Bahaa Eltahawy

An Integration of Cyberprivacy, Cybersecurity, and Smart Grid Strategies for Protecting Critical Infrastructure

ACTA WASAENSIA 569

University of Vaasa
VAASAN YLIOPISTO

ISBN 978-952-395-226-3 (print)
978-952-395-227-0 (online)

ISSN 0355-2667 (Acta Wasaensia 569, print)
2323-9123 (Acta Wasaensia 569, online)

URN https://urn.fi/URN:ISBN:978-952-395-227-0

PunaMusta Oy, Joensuu, 2025.

ACADEMIC DISSERTATION

To be presented, with the permission of the Board of the School of Technology and Innovations of the University of Vaasa, for public examination on the 26th of November, 2025, at noon.

Article based dissertation, School of Technology and Innovations, Computer Science.

Author	Bahaa Eltahawy https://orcid.org/0000-0001-6372-7547
Supervisors	Prof. Tero Vartiainen University of Vaasa. School of Technology and Innovations, Information Systems Science.
	Adj. Prof. Heidi Kuusniemi University of Vaasa. School of Technology and Innovations, Computer Science.
	University Lecturer Dr. Timo Mantere University of Vaasa. School of Technology and Innovations, Automation Technology..
Custos	Prof. Tero Vartiainen University of Vaasa. School of Technology and Innovations, Information Systems Science.
Reviewers	Prof. Pedro Nardelli Lappeenranta University of Technology. School of Energy Systems, Electrical Engineering.
	Simone Soderi, Dr.Sc. (Tech) Asst. Prof., IMT School for Advanced Studies Lucca. Adj. Prof., University of Oulu and University of Padova.
Opponent	Prof. Seppo Virtanen University of Turku. Faculty of Technology, Department of Computing.

Tiivistelmä

Tämä väitöskirja tarkastelee kriittisen infrastruktuurin suojelun kasvavaa tarvetta digitaalisen transformaation kiihtyessä. Teknologian kehitys on parantanut tehokkuutta ja verkkoyhteyksiä, mutta samalla lisännyt kyberriskejä ja yksityisyyshaasteita. Energiajärjestelmä, joka on olennainen osa kriittistä infrastruktuuria, on erityisen haavoittuvainen, sillä älyverkot ja sähköistäminen altistavat arkaluonteisia, operatiivisia ja henkilökohtaisia tietoja kehittyneille kyberuhille.

Vaikka kyberturvallisuutta, tietosuojaa ja älyverkon suojelua on tutkittu laajasti, niitä käsitellään usein erillisinä osa-alueina, mikä heikentää niihin liittyvien ratkaisujen tehokkuutta. Vastauksena tähän haasteeseen tämä väitöskirja kehittää integroidun viitekehyksen, joka yhdistää kunkin alan mallit, standardit ja strategiat. Lähestymistapa sovittaa yhteen tietoturvatoimenpiteet, tietosuojanormit ja älyverkon toimintavaatimukset, parantaen verkoston suojatasoa.

Tämä tutkimus hyödyntää mixed method -lähestymistapaa ja kritisoi perinteisiä kriittisen infrastruktuurin suojelumalleja, jotka keskittyvät resilienssiin ja ennaltaehkäisyyn, mutta eivät huomioi sosio-teknisiä dynamiikkoja ja kasvavia riippuvuuksia. Ehdotettu viitekehys laajentaa mallit seitsemään osa-alueeseen: hallinto, riskianalyysi, sosio-tekniset tekijät, järjestelmien vuorovaikutus, kybertietosuoja, suojelujärjestelmät ja arviointimittarit. Tämä laajempi näkökulma tarjoaa kattavamman perustan riskien ymmärtämiselle ja kokonaisvaltaisille suojelustrategioille.

Viitekehyksen kehittämisen lisäksi väitöskirja tunnistaa systeemisiä ja teknisiä puutteita, tarjoaa näkemyksiä energiajärjestelmistä ja antaa suosituksia standardeista, direktiiveistä ja koulutustyökaluista kriittisen infrastruktuurin suojelun tukemiseksi.

Asiasanat: kyberturvallisuus, kybersuoja, kriittinen infrastruktuuri, älyverkko.

Abstract

This dissertation addresses the need for robust critical infrastructure protection given the current drastic societal changes and rapid digital transformation. Advances in computation, communication, and data processing have brought unprecedented efficiency and connectivity. Yet, they have also introduced new cyber risks and privacy challenges across organizational, societal, and economic domains. The energy system – as a core component of critical infrastructure and a foundation for other essential services – exemplifies these dynamics. Smart grids and electrification initiatives expose sensitive operational and personal data to sophisticated cyber threats and privacy risks.

