Exploring Socio-technical Gaps in the Cybersecurity of Energy Informatics for Sustainability

Exploring Socio-Technical Gaps in the Cybersecurity of Energy Informatics for Sustainability

Duong Dang*
School of Technology and Innovations
Vaasa University, Wolffintie 34, 65200, Finland
duong.dang@uwasa.fi
Tero Vartiainen
School of Technology and Innovations
Vaasa University, Wolffintie 34, 65200, Finland
tero.vartiainen@uwasa.fi
* Corresponding authors

Introduction

As the main factor contributing to climate change, energy has been found to account for 60 percent of total global greenhouse gas emissions (United Nations [UN] 2022). Thus, the energy sector has begun to transition from conventional generators to clean and renewable generators. The UN has called for "affordable, reliable, sustainable, and modern energy for all" by 2030 (Sustainable Development Goal 7). The energy transition process must be supported by multidisciplinary research at all levels of the energy system concerning energy informatics (Staudt et al. 2019). In energy informatics, the use of information and communications technology (ICT) and digital technologies is explored to address challenges to the energy domain and sustain the energy system. The involvement of ICT and digital technologies has also brought new challenges. For example, firms require comprehensive approaches to sustaining their business models, such as those focusing on strategy (Dang and Vartiainen 2022), individuals (Dang et al. 2022, Mäkipää et al. 2020), society, technology, and the environment (Thai et al. 2022). Another challenge stems from cybersecurity threats that are embedded in ICT and energy devices and are thus introduced into the energy system.

The term cybersecurity refers to the protection of data, programs, networks, and devices from unauthorized access, attacks, or damage (Chhaya et al. 2020). Cyberattacks are one of the most common threats in the energy sector (Furnell and Emm 2017, Eltahawy and Dang 2022). To prevent cyberattacks, several solutions have been implemented, the majority of which are

based on technical approaches (Venkatachary et al. 2021). Most previous studies on the energy sector have applied a technical approach to devices or systems, while other aspects have been less researched (Ma 2022). However, the literature indicates that, regarding the prevention of cyber threats, the technological focus is not comprehensive enough (Bunker 2012). The reason is that technical systems, the humans who operate them, and organizational contexts are all important for ensuring sustainable energy (Malatji et al. 2019).

Thus, scholars have called for a holistic approach that addresses both technical and nontechnical issues to ensure the effectiveness of security measures (Malatji et al. 2020). As a result, several authors have reviewed the extant literature on the reported roles of nontechnical issues to identify socio-technical gaps in the research on cybersecurity in energy informatics. The socio-technical gap refers to a misalignment between the social and technical dimensions of a system. Moreover, issues such as awareness, policies, and organizational structures can be considered nontechnical, while specific technologies (e.g., firewalls and cyber-physical systems) can be considered technical issues (Whitman and Herbert 2022). Thus, in this chapter, we address the following research question: What are the socio-technical gaps in cyber security in energy informatics? To answer this question, we first identified the nontechnical issues of cyber security in energy informatics by conducting a literature review. We then reflected on socio-technical system theory to identify the socio-technical gaps in the field.

Socio-technical System and its Dimensions

According to the literature, to achieve effective cybersecurity measures, a holistic solution is needed (Malatji et al. 2019). For example, Hagen et al. (2008) found that nontechnical activities (e.g., awareness-creating activities) were more effective organizational measures than technical-administrative ones in information security measures. In a similar vein, Bella et al. (2015) argued that organizations comprise not only software and hardware processes but also people, physical objects, and geographies. Thus, cyber security measures should be approached as the social and technical dimensions of a system, whereas the system's environment should be considered the socio-technical system (Fig. 1). The term socio-technical systems reflects the idea that the design and work of any complex system can only be improved if the system's social and technical dimensions are combined in considering the system's environment (Appelbaum 1997).

<Insert Figure 1 here>

Fig. 1. Socio-technical system

The technical dimension provides the tools and resources used to conduct day-to-day work activities in organizations. This dimension includes technology (e.g., equipment, information, and techniques) and work activities (e.g., tasks and work organization). The social dimension includes functions (e.g., organizational structure) that enable systems of authority, communication, and workflow by people who influence and/or perform work activities in organizations. The social dimension also includes organizational functions (e.g., skills, culture, and policy) and actors or human beings (e.g., humans and human relations). Both social and technical dimensions are embedded within the environmental dimension (e.g., political, economic, and legal) (Malatji et al. 2020).

Description of Literature Study

This systematic review was conducted according to Petticrew and Roberts' (2006) guidelines, as follows: defining the question; carrying out the literature search; screening the identified literature; assessing the eligibility of remaining studies; extracting the data; making a critical appraisal; and synthesizing the literature. We followed Kossahl et al.'s (2012) suggestion to focus on articles containing the terms "energy informatics" OR "smart grid." We then identified the following terms related to cybersecurity (Taylor et al. 2020): "cyber security" OR "cybersecurity" OR "cyber-security."

The literature search was performed on 11 March 2022 and resulted in 1,151 records from the Scopus database, which is accepted as a de facto source for conducting systematic literature reviews. The Scopus database was searched using the following search string: (TITLE-ABS-KEY ("smart grid" OR "energy informatics") AND ("cyber security" OR "cybersecurity" OR "cyber-security") AND (LIMIT-TO (DOCTYPE, "cp" OR "ar" OR "ch"). The search was limited to peer-reviewed articles, as shown in Table 1, Step 1.

