybersecurity in the next generation mobility ecosystem with CARAMEL." *Transportation Research Procedia* 52 (2021): 307-314.

[3] Asghar, Muhammad Rizwan, Qinwen Hu, and Sherali Zeadally. "Cybersecurity in industrial control systems: Issues, technologies, and challenges." *Computer Networks* 165 (2019): 106946.

[4] Atlantic Council, 2022, Securing the energy transition against cyber threats, https://www.atlanticcouncil.org/in-depth-research-reports/report/securing-the-energy-transition-against-cyber-threats/

[5] Benyahya, Meriem, Anastasija Collen, Sotiria Kechagia, and Niels Alexander Nijdam. "Automated city shuttles: Mapping the key challenges in cybersecurity, privacy and standards to future developments." *Computers & Security* 122 (2022): 102904.

[6] Cassotta, Sandra, and Roman Sidortsov. "Sustainable cybersecurity? Rethinking approaches to protecting energy infrastructure in the European High North." *Energy Research & Social Science* 51 (2019): 129-133.

[7] Channon, Matthew, and James Marson. "THE liability for cybersecurity breaches of connected and autonomous vehicles." *Computer Law & Security Review* 43 (2021): 105628.

[8] Cheung, Kam-Fung, Michael GH Bell, and Jyotirmoyee Bhattacharjya. "Cybersecurity in logistics and supply chain management: An overview and future research directions." *Transportation Research Part E: Logistics and Transportation Review* 146 (2021): 102217.

[9] Chowdhury, Nabin, and Vasileios Gkioulos. "Cyber security training for critical infrastructure protection: A literature review." *Computer Science Review* 40 (2021): 100361.

[10] Dedrick, Jason, Keli A. Perrin, Ehsan Sabaghian, and Peter J. Wilcoxen. "Assessing cyber attacks on local electricity markets using simulation analysis: Impacts and possible mitigations." *Sustainable Energy, Grids and Networks* (2023): 100993.

[11] Dimitrov, Willian, Kamen Spasov, Ivan Trenchev, and Svetlana Syarova. "Complexity Assessment of Research Space for Smart City Cybersecurity." *IFAC-PapersOnLine* 55, no. 11 (2022): 1-6.

[12] Gao, Xiaxiang, Xiyun Yang, Lingzhuochao Meng, and Shuyan Wang. "Fast economic dispatch with false data injection attack in electricity-gas cyber–physical system: A data-driven approach." *ISA transactions* (2022).

[13] Gourisetti, Sri Nikhil Gupta, Ümit Cali, Kim-Kwang Raymond Choo, Elizabeth Escobar, Christopher Gorog, Annabelle Lee, Claudio Lima et al. "Standardization of the Distributed Ledger Technology cybersecurity stack for power and energy applications." *Sustainable Energy, Grids and Networks* 28 (2021): 100553.

[14] Guo, Meirong. "China's cybersecurity legislation, it's relevance to critical infrastructures and the challenges it faces." *International Journal of Critical Infrastructure Protection* 22 (2018): 139-149.

[15] Gur, Berna Akcali. "Cybersecurity, European digital sovereignty and the 5G rollout crisis." *Computer Law & Security Review* 46 (2022): 105736.

[16] Heymann, Fabian, Stéphane Henry, and Matthias Galus. "Cybersecurity and resilience in the swiss electricity sector: Status and policy options." *Utilities Policy* 79 (2022): 101432.

[17] Hueros-Barrios, Pablo José, Francisco Javier Rodríguez Sánchez, Pedro Martín, Carlos Jiménez, and Ignacio Fernández. "Addressing the cybersecurity vulnerabilities of advanced nanogrids: A practical framework." *Internet of Things* 20 (2022): 100620.

[18] Institut francias des relations internationals (IFRI), 2018, Cybersecurity in the Energy Sector: A comparative Analysis between Europe and the United States, https://www.ifri.org/sites/default/files/atoms/files/barichella_cybersecurity_energy_sector_2018.pdf

[19] Jarmakiewicz, Jacek, Krzysztof Parobczak, and Krzysztof Maślanka. "Cybersecurity protection for power grid control infrastructures." *International Journal of Critical Infrastructure Protection* 18 (2017): 20-33.

[20] Jimada-Ojuolape, Bilkisu, and Jiashen Teh. "Surveys on the reliability impacts of power system cyber–physical layers." *Sustainable Cities and Society* 62 (2020): 102384.

[21] Khan, Shah Khalid, Nirajan Shiwakoti, and Peter Stasinopoulos. "A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles." *Accident Analysis & Prevention* 165 (2022): 106515.

[22] Kim, Kyounggon, Jun Seok Kim, Seonghoon Jeong, Jo-Hee Park, and Huy Kang Kim. "Cybersecurity for autonomous vehicles: Review of attacks and defense." *Computers & Security* 103 (2021): 102150.

[23] Kolosok, I., and E. Korkina. "Applying the principles of cyber-physical management to enhance cybersecurity of the Demand Response Aggregator structure." *IFAC-PapersOnLine* 55, no. 9 (2022): 198-203.

[24] Krause, Tim, Raphael Ernst, Benedikt Klaer, Immanuel Hacker, and Martin Henze. "Cybersecurity in power grids: challenges and opportunities." *Sensors* 21, no. 18 (2021): 6225.

[25] Kumar, V. Ananda, Krishan K. Pandey, and Devendra Kumar Punia. "Cyber security threats in the power sector: Need for a domain specific regulatory framework in India." *Energy policy* 65 (2014): 126-133.

[26] Leszczyna, Rafał. "A review of standards with cybersecurity requirements for smart grid." *Computers & security* 77 (2018): 262-276.

[27] Moghadasi, Negin, Zachary A. Collier, Andrew Koch, David L. Slutzky, Thomas L. Polmateer, Mark C. Manasco, and James H. Lambert. "Trust and security of electric vehicle-to-grid systems and hardware supply chains." *Reliability Engineering & System Safety* 225 (2022): 108565.

[28] Pizzi, Giorgio. "Cybersecurity and its integration with safety for transport systems: not a formal fulfillment but an actual commitment." *Transportation research procedia* 45 (2020): 250-257.

[29] Quigley, Kevin, Calvin Burns, and Kristen Stallard. "'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection." *Government Information Quarterly* 32, no. 2 (2015): 108-117.

[30] Rajavuori, Mikko, and Kaisa Huhta. "Digitalization of security in the energy sector: evolution of EU law and policy." *The Journal of World Energy Law & Business* 13, no. 4 (2020): 353-367.

[31] Ratnam, Elizabeth L., Kenneth GH Baldwin, Pierluigi Mancarella, Mark Howden, and Lesley Seebeck. "Electricity system resilience in a world of increased climate change and cybersecurity risk." *The Electricity Journal* 33, no. 9 (2020): 106833.

[32] Reda, Haftu Tasew, Adnan Anwar, and Abdun Mahmood. "Comprehensive survey and taxonomies of false data injection attacks in smart grids: Attack models, targets, and impacts." *Renewable and Sustainable Energy Reviews* 163 (2022): 112423.

[33] Rodríguez, Miguel Ángel Sánchez, Javier Bermejo Higuera, Juan Ramón Bermejo Higuera, Juan Antonio Sicilia Montalvo, and Rubén González Crespo. "A systematic approach to analysis for assessing the security level of cyber-physical systems in the electricity sector." *Microprocessors and Microsystems* 87 (2021): 104352.

[34] Sanders, Peyton, Chris Bronk, and Morgan D. Bazilian. "Critical energy infrastructure and the evolution of cybersecurity." *The Electricity Journal* 35, no. 10 (2022): 107224.

[35] Sayed, Mohammad Ali, Ribal Atallah, Chadi Assi, and Mourad Debbabi. "Electric vehicle attack impact on power grid operation." *International Journal of Electrical Power & Energy Systems* 137 (2022): 107784.

[36] Taeihagh, Araz, and Hazel Si Min Lim. "Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks." *Transport reviews* 39, no. 1 (2019): 103-128.

[37] Tolba, Amr, and Zafer Al-Makhadmeh. "A cybersecurity user authentication approach for securing smart grid communications." *Sustainable Energy Technologies and Assessments* 46 (2021): 101284.

[38] Venkatachary, Sampath Kumar, Annamalai Alagappan, and Leo John Baptist Andrews. "Cybersecurity challenges in energy sector (virtual power plants)-can edge computing principles be applied to enhance security?." *Energy Informatics* 4, no. 1 (2021): 5.

[39] Yohanandhan, Rajaa Vikhram, Rajvikram Madurai Elavarasan, Rishi Pugazhendhi, Manoharan Premkumar, Lucian Mihet-Popa, and Vladimir Terzija. "A holistic review on Cyber-Physical Power System (CPPS) testbeds for secure and sustainable electric power grid–Part–I: Background on CPPS and necessity of CPPS testbeds." *International Journal of Electrical Power & Energy Systems* 136 (2022): 107718.

[40] Yohanandhan, Rajaa Vikhram, Rajvikram Madurai Elavarasan, Rishi Pugazhendhi, Manoharan Premkumar, Lucian Mihet-Popa, and Vladimir Terzija. "A holistic review on Cyber-Physical Power System (CPPS) testbeds for secure and sustainable electric power grid–Part–II: Classification, overview and assessment of CPPS testbeds." *International Journal of Electrical Power & Energy Systems* 137 (2022): 107721.

[41] Yohanandhan, Rajaa Vikhram, Rajvikram Madurai Elavarasan, Rishi Pugazhendhi, Manoharan Premkumar, Lucian Mihet-Popa, Junbo Zhao, and Vladimir Terzija. "A specialized review on outlook of future Cyber-Physical Power System (CPPS) testbeds for securing electric power grid." *International Journal of Electrical Power & Energy Systems* 136 (2022): 107720.

[42] Zhang, Bo, Richard B. Carlson, John G. Smart, Eric J. Dufek, and Boryann Liaw. "Challenges of future high power wireless power transfer for light-duty electric vehicles----technology and risk management." *Etransportation* 2 (2019): 100012.

[43] Zhang, Zhen. "Cybersecurity policy for the electricity sector: the first step to protecting our critical infrastructure from cyber threats." *BUJ Sci. & Tech. L.* 19 (2013): 319.