Despite extensive research in cybersecurity, cyberprivacy, and smart-grid protection, these areas are still largely treated as distinct domains, which limits their joint effectiveness against complex and evolving threats. To address this issue, this work develops a unified framework that integrates models, standards, and strategies from each field. By bridging technical and conceptual gaps, the framework aligns security measures with privacy norms and the operational requirements of smart grids, enhancing protection across interconnected systems.

This dissertation adopts a multidisciplinary, interpretative mixed-methods approach and employs a conceptual framework synthesis to address critical infrastructure protection. Current critical infrastructure protection models, typically organized around resilience and prevention strategies and the pillars of policies, processes and procedures; prevention, detection and mitigation; and vulnerabilities, threats and attacks, prove insufficient in addressing the current complexities, growing interdependencies, and the role of human and organizational factors. These models tend to be narrow and overly technical, often neglecting broader socio-technical dynamics and cross-system challenges. To better reflect these realities, the developed framework expands into seven domains: policies and organizational governance; risk and threat analysis; socio-technical and human factors; interdependencies and multi-system interaction; cyberprivacy and data governance; protection and mitigation schemes; and evaluation metrics. This expanded model, along with its functional description, offers a more comprehensive foundation for understanding risks and implementing effective, holistic protection strategies.

Building on these, the dissertation identifies systemic and technical gaps, offers insights into energy systems, and provides recommendations for standards, directives, and educational tools to support critical infrastructure protection.

Keywords: cybersecurity, cyberprivacy, critical infrastructure, smart-grid.

ACKNOWLEDGEMENT

"*In the name of Allah, the most gracious, the most merciful*"

This doctoral dissertation reflects my work and thoughts on cybersecurity and privacy over the past eight years. Its completion has only been possible because of the guidance, support, and encouragement I received from many people, and here I would like to thank them all.

I am deeply grateful to my supervisor, Professor Tero Vartiainen, who not only guided and supervised my work but also helped me understand what science truly is. My second supervisor and former boss, Professor Heidi Kuusniemi, has given me her unconditional support, and I can clearly say that without her kindness and encouragement this work would not have been possible. I also thank my third supervisor, University Lecturer Dr. Timo Mantere, who has been supporting me since my master's studies and has always been generous with his guidance.

Two people deserve special mention: Dr. Reino Virrankoski and Professor Mohammed Elmusrati. Dr. Virrankoski, first as my teacher and later as my boss, colleague, and friend, has guided and supported me through every stage of my studies and work, and through him I got the idea of this research and the direction of my whole academic career. Professor Elmusrati is one of the most decent people I have ever met, and I was truly privileged to have him as a teacher, colleague, and very dear friend. His sincere advice, generosity, guidance, and support – both in work and in life – have always been something I could rely on.

I feel privileged to have had such a wide circle of support, whether from friends, colleagues, or my beloved family. I am grateful to my friends and colleagues for being part of this journey; the moments we shared gave me strength to continue. I especially want to thank Mustafa Ahmed, Ulrich and Ajish Steurenthaler, Anita Hammam, Ramy Hussien, Ali Elashmawy, Andre Luhtajärvi, Hanna-Mari Hietamäki (and Amora), Helena Heimonen, Simon Storbjörk and Jessica Lindberg, Oskar Juszczyk, Tijana Anić, Mike Mekkanen, Mahmoud Elsanhoury, Duong Dang, Abol Basher, Johanna Solodov, Émilie Solier, Tobias Glocker, Hafiz Haq, Petra Berg, Mazaher Karimi, and Linda Turtola, as well as the entire Digi-Eco team, the Computing Sciences group, and my Friday football team, for their support, friendship, and the good times that kept me balanced.

I would also like to thank our dean, Dr. Raine Hermans, and University Lecturer Dr. Tomi Pasanen, head of Computing Sciences, for the fruitful discussions and for being supportive and approachable whenever needed.

Above all, none of this would have been possible without my family. Their unconditional support, belief in me, and constant encouragement gave me the strength to reach this point. To my parents, my brothers, my nephew, my uncles, and my grandmother – this is for you. I cannot thank you enough!

Vaasa, September 29, 2025

Preface

Theory is when you know everything, but nothing works…

Practice is when everything works, but no one knows why…

Around here, theory and practice are combined: nothing works, and no one knows why…

By: Anonymous

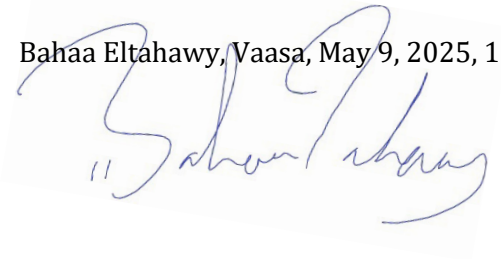
I found this quote online, it made me laugh, so I shared it with friends and colleagues, they laughed too and admitted it was true. This happened while I was writing this dissertation.

I started wondering, was it only a joke, a funny random quote I came across? Then, after a while I realized it was not at all. This three-line quote describes almost everything we experience – or try to address – right now, including this piece of research. Many times, we get caught up in our minds and theories that we do not actually know how things really are – or should be – in practice. Meanwhile, those who make things work often have no idea how or even why they work; but they are good at making them work. And in between are others – I hope I am one of them – who try to understand why things are the way they are and how to make them work, with no certainty whatsoever they will ever fully understand, or that things will finally work. We are just trying, and for now, that is pretty much all we can do.

It was not just a funny quote; it was a whole philosophy.

"Don't take me so seriously, it is just a joke, and I might be so wrong"

Bahaa Eltahawy, Vaasa, May 9, 2025, 11:12 PM



Contents

Figures

Tables

Abbreviations

A	Article
AAA	Authentication, Authorization, and Access Control
ADDIE	Analysis, Design, Development, Implementation, and Evaluation
AMI	Advanced Metering Infrastructure
CC-RSG	Cybersecurity Curricula Recommendations for Smart Grid
CER	Critical Entities Resilience
CI	Critical Infrastructure
CIA	Confidentiality, Integrity, and Availability
CIP	Critical Infrastructure Protection
COMPUSEC	Computer Security
CP	Cyberprivacy
CPS	Cyber-Physical Systems
CRA	Cyber Resilience Act
CS	Cybersecurity
CSF	Cybersecurity Framework
DER	Distributed Energy Resources
EBDES	Electricity-Based Digitalized Energy Systems
ENISA	European Union Agency for Cybersecurity
EU	European Union
GDPR	General Data Protection Regulation
HCI	Human-Computer Interaction
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
InfoSec	Information Security
IoT	Internet of Things
IPDRR	Identify, Protect, Detect, Respond, Recover
IS	Information Systems
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
MECE	Mutually Exclusive, Collectively Exhaustive

MLP	Multi-Level Perspective
MOOC	Massive Open Online Course
MSI	Multi-System Interaction
NIPP	National Infrastructure Protection Plan
NIS	Network and Information Systems Directive
NIS2	Network and Information Systems V2.
NIST	National Institute of Standards and Technology
NTC	Nordic Telemedicine Center
OT	Operational Technology
PbD	Privacy by Design
PET	Privacy Enhancing Technology
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIMS	Privacy Information Management System
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
REDISET	Resilient Digital Sustainable Energy Transition
SCADA	Supervisory Control and Data Acquisition
SESP	Smart Energy Systems Research Platform
SG	Smart Grid
SGAM	Smart Grid Architecture Model
SGCM	Smart Grid Conceptual Model
ST	Socio-Technical
STS	Socio-Technical Systems

Declaration of Generative AI and AI assisted technologies in the writing process

During the preparation of this work, OpenAI's ChatGPT was used with caution to improve the language, readability, flow, and transitions. The use of the tool was supervised, and after each interaction, the content was reviewed and edited as needed. I hereby confirm that I take full responsibility for the content, and that this is my original work, with no AI tools performing any tasks beyond what is stated above.

Articles

1. Eltahawy, Bahaa, and Reino Virrankoski. (2016). Into a Unified Information Privacy Preserving Model. In *the proceedings of the International Conference on Communications, Computer Science and Information Technology (ICCCSIT),* Dubai, United Arab Emirates, 12-14 March, 2016. Reprinted with permission.

2. Eltahawy, Bahaa, and Duong Dang. (2022). Understanding Cyberprivacy: Context, Concept, and Issues. *Wirtschaftsinformatik 2022 Proceedings. 21.* https://aisel.aisnet.org/wi2022/it_for_development/it_for_development/21. ©2022 Friedrich-Alexander-Universität, International Conference on Wirtschaftsinformatik. Reprinted with permission.

3. Romanovs, A., Bikovska, J., Peksa, J., Vartiainen, T., