TU Delft

Delft University of Technology

Document Version
Final published version

Licence
Dutch Copyright Act (Article 25fa)

Citation (APA)
Shah, R. T., van Eeten, M., Pieters, W., & Parkin, S. (2026). Human and Organizational Factors in Smart Grid Cybersecurity: A Systematic Literature Review. In E. Bergström, B. Hämmerli, A. Kitkowska, & J. Kävrestad (Eds.), *International Conference on Critical Information Infrastructures Security (CRITIS 2025)* (pp. 39-57). (Lecture Notes in Computer Science; Vol. 16291). Springer. https://doi.org/10.1007/978-3-032-19540-1_3

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright
In case the licence states “Dutch Copyright Act (Article 25fa)”, this publication was made available Green Open Access via the TU Delft Institutional Repository pursuant to Dutch Copyright Act (Article 25fa, the Taverne amendment). This provision does not affect copyright ownership.
Unless copyright is transferred by contract or statute, it remains with the copyright holder.

Sharing and reuse
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.

Human and Organizational Factors in Smart Grid Cybersecurity: A Systematic Literature Review

Ronak Tejas Shah[1(✉)], Michel van Eeten[1], Wolter Pieters[2], and Simon Parkin[1]

[1] Faculty of Technology, Policy and Management, Delft University of Technology, Delft, The Netherlands
{R.T.Shah,M.J.G.vanEeten,S.E.Parkin}@tudelft.nl
[2] Behavioural Science Institute, Radboud University, Nijmegen, The Netherlands
wolter.pieters@ru.nl

Abstract. The increasing digitalization of power systems into "smart grids" has introduced complex cybersecurity challenges. Although technical solutions dominate research in this area, non-technical factors crucial to smart grid cybersecurity remain unknown. This paper presents a systematic review of 27 studies examining how human and organizational factors are addressed in the smart grid cybersecurity literature. Our analysis reveals three key limitations: (1) a disconnect between proposed solutions and real-world challenges; (2) an overemphasis on individual operator decision-making during cyber incidents, despite empirical evidence supporting collaborative approaches; and (3) the imprecise use of concepts like "cybersecurity awareness" and "security culture", neglecting established human factors literature developed around these concepts. Future research should ground interventions in real-world operational complexities, ensuring alignment between empirical and methodological approaches.

Keywords: human factors · organizational factors · smart grids · cybersecurity · systematic literature review

1 Introduction

The shift to sustainable energy transition relies on integrating renewable sources into the power grid, which requires advanced controls, real-time monitoring, and intelligent electricity management to ensure stability and reliability [3,5,61]. To support this transition, power systems are adopting digital technologies, evolving into modern digitized infrastructures, also called smart grids. While these advancements improve operational efficiency, they also introduce cybersecurity challenges, making power systems more vulnerable to cyber threats [10,17,43].

Recent cyberattacks on energy infrastructure have demonstrated the severe economic and societal consequences that these attacks can have on a national

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2026
E. Bergström et al. (Eds.): CRITIS 2025, LNCS 16291, pp. 39–57, 2026.
https://doi.org/10.1007/978-3-032-19540-1_3

level. For example, cyberattacks on power systems in Ukraine, 2015 [66], 2016 [55], and 2022 [49] which involved coordinated cyberattacks using Industroyer malware to breach critical control systems and disrupt grid operations, eventually causing severe power outages. In 2023, SektorCERT [51], Denmark's cybersecurity center for critical infrastructures, reported a major cyberattack on the energy sector, affecting at least 22 companies. In this attack, SCADA control systems were compromised with malware, leading to disruption of power system operations.

How can smart grids be protected against cyber threats? While significant advances in cybersecurity research for smart grids have been made, these efforts have primarily focused on securing the technology [2,9,12,18,23,25,35]. But the abovementioned incidents have revealed challenges that extend well beyond purely technical factors. For instance, the 2015 Ukraine attack involved spearphishing emails targeting employees of multiple grid operators, suggesting a lack of cybersecurity awareness and training as a contributing factor. Similarly, the SektorCERT 2023 report describes how the scale of the cyberattacks exceeded incident response capacities, linking this failure to shortcomings in organizational preparedness and coordination. Hence, in studying cyberattacks on modern power systems it is essential to also look at human and organizational factors. However, our understanding of human and organizational factors in the cybersecurity of smart grids remains unclear. The number of studies is limited, and they are fragmented across various academic communities. We lack a coherent view of the state of the art and of potential gaps. This hinders this critical work from advancing.

In this paper, we aim at providing such a coherent view. Our primary research question is: What is the current state of research on human and organizational factors in the cybersecurity of smart grids, and what insights can guide future studies? Synthesizing the existing academic discourse on this topic can provide a foundation for social science scholars in the energy and cybersecurity domain to engage with the fragmented research landscape, addressing the lack of a consistent understanding of human and organizational factors in smart grid cybersecurity and advancing the maturity of research in this field.

To identify relevant papers, we developed a comprehensive search query covering key concepts from (i) smart grids, (ii) cybersecurity, and (iii) human and organizational factors. Our focus was on papers at the intersection of these three areas. After filtering 2000 initial matches from Google Scholar and Scopus, we examined 76 full-text peer-reviewed papers. Only 27 papers met the criteria for inclusion in the final review, revealing a striking scarcity of research in this area and signaling a clear need for deeper academic engagement.

The findings of this review highlight three key arguments. First, there is a misalignment between empirical findings and proposed solutions, leading to many studies operating in isolated silos. Second, a lot of cybersecurity solutions are often targeted at improving system operators' decision-making in managing cyber incidents, despite empirical evidence emphasizing the need for collaborative efforts across roles. Third, terms like cybersecurity awareness and secu-

rity culture are used abstractly, without drawing on well-established conceptual understanding from broader cybersecurity literature. These findings reflect critical gaps in existing research surrounding beyond-technical aspects of cybersecurity in smart grids.

This review starts by outlining the scope of cybersecurity in smart grids and the concept of human and organizational factors. It then details the methodology used to select papers for review and concludes with a discussion based on the studies included.

2 Cybersecurity in Smart Grids

In the existing literature, digitized power systems are discussed using various terminologies. The most commonly used term is "smart grids," but terms like "cyber-physical power systems," "power grid operations," and "modern power systems" are also prevalent [12,59,67]. Although these terms differ in some nuances, they generally refer to the same concept. Hence, for this review, we will adopt the popular term "smart grids". We use a well-established definition for "smart grids" from the European context. The European Commission defines smart grids as: "An electricity network that can cost efficiently integrate the behavior and actions of all users connected to it—generators, consumers, and those that do both—in order to ensure an economically efficient, sustainable power system with low losses and high levels of quality, security of supply, and safety" [1]. This definition highlights several key objectives: economic efficiency, low losses, high levels of quality, security of supply, and safety, all aimed at optimizing the current value chain of the electricity network from generation to delivery. Digitization is meant to bring the capabilities to fulfill these objectives, transforming traditional power systems into "smart grids" [17,25].

With the advent of digitalization, cybersecurity has naturally become a critical concern. Given the relatively recent emergence of cybersecurity challenges in this domain, policy makers, industry, and the scientific community have been exploring various perspectives [3,34,42]. Among these efforts, non-technical factors have gained recent attention as essential components of cybersecurity for smart grids [34,37,43,52,53]. To provide clarity for this review, we categorize these non-technical considerations under the term "human and organizational factors", appreciating its connotation in capturing individual and organizational dimensions within the rather ambiguous scope of non-technical factors.

3 Human and Organizational Factors

Defining "human factors" in the context of cybersecurity for smart grids presents significant challenges. Even within the computer science community studying cybersecurity, the conceptualization of the term "human factors" remains underdeveloped [11]. For instance, Kaur et al. [32] conducted a systematic review of "human factors" research in cybersecurity within computer science, covering literature from 2008 to 2018. The review distinguished between humans involved

in the development and operation of technical systems, and those humans who were end-users of a technical system. This distinction not only highlights the role of humans in technical environments, but also that there can be dependencies between different groups of users (in this case, professionals) who rely on each other. It suggests that "human factors" extend beyond just individual considerations to include the interdependencies that shape their interactions.

Concepts beyond focusing on individuals, like team dynamics and organizational culture, are also loosely grouped under the umbrella of "human factors" in existing cybersecurity literature. For example, Ioannou et al. [30] studied cybersecurity culture in incident response teams, focusing on factors of communication and coordination. Steinke et al. [57] conducted research on team dynamics in situations of cybersecurity incident response. The "Cyber-Security Culture" (CSC) framework proposed by Georgiadou et al. [22] incorporates both individual factors—such as individual awareness, attitudes, and skills—and organizational factors, including organizational policies and practices, emphasizing the importance of addressing organizational and individual factors together. These studies demonstrate that addressing both human (individual) and organizational factors (collective) in combination is essential, as a strong cybersecurity posture relies on the dynamic interaction between individual and organizational elements [11].

Hence, to clarify our approach, we adopt the concept of "human factors" from the computer science community and expand it to include collective factors, such as teams and organizations, thereby framing our review under the broader term "human and organizational factors." The following section details the methodology adopted in this review.

4 Methodology

The methodology of this literature review adheres to the guidelines set forth by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework [45]. The PRISMA framework was selected for its widespread adoption in systematic literature reviews and its ability to ensure transparency, reproducibility, and methodological rigor in study selection and reporting. The strategy was to collect the relevant peer-reviewed papers, without limiting the search to a specific time range and see how far back relevant papers meeting the set criteria could be found. We used a combination of two databases: Google Scholar and Scopus. Google Scholar is known for its ability to retrieve a broad range of relevant papers [24], while Scopus offers a more curated database of peer-reviewed articles [8]. This combination of Google Scholar and Scopus ensured both relevance and reliability, while avoiding redundancy with databases such as IEEE Xplore, ACM, and Springer, which are largely indexed in Scopus. Our choice to use Scopus and Google Scholar was also informed by empirical comparisons of bibliographic databases: Scopus offers broader journal coverage and more reliable citation indexing, while Google Scholar provides greater recall across grey literature and preprints. Using both maximizes retrieval breadth without sacrificing citation traceability [36,48].

4.1 Data Collection

The scope of this review is the intersection of three areas. To represent this, we developed keywords using a snowballing technique. We began with some pertinent papers that intersected the three domains like Scholtz et al. [52], Scholtz et al. [53], Le Blanc et al. [37], then scanned their references to find additional relevant research. This iterative process led to broad concepts derived from a collection of a few relevant papers, from which specific keywords and closely related terms were identified in Table 1.

Table 1. *List of keywords and synonyms derived from three overarching concepts*

Concepts	Keywords and Synonyms
Cyber security	cyber security; cybersecurity; cyber-attack; information security
Human factors	human factors; awareness; training; exercise; team; situational awareness; sensemaking; organization; risk; resilience; behavior; coordination; communication; collaboration; incident response; crisis
Power systems	power grid; smart grid; cyber-physical power systems; power systems; TSO (Transmission System Operator); DSO (Distribution System Operator); energy; electric power industry

We developed a search query for the keywords from Table 1 that uses Boolean operators (AND, OR) in combination with wildcards (e.g., "*" and "?") to include written variations of the keywords. Special attention was given to the different ways in which similar concepts are typically expressed in scientific discourse, such as "cyber security" and "cybersecurity," or "power grids" and "power grid," to ensure thorough coverage of potential results. The search query employed in this study is:

> (("cyber secur*" OR cybersecurity OR "cyber-attack*" OR "information security") AND ("human factor*" OR awareness OR training OR exercise OR team OR "situational awareness" OR sensemak* OR organisation* OR risk OR resili* OR behavio* OR coordination OR communication OR collaboration OR "incident response" OR crisis) AND ("power grid" OR "smart grid" OR "cyber-physical power system*" OR "power system*" OR TSO OR "Transmission System Operator" OR DSO OR "Distribution System Operator" OR energy OR "electric power industry"))

4.2 Eligibility

Figure 1 outlines the step-by-step selection process for this review. The search query produced 7,430 results on Google Scholar and 6,521 on Scopus. Given the large volume of papers retrieved, the initial results were ordered by relevance, leveraging the algorithmic capabilities of both platforms [16,63]. This ensured the most pertinent studies were prioritized, and the large volume of search results was managed effectively [46]. From these ordered results, the first 1000 papers from each database were selected, totaling 2000 papers. These 2000 papers were exported as BIBTeX files to Zotero, where duplicates, books, book sections, and thesis were removed, resulting in 1,746 unique papers.

This set of papers was assessed using defined inclusion and exclusion criteria. During the title and metadata screening, papers explicitly addressing all three core concepts—human and organizational factors, cybersecurity, and smart grids—or closely related terminologies were included for further review. Inclusion criteria also required papers to be peer-reviewed, written in English, and have full-text availability, narrowing the selection to 96 papers for abstract screening. Abstract screening applied exclusion criteria to remove papers lacking meaningful discussion of the intersection of these core concepts. For example, Gajanan et al. [18]—cyberattacks in smart grids systems, a review—was initially considered in the title and metadata screening, due to its broad scope but excluded after abstract review revealed no substantive discussion of non-technical aspects or human and organizational factors. Abstract screening excluded 20 papers, reducing the selection to 76 papers for full-text review.

The full-text review further excluded papers where human or organizational factors were mentioned only superficially or in passing. For instance, Alfiah and Prastiwi [2] briefly mention human factors in their conclusion as a potential challenge but did not integrate the concept into the main argument or analysis. Ultimately, 27 papers were selected for detailed review. This systematic process ensured that the final selection fully addressed the interplay between the three core concepts, aligning with the defined scope of this review.

4.3 Limitations

Despite the systematic methodology employed in this study, several limitations must be acknowledged:

1. **Scope of databases:** While Google Scholar and Scopus were chosen for their extensive, yet different, coverage of academic literature, relying solely on these databases may have excluded relevant studies only available in other databases or grey literature sources.

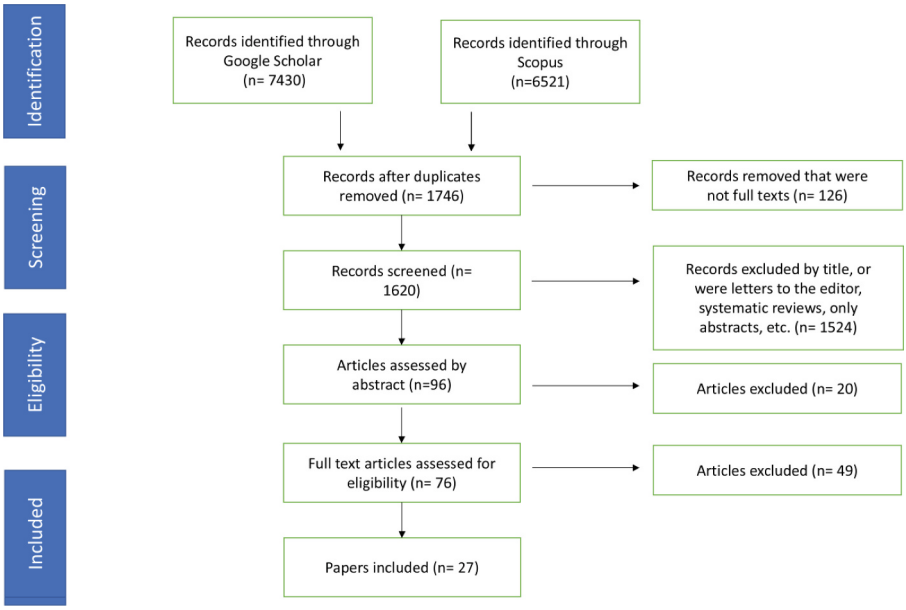


Fig. 1. Flowchart depicting the PRISMA process for study selection.

2. **Choice of only considering top results:** The search query produced over 10,000 results combined from both databases. Due to practical constraints in terms of time and resources, only the first 2000 papers filtered by relevance were selected for initial screening. Consequently, some potentially relevant studies might have been overlooked.
3. **Filtered by relevance:** On both databases, the results were filtered by relevance, which relies on the algorithms of the individual databases. While this approach theoretically increases the likelihood of retrieving a broader range of relevant papers, there is no transparency on how the "filtered by relevance" function works exactly for each database.
4. **Screening and selection process:** The initial screening process involved title and abstract reviews, which might have resulted in the exclusion of relevant studies that did not explicitly mention key terms in their titles or abstracts. Full-text reviews were only conducted on a subset of papers.
5. **Geographical and cultural bias:** The study may have a bias towards research conducted in Western and other countries that publish scientific research predominantly in English. This could result in an underrepresentation of perspectives and findings from non-Western regions—a challenge commonly observed in usable security research [26].
6. **Manual processes:** The process of manually selecting and screening papers introduces the possibility of human error and subjectivity. While efforts were made to standardize the selection criteria, inconsistencies may still arise.

The systematic methodology employed in this review ensured a thorough and structured approach to identifying the most relevant papers across all three domains. While acknowledging inherent limitations, this study aims to provide a comprehensive overview, contributing to this evolving field and guiding future research. The next section delves into synthesizing the findings from the reviewed literature.

5 Synthesizing the Existing Literature

The synthesis of the 27 reviewed papers was structured around eight criteria: (1) whether the paper has an empirical or methodological focus; (2) if it was an empirical paper, what population was studied; (3) what problem is being addressed or explored; (4) the research objective; (5) which theories or frameworks were adopted; (6) which human factors are identified; (7) which organizational factors are identified; and (8) which interventions are proposed. The findings are summarized in Table 2.

5.1 Empirical Versus Methodological Focus

Table 2 highlights an almost equal division between empirical (13 out of 27) and methodological (14 out of 27) studies, each pursuing distinct research objectives. Among the 13 empirical papers, 10 studies the population of practitioners—individuals actively working within power system organizations—while two studies subject matter experts. An exception is Krkoleva Mateska et al. [34], which examines how organizations implement cybersecurity compliance, specifically focusing on transmission system operators (TSOs) in Southeast Europe. Most empirical studies (9 out of 13) utilize qualitative methods, such as interviews and exercise observations, with a common research objective of exploring cybersecurity challenges within smart grids. The remaining four empirical studies employ quantitative methods to validate specific factors like cybersecurity awareness, workforce competency [20,21,28], and cybersecurity compliance [34]. The research objective of validation in this case involves evaluating how cybersecurity-related factors are operationalized within power system organizations [21].

Methodological studies primarily center on providing solutions as their main research objective, with a few notable exceptions. Chowdhury & Gkioulos [13] conducted a systematic literature review to explore optimal cybersecurity training methods for critical infrastructure, including the energy sector. Wallis & Leszczyna [65] applied a cybersecurity applicability framework [38] to validate the practical adaptability of the European Energy Information Sharing and Analysis Center (EE-ISAC) [39]. Some methodological studies incorporate stakeholder engagement to improve the practical relevance of their solutions. For example, Teufel & Teufel [60] consulted experts to develop information security guidelines, and Boroomand et al. [7] for designing automation strategies. However, in both cases, the studies argue for a solution—training in one, automation

Table 2. Dissecting the findings from the literature (Part 1). Column 3: E = Empirical, M = Methodological

Year	Ref.	Type	Population Studied	Problem Being Addressed	Research Objective	Theory/Framework Adopted	Human Factors	Organizational Factors	Proposed Intervention
2024	[19]	E	Practitioners	Risk assessment	Exploratory	N/A	Interdisciplinary knowledge	Common understanding	Collaboration across domains
2024	[47]	M	Experts	Capability development	Solution	Design science methodology	Individual skills	N/A	Curriculum design
2024	[62]	M	N/A	Risk assessment	Solution	Network theory	Decision making	N/A	Modeling human actions
2023	[20]	E	Practitioners	Capability development	Validation	Cyber-Security Culture (CSC)	Cybersecurity awareness	Workforce competency	Improving security culture
2023	[14]	M	N/A	Information management	Solution	N/A	Decision making	N/A	Improving visualization for operators
2023	[43]	E	Experts	Risk assessment	Exploratory	Sociotechnical Imaginaries	Perspective	N/A	Vision driven by technical considerations
2022	[21]	E	Practitioners	Capability development	Validation	N/A	Cybersecurity awareness	Workforce competency	Improving security culture
2022	[42]	E	Practitioners	Capability development	Exploratory	N/A	Perspective	N/A	Non-aligned practitioner and academic perspectives
2022	[65]	M	N/A	Capability development	Validation	Cybersecurity applicability	N/A	N/A	Applicability of European Energy ISAC
2022	[41]	M	N/A	Information management	Solution	N/A	Decision making	N/A	Improving visualization for operators
2021	[34]	E	Organizations	Capability development	Exploratory	N/A	N/A	Compliance	Ensuring inter-organizational compliance
2021	[13]	M	N/A	Capability development	Exploratory	N/A	N/A	Training	No optimum training method
2021	[54]	E	Experts	Capability development	Exploratory	N/A	Individual skills	N/A	Curriculum design
2020	[56]	M	N/A	Risk assessment	Solution	Design Thinking	Decision making	N/A	Threat prioritization
2020	[58]	M	N/A	Risk assessment	Solution	CIRA Method	Decision making	N/A	SGAM-H with human layer
2019	[39]	M	N/A	Information management	Solution	N/A	N/A	Common understanding	European Energy ISAC
2018	[53]	M	Practitioners	Information management	Solution	UCD framework, Situational Awareness	Role specific information	Common understanding	Tool for improving collective SA
2017	[37]	E	Practitioners	Incident response	Exploratory	N/A	Role specific information	Common understanding	Collaboration across domains

(*continued*)

Table 2. (*continued*)

Year	Ref.	Type	Population Studied	Problem Being Addressed	Research Objective	Theory/Framework Adopted	Human Factors	Organizational Factors	Proposed Intervention
2016	[6]	E	Practitioners	Incident response	Exploratory	N/A	Perspective	Training	Collaboration across domains
2016	[31]	E	Practitioners	Incident response	Exploratory	N/A	Interdisciplinary knowledge	Common understanding	Collaboration across domains
2016	[52]	E	Practitioners	Incident response	Exploratory	N/A	Perspective	Common understanding	Collaboration across domains
2015	[60]	M	Experts	Risk assessment	Solution	OECD Standards	Cybersecurity awareness	N/A	Information security guidelines (CEIS)
2014	[40]	E	Practitioners	Incident response	Exploratory	N/A	Perspective	Training	Collaboration across domains
2014	[50]	M	N/A	Risk assessment	Solution	Routine Activities, Rational Choice	Decision making	N/A	PARE RISKS framework
2013	[4]	M	N/A	Risk assessment	Solution	Game theory	Decision making	N/A	Modeling attacker-operator interaction
2013	[28]	E	Practitioners	Capability development	Validation	N/A	Cybersecurity awareness	Workforce competency	Improving security culture
2010	[7]	M	Experts	Risk assessment	Solution	Human-Automation Interaction	Decision making	N/A	Human-automation framework

in the other—implicitly assuming what the problem is, without deriving it from practice.

With the exception of two studies that incorporate elements of real-world context, most methodological studies rely purely on assumptions to design interventions, overlooking the complexities that become visible when studying how problems are understood and experienced in actual practice. Gallardo et al. [19], for instance, surfaced needs expressed by OT practitioners—such as "make existing OT systems more usable"—emphasizing improvements to current systems rather than introducing completely new solutions. If such practitioner-informed concerns were considered, they could meaningfully shape the problem framings underlying methodological efforts. Hence, comparing the problems explored and addressed by empirical and methodological studies would provide insight into how the complexities of reality are represented in the literature and reveal the assumptions that shape methodological proposals. The next section examines this further by analyzing the alignment—or lack thereof—between the problems empirical and methodological approaches explore and address.

5.2 The Problems Explored Versus the Problems Addressed

When analyzing all the papers collectively, clear problem-focused themes begin to emerge, with empirical and methodological studies diverging in their areas of emphasis. Column 5 in Table 2 outlines these problem-focused themes. Risk assessment of cyber threats and capability development for incident response are central themes shared across both domains. Methodological studies predominantly focus on risk assessment, with half of them—Umunnakwe et al. [62], Snow et al. [56], Szekeres & Snekkenes [58], Rege [50], Backhaus et al. [4], Teufel & Teufel [60], and Boroomand et al. [7]—proposing frameworks to better assess cybersecurity risks in smart grids. These solutions, however, show minimal alignment with empirical studies, which focus on understanding the nature and scope of cybersecurity risks from real-world perspectives. For example, Gallardo et al. [19] analyzes how different disciplines, such as energy operations and information technology, approach cybersecurity as a risk to smart grids, based on interviews with energy operations teams and cybersecurity analysts, while Michalec et al. [43] captures expert perspectives on emerging cybersecurity risks and their potential evolution. Hence, empirical studies focus on contextual understanding by drawing insights from practitioners and experts, whereas methodological studies prioritize advancing risk assessment models grounded in technical frameworks, with human factors incorporated as an additional layer.

This misalignment is also evident in studies addressing capability development for incident response. Empirical studies, based on insights from practitioners and experts, identify key challenges such as cybersecurity skill gaps in the smart grid domain [54], overestimation of organizational capacities to manage cyber incidents [34,42], workforce incompetency in managing cyber incidents [20,21,28], lack of standardised training schedules [6,40], unclear documentation [40], and divergent practitioner views on cybersecurity in smart grids [6,40,42]. In contrast, methodological studies do not pick-up on this identified challenges,

and have discussed solutions like the European Energy Information Sharing and Analysis Center (EE-ISAC) to enable information sharing across organizations [39,65], or, explore optimum training method for cybersecurity training in critical infrastructure [13].

The divide between empirical and methodological studies extends beyond the problems they address to justify the interventions they propose, as they often aim to achieve different objectives. Typically, methodological studies focus on tools designed specifically for system operators [7,14,41], arguing that enhancing their capabilities will improve overall cyber incident response. However, a key underlying assumption of these solutions is that system operators bear the major responsibility for managing cyber incidents [7,14,41]. This assumption is not fully supported by empirical findings, which instead emphasize that incident response is largely a collaborative effort involving multiple actors who interact, communicate, and collectively make sense of situations to devise appropriate responses [6,31,37,40,52,53]. Therefore, while interventions like improved operator visualizations may contribute to these collaborative efforts, it remains unclear (1) what roles and responsibilities operators actually hold and are expected to hold during cyber incidents and (2) how operators themselves would perceive these additional capabilities. Empowering operators with additional tools and technologies without understanding their perspectives could be counterintuitive, and potentially overload an already cognitively demanding task [44,64].

In summary, two key insights emerge when comparing empirical and methodological studies through the lens of the problems they address. First, a consistent misalignment exists between the challenges investigated in empirical studies and the interventions designed in methodological studies. This disconnect can be attributed to differing disciplinary incentives: methodological studies, frequently published in computer science or power engineering venues, prioritize artifact/tool design, while empirical studies, often found in other disciplines, focus on understanding real-world problems. Second, methodological studies exhibit a strong tendency to focus solutions on system operators, despite limited empirical evidence clearly defining their roles or responsibilities in managing cyber incidents. In Klein's work on decision-making [33], for instance, importance is given to the need for 'common ground' between professionals who have to coordinate; this includes how they collectively resolve ambiguous situations, but also address ambiguities between team members to reach a common understanding, and help each other in order to perform better as a team. This includes not only when each team member uses their own provisioned tools, but also how they coordinate meaningfully with each other when incidents arise.

The next section shifts focus from the problems these studies address to how they address them. It discusses the specific factors emphasized in empirical versus methodological studies and analyzes the proposed interventions to reflect on their broader implications and potential future research directions.

5.3 Human and Organizational Factors and Interventions

This review identifies ten factors—six human and four organizational—detailed in columns 8 and 9 of Table 2, along with corresponding interventions in column 10. This section analyzes how the literature consider these factors, comparing empirical findings with methodological approaches to demonstrate alignment or gaps.

A prominent organizational factor discussed in the literature is the need for establishing a common understanding of cybersecurity. Empirical studies highlight cross-departmental collaboration as the intervention to achieve common understanding, also emphasizing human factors such as interdisciplinary knowledge exchange, divergent practitioner perspectives, and role-specific information [19,31,37,52]. This collaboration is also pointed as an intervention in empirical studies addressing the organizational factor of training, to improve the outcomes of training exercises [6,40,42]. In contrast, methodological studies accounting for organizational factor of establishing common understanding and training prioritize inter-organizational information sharing [39,65], and finding an optimum medium of training [13]. An exception is Scholtz et al. [53], who design role-specific tools to improve intra-organizational collaboration by achieving common understanding of incidents, based on prior empirical work [52]. A second exception aligning empirical and methodological approaches is the work by Siemers et al. [54] and Pirta-Dreimane et al. [47], who address the human factor of individual skills and propose a curriculum design framework to address the cybersecurity skill gap in the smart grid industry.

Cybersecurity awareness and workforce competency are also addressed as a blend of human and organizational factors, specifically in the empirical papers [20,21,28]. However, these studies often lack engagement with established literature on concepts such as cybersecurity awareness—defined as an individual's understanding of cyber risks and their ability to act securely; security culture—the shared values, norms, and practices within an organization that shape security-related behavior; and human-centered cybersecurity—an approach that emphasizes practitioners' lived experiences, needs, and constraints in socio-technical environments [15,29,30,68]. This inconsistent use of terminology is not limited to empirical studies; methodological studies, such as Teufel & Teufel's [60] proposed guidelines for distributed grids, also exhibit ambiguity in interpreting cybersecurity awareness.

Such challenges are again not isolated to the smart grid domain, where sectors including energy and beyond define "security awareness" in different ways, but also have regulations which under-specify what security awareness (and in turn, "security culture") should include, thereby leaving practitioners – and their vendors – to decide this [27]. This extends to whether there is support for users who are not able to follow the training and thereby work securely, which would be key in critical domains such as energy provision. However, with the focus in the energy sector on incident response, there may be opportunities to hook user support into existing sectoral approaches. Further, assurance measures may be gathered, and woven into incident-planning procedures (e.g., logging user diffi-

culties and addressing them, which is generally not a regular part of security awareness management).

Methodological studies further emphasize decision-making as a prominent human factor, addressing it from both defender and attacker perspectives. For defenders, proposed solutions focus on technical tools, such as improved visualizations, game-theoretic models, and automated detection processes [4,7,14,41,58]. From the attacker's perspective, frameworks are developed to evaluate attack severity based on assumptions about attacker behavior [50,56,62]. This dominant focus on decision-making in methodological studies is entirely absent in empirical studies, further raising questions about the applicability of these interventions.

To summarize, the analysis of factors and proposed interventions reveals a consistent disconnect between the focus of empirical research and methodological approaches. Empirical studies address the factor of common understanding within the scope of an organization, while methodological studies focus on solutions that ensure inter-organizational information sharing to achieve common understanding. Additionally, decision-making emerges as a dominant human factor in methodological studies but is entirely absent in empirical studies. Another observation from this analysis of factors is that many empirical studies fail to engage with established literature on well-discussed human factors concepts like security culture and cybersecurity awareness, resulting in ambiguous interpretations across studies.

6 Conclusion and Future Research Directions

This systematic literature review analyzed the state-of-the-art on human and organizational factors in addressing cybersecurity challenges within smart grids. Examining 27 studies, we identified three key limitations in the current literature: (1) a significant disconnect between proposed solutions and the real-world cybersecurity complexities; (2) an overemphasis on system operators' decision-making in methodological studies, without a corresponding empirical understanding of their actual roles and responsibilities during cyber incidents; and (3) the imprecise and inconsistent use of concepts such as "cybersecurity awareness" and "security culture," without grounding them in the established literature surrounding these topics. While a substantial body of research exists on human and or organizational factors in cybersecurity of computer science domain, this review reveals a critical gap in its application within the smart grid context.

To improve the contribution of non-technical academic research to smart grid cybersecurity, future research should improve the alignment between real-world challenges highlighted by empirical studies and the proposed solutions. This integration requires methodological studies to be informed by the operational realities of smart grid environments, while empirical investigations should focus on addressing specific gaps in current practice to inform the design and assumptions of proposed methodologies. This integrated and collaborative approach will facilitate the development of targeted, actionable solutions, ultimately strengthening the resilience of smart grids.

Funding Acknowledgment. We wish to thank our participants for their contributions to the study. This work has been partially supported by the RESCUE project (Grant No. ESI.2019.006), funded by the Netherlands Organization for Scientific Research (NWO).

References

1. Commission staff working document: Definition, expected services, functionalities and benefits of smart grids. European Commission staff working document, European Commission, Brussels (2011)
2. Alfiah, F., Prastiwi, N.R.: Cyber security in smart grid technology: a systematic review. Int. J. Cyber IT Serv. Manage. **2**(1), 48–54 (2022). https://doi.org/10.34306/ijcitsm.v2i1.79
3. Alvarez-Alvarado, M., et al.: Cyber-physical power systems: a comprehensive review about technologies drivers, standards, and future perspectives. Comput. Electr. Eng. **116** (2024). https://doi.org/10.1016/j.compeleceng.2024.109149
4. Backhaus, S., et al.: Cyber-physical security: a game theory model of humans interacting over control systems. IEEE Trans. Smart Grid **4**(4), 2320–2327 (2013)
5. Badal, F., Sarker, S., Nayem, Z., Moyeen, S., Das, S.: Microgrid to smart grid's evolution: technical challenges, current solutions, and future scopes. Energy Sci. Eng. **11**(2), 874–928 (2023). https://doi.org/10.1002/ese3.1319
6. Bartnes, M., Moe, N.B., Heegaard, P.E.: The future of information security incident management training: a case study of electrical power companies. Comput. Secur. **61**, 32–45 (2016)
7. Boroomand, F., et al.: Cyber security for smart grid: a human-automation interaction framework. In: IEEE PES Innovative Smart Grid, pp. 1–6. IEEE (2010)
8. Burnham, J.F.: Scopus database: a review. Biomed. Digit. Libr. **3**(1), 1 (2006). https://doi.org/10.1186/1742-5581-3-1
9. Cai, J., Zheng, Y., Zhou, Z.: Review of cyber-security challenges and measures in smart substation. In: 2016 International Conference on Smart Grid and Clean Energy Technologies, ICSGCE 2016, pp. 65–69. Institute of Electrical and Electronics Engineers Inc. (2017). https://doi.org/10.1109/ICSGCE.2016.7876027
10. Cassotta, S., Sidortsov, R.: Sustainable cybersecurity? Rethinking approaches to protecting energy infrastructure in the European High North. Energy Res. Soc. Sci. **51**, 129–133 (2019). https://doi.org/10.1016/j.erss.2019.01.003
11. Ceesay, E., Myers, K., Watters, P.: Human-centered strategies for cyber-physical systems security. ICST Trans. Secur. Safety **4**(14), 154773 (2018). https://doi.org/10.4108/eai.15-5-2018.154773
12. Chatterjee, K., Padmini, V., Khaparde, S.: Review of cyber attacks on power system operations. In: 2017 IEEE Region 10 Symposium (TENSYMP), pp. 1–6 (2017). https://doi.org/10.1109/tenconspring.2017.8070085
13. Chowdhury, N., Gkioulos, V.: Cyber security training for critical infrastructure protection: a literature review. Comput. Sci. Rev. **40**, 100361 (2021). https://doi.org/10.1016/j.cosrev.2021.100361
14. Cobilean, V., et al.: A review of visualization methods for cyber-physical security: smart grid case study. IEEE Access **11**, 59788–59803 (2023). https://doi.org/10.1109/ACCESS.2023.3286304

15. de Bruijn, H., Janssen, M.: Building Cybersecurity Awareness: the need for evidence-based framing strategies. Gov. Inf. Q. **34**(1), 1–7 (2017). https://doi.org/10.1016/j.giq.2017.02.007
16. Elsevier Support Center: What content is included in scopus? (2025). https://service.elsevier.com/app/answers/detail/a_id/14182/supporthub/scopus/. Accessed 9 July 2025
17. Farhan, M., et al.: Towards next generation Internet of Energy system: framework and trends. Energy AI **14** (2023). https://doi.org/10.1016/j.egyai.2023.100306
18. Gajanan, L., Kirar, M., Raju, M.: Cyber-attacks on smart grid system: a review. In: 2022 IEEE 10th Power India International Conference, PIICON 2022. Institute of Electrical and Electronics Engineers Inc. (2022). https://doi.org/10.1109/PIICON56320.2022.10045208
19. Gallardo, A., Erbes, R., Le Blanc, K., Bauer, L., Cranor, L.F.: Interdisciplinary approaches to cybervulnerability impact assessment for energy critical infrastructure. In: Proceedings of the CHI Conference on Human Factors in Computing Systems, Honolulu HI USA, pp. 1–24. ACM (2024). https://doi.org/10.1145/3613904.3642493
20. Georgiadou, A., Michalitsi - Psarrou, A., Askounis, D.: A security awareness and competency evaluation in the energy sector. Comput. Secur. **129** (2023). https://doi.org/10.1016/j.cose.2023.103199
21. Georgiadou, A., Michalitsi-Psarrou, A., Askounis, D.: Evaluating the cyber-security culture of the EPES sector: applying a cyber-security culture framework to assess the EPES sector's resilience and readiness. In: ACM International Conference Proceeding Series. Association for Computing Machinery (2022). https://doi.org/10.1145/3538969.3543813
22. Georgiadou, A., Mouzakitis, S., Bounas, K., Askounis, D.: A cyber-security culture framework for assessing organization readiness. J. Comput. Inf. Syst. **62**(3), 452–462 (2022). https://doi.org/10.1080/08874417.2020.1845583
23. Ghiasi, M., Niknam, T., Wang, Z., Mehrandezh, M., Dehghani, M., Ghadimi, N.: A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: past, present and future. Electric Power Syst. Res. **215** (2023). https://doi.org/10.1016/j.epsr.2022.108975
24. Haddaway, N.R., Collins, A.M., Coughlin, D., Kirk, S.: The role of google scholar in evidence reviews and its applicability to grey literature searching. PLoS ONE **10**(9), e0138237 (2015). https://doi.org/10.1371/journal.pone.0138237
25. Hasan, M.K., Habib, A.A., Shukur, Z., Ibrahim, F., Islam, S., Razzaque, M.A.: Review on cyber-physical and cyber-security system in smart grid: standards, protocols, constraints, and recommendations. J. Netw. Comput. Appl. **209**, 103540 (2023). https://doi.org/10.1016/j.jnca.2022.103540
26. Hasegawa, A.A., Inoue, D., Akiyama, M.: How WEIRD is usable privacy and security research? In: 33rd USENIX Security Symposium (USENIX Security 2024), pp. 3241–3258 (2024)
27. Hielscher, J., Parkin, S.: "What keeps people secure is that they met the security team": deconstructing drivers and goals of organizational security awareness. In: 33rd USENIX Security Symposium (USENIX Security 2024), pp. 3295–3312 (2024)
28. Holm, H., Flores, W.R., Ericsson, G.: Cyber security for a Smart Grid - What about phishing? In: IEEE PES ISGT Europe 2013, pp. 1–5 (2013). https://doi.org/10.1109/ISGTEurope.2013.6695407
29. Hossain, M.N., Hassan, M.M., Monir, R.J., Sayeed, M.S., Wajiha, S., Ullah, S.W.: Cyber security and people: human nature, psychology, and training affect user

awareness, social engineering, and security professional education and preparedness. In: 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), pp. 1–5. IEEE (2023)
30. Ioannou, M., Stavrou, E., Bada, M.: Cybersecurity Culture in Computer Security Incident Response Teams: investigating difficulties in communication and coordination. In: 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), pp. 1–4 (2019). https://doi.org/10.1109/CyberSecPODS.2019.8885240
31. Jaatun, M.G., Bartnes, M., Tøndel, I.A.: Zebras and lions: better incident handling through improved cooperation. In: Fahrnberger, G., Eichler, G., Erfurth, C. (eds.) I4CS 2016. CCIS, vol. 648, pp. 129–139. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-49466-1_9
32. Kaur, M., Eeten, M., Janssen, M., Borgolte, K., Fiebig, T.: Human factors in security research: lessons learned from 2008-2018. ACM SIGCAS Computers and Society (2021)
33. Klein, G.A.: Streetlights and Shadows: Searching for the Keys to Adaptive Decision Making. MIT Press (2011)
34. Krkoleva Mateska, A., Krstevski, P., Borozan, S.: Overview and improvement of procedures and practices of electricity transmission system operators in South East Europe to mitigate cybersecurity threats. Systems **9**(2), 39 (2021). https://doi.org/10.3390/systems9020039
35. Kumar, V., Prasad, J., Samikannu, R.: A critical review of cyber security and cyber terrorism - threats to critical infrastructure in the energy sector. Int. J. Crit. Infrastruct. **14**(2), 101–119 (2018). https://doi.org/10.1504/IJCIS.2018.091932
36. Lasda Bergman, E.M.: Finding citations to social work literature: the relative benefits of using web of science, scopus, or google scholar. J. Acad. Librariansh. **38**(6), 370–379 (2012). https://doi.org/10.1016/j.acalib.2012.08.002
37. Le Blanc, K., Ashok, A., Franklin, L., Scholtz, J., Andersen, E., Cassiadoro, M.: Characterizing cyber tools for monitoring power grid systems: what information is available and who needs it? In: 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 3451–3456 (2017). https://doi.org/10.1109/SMC.2017.8123164
38. Leszczyna, R.: Aiming at methods' wider adoption: applicability determinants and metrics. Comput. Sci. Rev. **40**, 100387 (2021). https://doi.org/10.1016/j.cosrev.2021.100387
39. Leszczyna, R., Wallis, T., Wróbel, M.R.: Developing novel solutions to realise the European Energy – Information Sharing & Analysis Centre. Decis. Support Syst. **122**, 113067 (2019). https://doi.org/10.1016/j.dss.2019.05.007
40. Line, M.B., Tøndel, I.A., Jaatun, M.G.: Information security incident management: planning for failure. In: 2014 Eighth International Conference on IT Security Incident Management & IT Forensics, pp. 47–61 (2014). https://doi.org/10.1109/IMF.2014.10
41. Mawle, P.P., Dhomane, G., Narukullapati, B.K., Venkatesh, P., Chakravarthi, M.K., Kumar Shukla, S.: A novel framework for data visualization via power system monitoring control and protection based on wireless communication. In: 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp. 1056–1060 (2022). https://doi.org/10.1109/ICACITE53722.2022.9823492
42. Meyer, J., Apruzzese, G.: Cybersecurity in the smart grid: practitioners' perspective. In: Industrial Control Systems Security Workshop (ICSS). arXiv (2022). https://doi.org/10.48550/arXiv.2210.13119

43. Michalec, O., Shreeve, B., Rashid, A.: Who will keep the lights on? Expertise and inclusion in cyber security visions of future energy systems. Energy Res. Soc. Sci. **106**, 103327 (2023). https://doi.org/10.1016/j.erss.2023.103327
44. Obradovich, J.H.: Understanding cognitive and collaborative work: observations in an electric transmission operations control center. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 55, no. 1, pp. 247–251 (2011). https://doi.org/10.1177/1071181311551051
45. Page, M.J., et al.: PRISMA 2020 explanation and elaboration: Updated guidance and exemplars for reporting systematic reviews. BMJ p. n160 (2021). https://doi.org/10.1136/bmj.n160
46. Petersen, H., Poon, J., Poon, S.K., Loy, C.: Increased workload for systematic review literature searches of diagnostic tests compared with treatments: challenges and opportunities. JMIR Med. Inform. **2**(1), e11 (2014). https://doi.org/10.2196/medinform.3037. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4288066/
47. Pirta-Dreimane, R., et al.: Enhancing smart grid resilience: an educational approach to smart grid cybersecurity skill gap mitigation. Energies **17**(8), 1876 (2024)
48. Pranckutė, R.: Web of science (WOS) and Scopus: the titans of bibliographic information in today's academic world. Publications **9**(1), 12 (2021). https://doi.org/10.3390/publications9010012. https://www.mdpi.com/2304-6775/9/1/12
49. Rattray, G., Brown, G.: The cyber defense assistance imperative: Lessons from Ukraine. Casestudy, The Aspen Institute (2023)
50. Rege, A.: A criminological perspective on power grid cyber attacks: using routine activities theory to rational choice perspective to explore adversarial decision-making. J. Homel. Secur. Emerg. Manage. **11**(4), 463–487 (2014)
51. Ribeiro, A.: SektorCERT reports cyber attack against Danish critical infrastructure, raises concerns of state involvement (2023)
52. Scholtz, J., Franklin, L., Le Blanc, K., Andersen, E.: Cybersecurity awareness in the power grid. In: Nicholson, D. (ed.) Advances in Human Factors in Cybersecurity. AISC, pp. 183–193. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-41932-9_15
53. Scholtz, J.C., et al.: Employing a user-centered design process for cybersecurity awareness in the power grid. J. Hum. Perform. Extreme Environ. **14**(1) (2018). https://doi.org/10.7771/2327-2937.1094
54. Siemers, B., et al.: Modern trends and skill gaps of cyber security in smart grid. In: IEEE EUROCON 2021 - 19th International Conference on Smart Technologies, pp. 565–570 (2021). https://doi.org/10.1109/EUROCON52738.2021.9535632
55. Slowik, J.: CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack. Forensics, Dragos Inc, USA (2019)
56. Snow, S., Happa, J., Horrocks, N., Glencross, M.: Using design thinking to understand cyber attack surfaces of future smart grids. Front. Energy Res. **8**, 591999 (2020). https://doi.org/10.3389/fenrg.2020.591999
57. Steinke, J., et al.: Improving cybersecurity incident response team effectiveness using teams-based research. IEEE Secur. Priv. **13**(4), 20–29 (2015). https://doi.org/10.1109/MSP.2015.71
58. Szekeres, A., Snekkenes, E.: Representing decision-makers in SGAM-H: the smart grid architecture model extended with the human layer. In: Eades III, H., Gadyatskaya, O. (eds.) GraMSec 2020. LNCS, vol. 12419, pp. 87–110. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-62230-5_5
59. Tatipatri, N., Arun, S.: A comprehensive review on cyber-attacks in power systems: impact analysis, detection, and cyber security. IEEE Access **12**, 18147–18167 (2024). https://doi.org/10.1109/ACCESS.2024.3361039

60. Teufel, S., Teufel, B.: Crowd energy information security culture - security guidelines for smart environments. In: 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity), Chengdu, China, pp. 123–128. IEEE (2015). https://doi.org/10.1109/SmartCity.2015.58
61. Trahan, R.T., Hess, D.J.: Who controls electricity transitions? Digitization, decarbonization, and local power organizations. Energy Res. Soc. Sci. **80**, 102219 (2021). https://doi.org/10.1016/j.erss.2021.102219
62. Umunnakwe, A., Sun, S., Davis, K.: Toward proactive cyber-physical-human risk assessment in power systems. In: 2024 IEEE Texas Power and Energy Conference (TPEC), pp. 1–6 (2024). https://doi.org/10.1109/TPEC60005.2024.10472174
63. Utrecht University Library: What does relevance ranking mean on Google Scholar? (2023). https://libguides.library.uu.nl/googlescholar_en/find-out-more. Accessed 09 July 2025
64. von Meier, A.: Occupational cultures as a challenge to technological innovation. IEEE Trans. Eng. Manage. **46**(1), 101–114 (1999). https://doi.org/10.1109/17.740041
65. Wallis, T., Leszczyna, R.: EE-ISAC–practical cybersecurity solution for the energy sector. Energies **15**(6), 2170 (2022). https://doi.org/10.3390/en15062170
66. Whitehead, D.E., Owens, K., Gammel, D., Smith, J.: Ukraine cyber-induced power outage: analysis and practical mitigation strategies. In: Conference for Protective Relay Engineers, pp. 1–8 (2017). https://doi.org/10.1109/cpre.2017.8090056
67. Yohanandhan, R.V., Elavarasan, R.M., Manoharan, P., Mihet-Popa, L.: Cyber-Physical Power System (CPPS): a review on modeling, simulation, and analysis with cyber security applications. IEEE Access **8**, 151019–151064 (2020). https://doi.org/10.1109/ACCESS.2020.3016826
68. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł, Cetin, F., Basim, H.N.: Cyber security awareness, knowledge and behavior: a comparative study. J. Comput. Inf. Syst. **62**(1), 82–97 (2022). https://doi.org/10.1080/08874417.2020.1712269