Table 1. Steps Used to Conduct the Literature Review

Step	Description	Change	#
1	The literature search string	1,151	1,151
2	Duplicate record or not relevant	-85	1,066
3	Survey or Literature review paper	-43	1,023
4	Technical papers	-877	216
5	Full papers	-5	211

			211

We then performed screening and eligibility checks through searching for titles and abstracts (Step 2). Next, the records were screened for survey and literature review articles focusing on technical issues (Step 3). In Step 4, we determined whether these articles were purely technical, and if so, we omitted them. In Step 5, we read the full papers, five of which we eliminated because they did not meet the research criteria. Because the *Energy Informatics* journal is considered one of the most important publications in the field, we conducted a search of all volumes of the journal using a similar search string. We then conducted forward and backward reference searches of the omitted articles, screened them, and determined those that were eligible. Two articles were added to the previous selection. As a result, we selected 213 articles for this literature review.

The selected articles were coded and synthesized following the guidelines of Webster and Watson (2002). Paré et al.'s (2015) guidelines were followed to ensure the quality of the synthesis, such as its rigor and relevance. The selected articles were coded as follows. Each paper was analyzed based on a review framework, including the core content of the article, the method, theories, and recommendations for future research. We then identified patterns that emerged in the previous step and grouped them into broader topics. Next, two researchers discussed and revised these topics until a consensus was reached. This resulted in the identification of seven issues, which are presented in the next section.

Nontechnical Issues in the Cybersecurity of Energy Informatics

To identify socio-technical gaps in the reviewed articles, we first identified nontechnical issues that were discussed in the articles selected for the literature review.

Education Issue

Education was among the nontechnical issues that emerged from the study. Table 2 shows a brief overview of educational cybersecurity in energy informatics.

Table 2. Education Topics Involving Cybersecurity in Energy Informatics

Program type	Examples	Selected sources
Training program for students	Curriculum, courses (STEM and undergraduate students) Platforms	Kuzlu et al. (2021), Loo and Babinkostova (2020), Navarro et al. (2015) Yardley et al. (2015)

Training program for professional	Skill gaps, workforce, team-taught, and living lab	Srivastava et al. (2017)

Two main types of training programs were discussed, each of which focused on a topic. In particular, the curriculum for cybersecurity in energy informatics was addressed at three equally important levels: cyber security for all, cyber operations, and cyber-informed engineering curriculum (Loo and Babinkostova 2020). In the cyber-informed engineering curriculum, students in science, technology, engineering, and mathematics (STEM) focused on four tracks: software, hardware, firms' power systems, and industrial processes. These articles discussed smart grid education, stating that the curriculum for training should include classical training, manual training, web-based training, and c-level training courses. Kuzlu et al. (2021) argued that smart grid courses should be a part of the electrical engineering technology curriculum, and should include three categories: main smart grid components, communication technologies, cyber security, and smart grid applications. Srivastava et al. (2017) designed a course called Cyberinfrastructure for the Smart Grid. The course's topics, learning objectives, assessment activities, and lessons learned were based on course evaluations obtained from industries and sectors.

Platforms for energy informatics in cyber security education were also explored. For example, Yardley et al. (2015) discussed an energy informatics cyber security education platform based on four pedagogical pillars: active learning, project-based learning, Piaget's learn-by-doing posture, and constructivism. The authors showed that the platform should include the following topics: ethical approach to assessments, enumeration techniques, assessment techniques, and SCADA-specific manipulation and assessment. Soultatos et al. (2020) discussed a cybersecurity training platform called THREAT-ARREST, which offers training on known and/or new advanced cyberattack scenarios. The platform provides security testing, monitoring, and assessment tools at different layers in the implementation stack (e.g., tools for the network, infrastructure, and application layers).

Human Issue

Technology plays a vital role in fighting cybercrime threats. However, previous studies have emphasized that technology cannot always affect cybercrime. Instead, human behavior is considered a critical component because humans can be vulnerable and easily deceived. Therefore, technical advances alone are inadequate for preventing cybercrime. According to

Back and LaPrade (2019), both technology and human factors must be considered in approaches to cybersecurity.

We identified two issues regarding human perspectives in the selected articles: the role of human failures in security and cyber security leadership. In particular, Aldabbas and Teufel (2016) argued that the security of smart technologies in energy systems cannot rely solely on technical solutions. Humans play a significant role in the failure of cyber security, whether intentional or unintentional. These authors also presented a human-oriented framework for failure reduction to enhance security. Auffret et al. (2017) discussed the importance of cyber security governance and technology principles in tackling cyber security challenges in industrial control systems and smart grid systems, which would help enterprises protect against cyber threats. Human issues such as management, including technical management (Lamba et al. 2019), were addressed, although there were no significant discussions on their relationship to human issues.

Cyber Security Awareness Issue

Hagen et al. (2008) found that awareness measures played a significant role in the effectiveness of organizational security and were more important than technical–administrative security measures. Examples of awareness included training, awareness programs, user participation, and top management commitment. Two types of awareness were frequently discussed in the selected papers, as shown in Table 3.

Table 3. Types of Awareness of Cybersecurity in Energy Informatics

Types of Awareness	Examples	Selected sources
Social awareness	Human factor	Singh et al. (2017), Greitzer (2010), Scholtz et al. (2016)
	Behaviors	Holm et al. (2013)
Situation awareness	Tools help operators aware of threats	Angelini and Santucci (2015), Mavridou and Papa (2012), Mavridou et al. (2012)

Social awareness helps to improve cyber security in energy informatics. For example, Singh et al. (2017) proposed that building greater social sensitivity into the operation of the system

would enhance demand-side and emergency management. The awareness included four perspectives: socioeconomic consumer data; load disaggregation capability; end-use device database; and smart power hubs. Scholtz et al. (2016) conducted interviews with dispatchers, concluding that dispatchers should not be solely responsible for monitoring systems for signs of cyberattacks because several actors are also important (e.g., IT personnel, procedures, and cyber security information). Holm et al. (2013) studied the awareness of phishing and concluded that although users are deceived, they do not report such attacks, and it is important that managers be aware of this issue.

Situation awareness was another topic that emerged from the literature review. The selected studies indicated that architecture and tools are required to help operators monitor and be aware of actual threats that exist between the network level and the business level (Angelini and Santucci 2015, Mavridou et al. 2012).

Policy Issue

We placed articles on legal, regulatory, and policy topics in the category of policy issues. Two types of policies that were discussed in these studies were policy challenges in cyber security in energy informatics and policies themselves, as shown in Table 4.

Table 4. Policy on Cyber Security in Energy Informatics

Types	Selected sources
Policy challenges	Mah et al. (2014), Kasper (2014), Campbell (2016), Mylrea (2017), Antonov et al. (2021)
Policy itself	Mylrea (2017), Kasper (2014), Campbell (2016)

Most articles in this category focused on policy challenges regarding cyber security in energy informatics. For example, one concern was that products in energy informatics focused on testing essential functionalities but were not concerned with cybersecurity or privacy until large-scale deployment (Kasper 2014). Therefore, this author called for the intervention of regulators in bridging gaps in the identification and designation of national critical infrastructures and critical information infrastructures in organizations, such as member states of the European Union (EU), such as clear guidance on mandates and roles, rules for mandatory risk assessments, and alternative methodologies and standards for the application of cyber security measures).

Privacy, personal data and data security were also concerns (Antonov et al. 2021). For example, the GDPR framework could be fulfilled when an increasing number of devices are used in the energy informatics field (e.g., smart devices), concerns about privacy and data security in sharing information in applications, and government-industry coordination (Campbell 2016).

Geography Issue

Table 5 shows the geographical regions and topics discussed in the literature on cybersecurity in energy informatics. These articles were based on studies conducted in the EU, North America, and Asia.

Table 5. Regions and Topics in Cyber Security in Energy Informatics

Region	Example	Selected sources
EU	Cybersecurity framework IT security	Pavleska et al. (2020), Genzel et al. (2017), Pearson (2011), Holzleitner and Reichl (2017) Wagner et al. (2012)
US	Risk analysis framework	Baggott and Santos (2020)
Asia	Cybersecurity threats Roles of cybersecurity	Ananda Kumar et al. (2014), Kumar and Inbaraj (2020), Rohokale and Prasad (2017) Ugale et al. (2011)

In general, the NIST Cyber Security Framework and ISO standards have been widely adopted by the EU's critical infrastructure (e.g., ISO 27001, or ISA 62443). The European Union Agency for Cyber Security provides security guidelines to support the implementation of high security standards for critical infrastructures. The Department of Homeland Security also provides security guidelines. In particular, the NIST has drafted a cyber security framework that defines a set of cyber security activities regulated by international security standards and provides a methodology that complements the risk management process, thus helping organizations implement a cyber security plan. The framework has been broadly applied across many critical sectors. Furthermore, Pavleska et al. (2020) proposed the reference model for information assurance and security, which provides a general methodological cycle for the full life of an information system, including its inception, operation, monitoring, and retirement.

Renewable energy resources are decentralized and interconnected to virtual power plants using shared networks (e.g., WAN, the Internet), standard IT protocols, commercial off-the-shelf hardware, and software. This development has raised security concerns, as known threats

from office ITs are applicable to industrial control systems (Genzel et al. 2017). Thus, standardization is mandatory to ensure sophisticated security mechanisms throughout the entire network (Wagner et al. 2012). Although the US and the EU have focused on solutions, it appears that Asian countries have discussed threats and the need for solutions. For example, Ananda Kumar et al. (2014) described the need for a domain-specific regulatory framework in India, and Rohokale and Prasad (2017) investigated the role of technology in cyber security.

Standards Issue

The standards issue includes topics on standards, frameworks, and models. There were 28 articles in this category, which we categorized into two topics: cybersecurity standards in general (e.g., NIST and IEC) and specific cybersecurity standards (e.g., standards for SCADA systems), as shown in Table 6.

Table 6. Standards in Cyber Security in Energy Informatics

Category	Example	Selected sources
Standard	Cyber security assessment	Leszczyna (2018)
	Overview	Ruland et al. (2017)
	Technical countermeasures	Hussain et al. (2018)
	Guidelines	Leszczyna (2019), Goraj et al. (2012)
Particular	SCADA system cyber security standards	Sommestad et al. (2010)
	Digital twins	Atalay and Angin (2020)

Because security evaluations and assessments pose significant challenges to both developers and operators, several articles focused on cyber security assessment standards (Leszczyna 2018). Security assessment has been defined according to several standards or government agencies, such as IEC TS 62351-1, NIST SP 800-53/800-115, or the DHS. Security assessment techniques have also been examined (Leszczyna 2018), such as passive reviews, vulnerability identification, and vulnerability analyses. Several standards, regulations, and guidelines have been studied, such as IEC 62351, ISO/IEC 27000/15118, and NIST SP 800-53/800-82 (Ruland et al. 2017). Leszczyna (2019) examined guidelines for standardized cybersecurity controls, and Castro et al. (2018) discussed high-level guidelines that allow for simplifying security assessments in distribution networks. In terms of technical countermeasures, regulatory bodies related to smart grids have been found to exist at both national and international levels, such as NIST in the US, SGCC in China, and IEEE/IEC worldwide. The industry follows these standards to ensure quality and acceptance by clients (e.g., IEC 62351/62541, RFC 6272, and

NIST 7628) (Hussain et al. 2018). However, cyberattacks and countermeasures have been studied mainly by academics who have focused on existing issues and proposed preventive measures and protection approaches to increasing the resiliency of smart grids in the face of internal and external attacks.

The articles in this category also focused on standards for a specific system. For example, Sommestad et al. (2010) discussed SCADA system cyber security standards. They compared different SCADA cybersecurity standards and guidelines concerning the threats and countermeasures they described. These authors also made comparisons with the international standard ISO/IEC 27002. They concluded that SCADA-specific standards focus on technical countermeasures, such as firewalls and intrusion detection, whereas ISO/IEC 17799 focuses on organizational countermeasures. Other articles discussed digital twin standards or information security standard architectures applied to guide electric power utilities (Gourisetti et al. 2021).

Risk, Challenge, and Solution Issues

Many of the selected articles in this category focused on risks (Civlez et al. 2020, Lamba et al. 2019), challenges (Velayutham et al. 2021), and solutions (Abir et al. 2021, Velayutham et al. 2021) for cyber security in energy informatics. First, risk topics included the risk assessment of power information control systems (Woo et al. 2019), energy Internet (Wei et al. 2017), digital secondary substations, renewable energy (de Peralta et al. 2020), smart grids (Smith and Pate-Cornell 2018), physical systems, and economic risk (Hébert 2013). Alshawish and de Meer (2019) proposed a methodology to support defenders of electric power networks in assessing priorities and making decisions on the importance of remediation activities. Forty-eight articles discussed challenges and solutions, among which challenges in smart grids were a frequent topic (30 of 48 articles). Examples are hyperphysical challenges (Dumitrache and Dogaru 2015), information security and privacy challenges (Alrefaei et al. 2021), technology challenges (e.g., AI, big data, and IoT) (Abir et al. 2021, Younes et al. 2021), and communications challenges (Srivastava et al. 2022). In addition to the smart grid, challenges in modeling were addressed (de Kinderen and Kaczmarek-Heß 2021). Third, the topics included solutions in general (Silpa et al. 2018, Velayutham et al. 2021), solutions to cyber security in a physical system (Essa et al. 2018, Zhou et al. 2017), on the demand side (Ipakchi 2011), in blockchains, solutions for cyber security (Moradi et al. 2019), and guidelines for NISTIR 7628 (Harvey et al. 2014).

Discussion

Socio-Technical Gaps in Cyber Security in Energy Informatics

Based on the findings of our literature review, we discuss the following socio-technical gaps in the context of cyber security in energy informatics.

Misalignment between Technical Dimensions and Social Dimensions

The findings suggest that the literature in this field focuses mainly on technocentric approaches to addressing cyber security risk, neglecting the general need for a sustainable energy system. The findings of our review suggest that at least 90% of cyberattacks result from human error or behavior and that humans are the weakest link in the enterprise security chain (Carlton et al. 2019, Heartfield and Loukas 2018, Malatji et al. 2020). However, existing security solutions and frameworks consider cyber security primarily a technical issue (Malatji et al. 2019). Not surprisingly, most standards related to cybersecurity in energy informatics focus on technical dimensions. Thus, the social and environmental dimensions have been less researched and discussed. Our findings indicate that technical and social dimensions have been misaligned in cybersecurity in energy informatics.

To address these misalignments, we suggest that socio-technical views (e.g., patterns of behavior, knowledge, people relations, team groups, customs, physical environment, built environment, and geographical locations, among others) should be considered in all measures used to respond to cyber security threats in the energy informatics field. The reason is that the social, technical, and environmental dimensions are crucial for enterprise system security safeguards and maintaining acceptable levels of organizational system performance, reliability, and cost (Borky and Bradley 2019, Malatji et al. 2020).

Social and Technical Awareness of Cyber Security Topics

A lack of awareness is considered one of the most important human-related issues because it is the main cause of security breaches (Kritzinger and von Solms 2005). Thus, human-centered approaches should be applied when organizations deal with security threats and vulnerabilities. Moreover, because awareness, including situational awareness, is also a key factor in cyber defense, operators should intervene, mitigate risks, and determine the effects on an organization's mission (Angelini and Santucci 2015). It has been argued that an effective awareness program could be the most cost-effective initiative that a company could take to protect its critical information assets (Gardner and Thomas 2015). Unfortunately, among the articles selected for this literature review, the few that focused on this approach did not consider the socio-technical aspects of awareness.

To improve awareness from both technical and social perspectives, future research should focus on a cybersecurity awareness program that helps involved stakeholders become aware of security policies and issues in the organization, as well as understand the importance of cybersecurity. These awareness programs should be included in training programs, educational curricula, policies, and standards. Such programs should include not only technical and societal aspects of awareness but also national and international perspectives on this issue. For example, an assessment of the maturity of the cybersecurity awareness framework in organizations could help organizations develop a holistic approach to cybersecurity measures, thus improving their cybersecurity.

Holistic Cyber Security Frameworks and Standards

Many articles have discussed frameworks, such as standards and models, and solutions, including risks and challenges. For example, capability models have been used to assess the maturity of cyber security capability in institutions. Several maturity models and frameworks for cyber security have been proposed, such as the Center for Internet Security, Capability Maturity Model Integration, COBIT 5 for Information Security, ISO/IEC 27002, and ITIL. However, most mature cyber security capability frameworks focus on technical issues (Malatji et al. 2019). Moreover, in the articles selected for this literature review, there was no discussion about the maturity of cyber security capability in energy informatics regarding both the social and technical dimensions.

To address this gap, future research in this field should focus not only on technical dimensions but also on the security requirements of the social dimension in the energy sector. For example, dynamic capability models should be considered from a holistic view of technical, social, and environmental aspects, which we term the "dynamic security agility" approach. Here, we refer to dynamic capability as the ability to purposefully adapt an organization's resource base to address rapidly changing environments (Teece et al. 1997).

Imbalance in Educational Cybersecurity

Our findings showed that two types of training programs have been discussed in the literature: training programs for professionals and training programs for students. The findings also revealed that curricula in computer science and engineering have focused on technical matters; hence, the views of other disciplines regarding information systems, human behavior, and management have not been considered.

To improve this situation, we suggest that cybersecurity in energy informatics should apply a holistic view that includes both technical and nontechnical issues to increase the effectiveness of security measures (Malatji et al. 2020). Educational programs should use holistic approaches that include technical, social, and environmental contexts. For example, these programs could be built based on socio-technical systems with dynamic capabilities. For example, social dimensions include human issues and awareness issues, whereas environmental dimensions include policy issues and geographical issues. This approach could involve higher-level activities that enable an organization to change its resources to achieve organizational survival and growth.

Conclusions

This study makes several contributions to the literature by identifying socio-technical gaps in previous research. Closing these gaps would help organizations respond to cyber threats in a socio-technical manner, which would sustain their energy systems. Based on further research in this field, organizations would develop a holistic approach to responding to security threats and vulnerabilities without emphasizing one aspect more than the other. That is, the technical dimensions, social dimensions, and environmental dimensions of organizational work practices should be considered equally important.

We also contribute to the literature by identifying common nontechnical issues in cyber security in energy informatics. In particular, the findings of this review study suggest that overly technocentric approaches to cyber security have been applied in this field. This finding is in line with previous studies that found that existing security solutions or frameworks considered cyber security primarily a technical issue (Laybats and Tredinnick 2016). Nonetheless, in the articles selected for this review, we identified seven nontechnical issues that have been discussed in the literature: education, human input, awareness, policy, geography, standards, risk, challenges, and solutions.

Our chapter also has several practical implications. First, nontechnical approaches can help managers and policymakers apply holistic measures to prevent cybercrime. For example, cybersecurity awareness should be considered a priority by managers to ensure the effectiveness of organizational security. Nontechnical approaches are as important as technical-administrative security measures. Second, policymakers should be aware that cybersecurity in energy informatics has been subject to an overly technocentric focus, which has led to the neglect of an overall consideration of cyber defenses and cyber measures. Thus, new policies

on this topic should include technical, social, and environmental dimensions so that every aspect of cyber security is covered. Third, educators can use this study as a reference for developing programs and curricula regarding cyber security in energy informatics.

This study has the following limitations. Only articles in English were selected and analyzed, which may have biased the results. In addition, only the online Scopus database was searched, so relevant articles published in journals, book chapters, or conferences not indexed in this database may have been missed.

Acknowledgments

A previous version of this chapter was presented at the 11th DACH+ Conference on Energy Informatics, 15-16 September 2022 (Freiburg im Breisgau, Germany) as poster paper #S33, "Cyber Security in Energy Informatics: A Non-technical Perspective".

References

Abir, S. M. A. A., A. Anwar, J. Choi and A. S. M. Kayes. 2021. Iot-enabled smart energy grid: Applications and challenges. IEEE Access 9: 50961–50981.

Aldabbas, M. and B. Teufel. 2016. Human aspects of smart technologies' security: The role of human failure. Journal of Electronic Science and Technology 14: 311–318.

Alrefaei, F., A. Alzahrani, H. Song, M. Zohdy and S. Alrefaei. 2021. Cyber physical systems, aare new challenge, and security issues for the aviation. 2021 IEEE International IOT, Electronics and Mechatronics Conference, IEMTRONICS 2021.

Alshawish, A. and H. de Meer. 2019. Risk mitigation in electric power systems: Where to start? Energy Informatics 2: 1–25.

Ananda Kumar, V., K. K. Pandey and D. K. Punia. 2014. Cyber security threats in the power sector: Need for a domain specific regulatory framework in India. Energy Policy 65: 126–133.

Angelini, M. and G. Santucci. 2015. Visual cyber situational awareness for critical infrastructures. In B. P., I. T., and T. S. (eds.), 8th International Symposium on Visual Information Communication and Interaction, VINCI 2015: 83–92.

Antonov, A., T. Haring, T. Korotko, A. Rosin, T. Kerikmae and H. Biechl. 2021. Pitfalls of Machine Learning Methods in Smart Grids: A Legal Perspective. 5th ISCSIC 2021: 248–256.

Appelbaum, S. H. 1997. Socio-technical systems theory: an intervention strategy for organizational development. Management Decision 35: 452–463.

Atalay, M. and P. Angin. 2020. A Digital Twins Approach to Smart Grid Security Testing and Standardization. 2020 IEEE International Workshop on Metrology for Industry 4.0 and IoT, MetroInd 4.0 and IoT 2020: 435–440.

Auffret, J.-P., J. L. Snowdon, A. Stavrou, J. S. Katz, D. Kelley, R. S. Rahman, et al. 2017. Cybersecurity Leadership: Competencies, Governance, and Technologies for Industrial Control Systems. Journal of Interconnection Networks 17.

Back, S. and J. LaPrade. 2019. The Future of Cybercrime Prevention Strategies: Human Factors and A Holistic Approach to Cyber Intelligence. The International Journal of Cybersecurity Intelligence and Cybercrime 2: 1–4.

Baggott, S. S. and J. R. Santos. 2020. A Risk Analysis Framework for Cyber Security and Critical Infrastructure Protection of the U.S. Electric Power Grid. Risk Analysis 40: 1744–1761.

Bella, G., P. Curzon and G. Lenzini. 2015. Service security and privacy as a socio-technical problem. Journal of Computer Security 23: 563–585.

Borky, J. M. and T. H. Bradley. 2019. Protecting Information with Cybersecurity. Effective Model-Based Systems Engineering: 345–404.

Bunker, G. 2012. Technology is not enough: Taking a holistic view for information assurance. Information Security Technical Report 17: 19–25.

Campbell, R. J. 2016. The smart grid and cybersecurity-regulatory policy and issues. In Electricity Delivery and Security: Federal Oversight, Activities and Funding. Nova Science.

Carlton, M., Y. Levy and M. Ramim. 2019. Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. Information and Computer Security 27: 101–121.

Castro, F., J. Velásquez, D. Babazadeh and S, Lehnhoff. 2018. Systematic dynamic assessment for resilient operation of distribution networks. Energy Informatics 1: 243–263.

Chhaya, L., P. Sharma, A. Kumar and G. Bhagwatikar. 2020. Cybersecurity for Smart Grid: Threats, Solutions and Standardization. In Green Energy and Technology. Springer.

Civlez, M., M. Demirtas, I. Cetinbas and H. Akinc. 2020. Security Applications for Reliable Energy Management in a Microgrid. 2nd ICECCE 2020.

Dang, D. and T. Vartiainen. 2022. Digital Strategy in Information Systems: A Literature Review and an Educational Solution Based on Problem-Based Learning. Journal of Information Systems Education 33: 261–282.

Dang, D., T. Mäenpää, J. Mäkipää and T. Pasanen. 2022. The Anatomy of Citizen Science Projects in Information Systems. First Monday 57.

de Kinderen, S. and M. Kaczmarek-Heß. 2021. Making a Case for Multi-level Reference Modeling – A Comparison of Conventional and Multi-level Language Architectures for Reference Modeling Challenges. Wirtschaftsinformatik, WI 2021.

de Peralta, F. A., A. M. Gorton, M. D. Watson, R. M. Bays, J. R. Boles, B.T. Gorton, et al. 2020. Cybersecurity resiliency of marine renewable energy systems–part 1: Identifying cybersecurity vulnerabilities and determining risk. Marine Technology Society Journal 54: 97–107.

Dumitrache, I. and D. I. Dogaru. 2015. Smart grid overview: Infrastructure, cyber-physical security and challenges. 20th International Conference on Control Systems and Computer Science, CSCS 2015.

Essa, A., T. Al-Shoura, A. Al Nabulsi, A. R. Al-Ali and F. Aloul. 2018. Cyber Physical Sensors System Security: Threats, Vulnerabilities, and Solutions. 2nd ICSGSC 2018: 62–67.

Eltahawy, B. and D. Dang. 2022. Understanding Cyberprivacy: Context, Concept, and Issues. Wirtschaftsinformatik 2022 Proceedings.

Furnell, S, and D. Emm. 2017. The ABC of ransomware protection. Computer Fraud and Security 2017: 5–11.

Gardner, B. and V. Thomas. 2015. Building an Information Security Awareness Program: Defending Against Social Engineering Hacks and Technical Threats. Elsevier.

Genzel, C.-H., O. Hoffmann and R. Sethmann. 2017. IT-security for smart grids in Germany: Threats, countermeasures and perspectives. 16th ECCWS 2017:137–145.

Goraj, M., J. Gill and S. Mann. 2012. Recent developments in standards and industry solutions for cyber security and secure remote access to electrical substations. 11th IET DPSP 2012, 2012(593 CP).

Gourisetti, S. N. G., Ü. Cali, K.-K. R. Choo, E. Escobar, C. Gorog, A. Lee, et al. 2021. Standardization of the Distributed Ledger Technology cybersecurity stack for power and energy applications. Sustainable Energy, Grids and Networks 28.

Greitzer, F. L. 2010. Wide-area situation awareness in electric power grid. Cyber Security, Situation Management, and Impact Assessment II; and Visual Analytics for Homeland Defense and Security II, 7709.

Hagen, J. M., E. Albrechtsen and J. Hovden. 2008. Implementation and effectiveness of organizational information security measures. Information Management and Computer Security 16: 377–397.

Harvey, M., D. Long and K. Reinhard. 2014. Visualizing NISTIR 7628, Guidelines for smart grid cyber security. 2014 IEEE PECI.

Heartfield, R. and G. Loukas. 2018. Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. Computers and Security 76: 101–127.

Hébert, C. 2013. The most critical of economic needs (risks): A quick look at cybersecurity and the electric grid. Electricity Journal 26: 15–19.

Holm, H., W. R. Flores and G. Ericsson. 2013. Cyber security for a Smart Grid - What about phishing? 2013 4th IEEE/PES Innovative Smart Grid Technologies Europe, ISGT Europe 2013.

Holzleitner, M.-T. and J. Reichl. 2017. European provisions for cyber security in the smart grid – an overview of the NIS-directive . Elektrotechnik Und Informationstechnik, 134: 14–18.

Hussain, S., M. Meraj, M. Abughalwa and A. Shikfa. 2018. Smart Grid Cybersecurity: Standards and Technical Countermeasures. 2018 International Conference on Computer and Applications, ICCA 2018: 136–140.

Ipakchi, A. 2011. Demand side and distributed resource management - A transactive solution. 2011 IEEE PES General Meeting: The Electrification of Transportation and the Grid of the Future.

Kasper, A. 2014. Legal aspects of cybersecurity in emerging technologies: Smart grids and big

data: European answers to security breaches and “common” cyber crime. Springer.

Kossahl, J., S. Busse and L. M. Kolbe. 2012. The Evolvement of Energy Informatics in the Information Systems Community - A Literature Analysis and Research Agenda. ECIS 2012 Proceedings.

Kritzinger, E., and von Solms, P. S. H. 2005. Five Non-Technical Pillars of Network Information Security Management 277–287.

Kumar, V. and P. Inbaraj. 2020. Overview on Cyber Security Threats Involved in the Implementation of Smart Grid in Countries like India. In Lecture Notes on Data Engineering and Communications Technologies 31: 678–684.

Kuzlu, M., O. Popescu and V. M. Jovanovic. 2021. Development of a Smart Grid Course in an Electrical Engineering Technology Program. 2021 ASEE Virtual Annual Conference, ASEE 2021.

Lamba, V., N. Šimková and B. Rossi. 2019. Recommendations for smart grid security risk management. Cyber-Physical Systems 5: 92–118.

Laybats, C. and L. Tredinnick. 2016. Information security. Business Information Review 33: 76–80.

Leszczyna, R. 2018. Standards on cyber security assessment of smart grid. International Journal of Critical Infrastructure Protection 22: 70–89.

Leszczyna, R. 2019. Standards with cybersecurity controls for smart grid—A systematic analysis. International Journal of Communication Systems 32:6.

Loo, S. M. and L. Babinkostova. 2020. Cyber-physical systems security introductory course for STEM Students. 2020 ASEE Virtual Annual Conference, ASEE 2020.

Ma, Z. 2022. The importance of systematical analysis and evaluation methods for energy business ecosystems. Energy Informatics 2022 5: 1–6.

Mah, D., K. P.-Y. Leung and P. Hills. 2014. Smart grids: The regulatory challenges.

Malatji, M., A. Marnewick and S. von Solms. 2020. Validation of a socio-technical management process for optimising cybersecurity practices. Computers and Security 95: 101846.

Malatji, M., S. Von Solms and A. Marnewick. 2019. Socio-technical systems cybersecurity framework. Information and Computer Security 27: 233–272.

Mavridou, A. and M. Papa. 2012. A situational awareness architecture for the smart grid. In Joint 7th ICGS3 2011, and the 4th Conference on e-Democracy 99: 229–236.

Mavridou, A.,V. Zhou, J. Dawkins and M. Papa. 2012. A situational awareness framework for securing the smart grid using monitoring sensors and threat models. International Journal of Electronic Security and Digital Forensics 4: 138–153.

Mäkipää, J-P., D. Dang, T. Mäenpää and T. Pasanen. 2020. Citizen Science in Information Systems Research: Evidence from a Systematic Literature Review. Hawaii International Conference on System Sciences 2020 (HICSS-53).

Moradi, J., H. Shahinzadeh, H. Nafisi, G.B. Gharehpetian and M. Shaneh. 2019. Blockchain, a Sustainable Solution for Cybersecurity Using Cryptocurrency for Financial Transactions in Smart Grids. 24th Electrical Power Distribution Conference, EPDC 2019: 47–53.

Mylrea, M. 2017. Smart energy-internet-of-things opportunities require smart treatment of legal, privacy and cybersecurity challenges. Journal of World Energy Law and Business 10: 147–158.

Navarro, D., J. C. Mendez, K. Berrios, E. Ortiz-Rivera and E. Arzuaga. 2015. Using cybersecurity as an engineering education approach on computer engineering to learn about Smart Grid technologies and the next generation of electric power systems. 44th Annual Frontiers in Education Conference.

Paré, G., M.C. Trudel, M. Jaana and S. Kitsiou. 2015. Synthesizing information systems knowledge: A typology of literature reviews. Information & Management 52: 183–199.

Pavleska, T., H. Aranha, M. Masi and G. P. Sellitto. 2020. Drafting a cybersecurity framework profile for smart grids in EU: A goal-based methodology. 16th European Dependable Computing Conference 1279:143–155.

Pearson, I. L. G. 2011. Smart grid cyber security for Europe. Energy Policy 39: 5211–5218.

Petticrew, M. and H. Roberts. 2006. Systematic Reviews in the Social Sciences: A Practical Guide (First Edit). Blackwell.

Rohokale, V. and R. Prasad. 2017. Role and importance of the cyber security for developing smart cities in India. River Publishers.

Ruland, K. C., J. Sassmannshausen, K. Waedt and N. Zivic. 2017. Smart grid security – an overview of standards and guidelines . Elektrotechnik Und Informationstechnik 134: 19–25.

Scholtz, J., L. Franklin, K. Le Blanc and E. Andersen. 2016. Cybersecurity awareness in the power grid. International Conference on Human Factors in Cybersecurity, 2016. Springer.

Silpa, P., G. S. Menon and S. N. Rao. 2018. MICRO GRID: Security Issues and Solutions. 8th IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2017.

Singh, A., A. Pooransingh, C. J. Ramlal and S. Rocke. 2017. Toward Social Awareness in the Smart Grid. 8th International Conference on Computational Intelligence and Communication Networks, CICN 2016.

Smith, M. D. and M. E. Pate-Cornell. 2018. Cyber risk analysis for a smart grid: How smart is smart enough? A multiarmed bandit approach to cyber security investment. IEEE Transactions on Engineering Management 65: 434–447.

Sommestad, T., G. N. Ericsson and J. Nordlander. 2010. SCADA system cyber security - A comparison of standards. IEEE PES General Meeting, PES 2010.

Soultatos, O., K. Fysarakis, G. Spanoudakis, H. Koshutanski, E. Damiani, K. Beckers, et al. 2020. The THREAT-ARREST Cyber-Security Training Platform. 2nd International Workshop on Information and Operational Technology (IT and OT) security systems, IOSec 2019, Vol. 11981 LNCS: 199–214.

Srivastava, A. K., A. L. Hahn, O. O. Adesope, C. H. Hauser and D. E. Bakken. 2017. Experience with a multidisciplinary, team-taught smart grid cyber infrastructure course. IEEE Transactions on Power Systems 32: 2267–2275.

Srivastava, I., S. Bhat and A. R. Singh. 2022. Smart Grid Communication: Recent Trends and Challenges. In Lecture Notes in Electrical Engineering 824: 49–75.

Staudt, P., S. Lehnhoff and R. Watson. 2019. Energy Informatics. Business & Information Systems Engineering 61: 767–769.

Taylor, P. J., T. Dargahi, A. Dehghantanha,R. M. Parizi and K. K. R. Choo. 2020. A systematic literature review of blockchain cyber security. Digital Communications and Networks 6: 147–156.

Teece, D. J., G. Pisano and A. Shuen. 1997. Dynamic capabilities and strategic management. Strategic Management Journal 18: 509–533.

Thai, D. M., D. Dang, M. Falch, C. B. Xuan and T. T. T. Thu. 2022. Factors Affecting the Sustainability of Telecentres in Developing Countries. Telecommunications Policy 46: 102265.

Ugale, B. A., P. Soni, T. Pema and A. Patil. 2011. Role of cloud computing for smart grid of India and its cyber security. 2011 Nirma University International Conference on Engineering: Current Trends in Technology, NUiCONE 2011.

UN. 2022. Energy - United Nations Sustainable Development. https://www.un.org/sustainabledevelopment/energy/ [Accessed 06 June 2022]

Velayutham, Y., N. A. A. Bakar, N. H. Hassan and G. N. Samy. 2021. IoT security for smart grid environment: Issues and solutions. Jordanian Journal of Computers and Information Technology 7: 13–24.

Venkatachary, S. K., A. Alagappan and L. J. B. Andrews. 2021. Cybersecurity challenges in energy sector (virtual power plants) - can edge computing principles be applied to enhance security? Energy Informatics 4: 1–21.

Wagner, M., M. Kuba and A. Oeder. 2012. Smart grid cyber security: A German perspective. 2012 International Conference on Smart Grid Technology, Economics and Policies, SG-TEP 2012.

Webster, J. and R. T. Watson. 2002. Analyzing the Past to Prepare for the Future: Writing a Literature Review on JSTOR. MIS Quarterly 26: xiii–xxiii.

Wei, M., Z. Yang, F. Zhou and H. Hou. 2017. Discussion on risk assessment of energy internet. 2017 IEEE Conference on Energy Internet and Energy System Integration.

Whitman, M. and M. Herbert. 2022. Principles of Information Security (7th Ed.,). Cengage Learning.

Woo, P. S., S. S. Hwang, S. H. Hwang and B. H. Kim. 2019. Risk assessment for the security of power information control systems. International Journal of Smart Grid and Clean Energy 8: 488–494.

Yardley, T., S. Uludag, K. Nahrstedt and P. Sauer. 2015. Developing a Smart Grid cybersecurity education platform and a preliminary assessment of its first application. 44th Annual Frontiers in Education Conference, FIE 2014, 2015.

Younes, Z., I. Alhamrouni S. Mekhilef and M. R. B. Khan. 2021. Blockchain Applications and Challenges in Smart grid. 5th IEEE Conference on Energy Conversion, CENCON 2021 208–213.

Zhou, K., T. Liu and L. Liang. 2017. Security in cyber-physical systems: Challenges and solutions. International Journal of Autonomous and Adaptive Communications Systems 10: 391–408.

Keywords: energy informatics, nontechnical issues, cyber security, socio-technical gap, literature review, sustainability, energy sector, cyber security awareness, holistic cyber security framework, educational cyber security

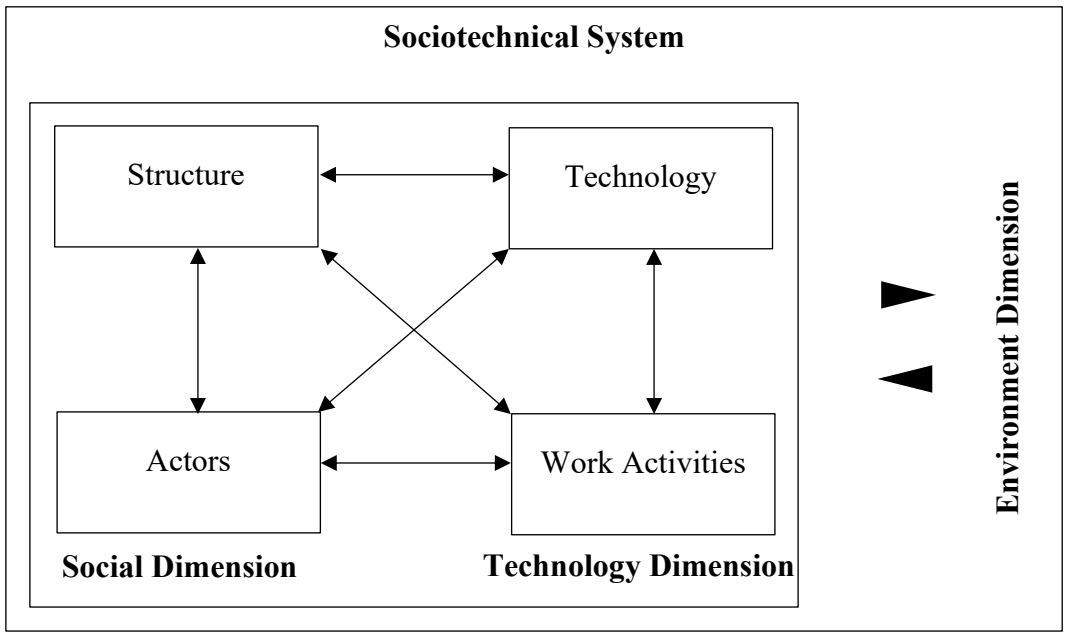

Figure 1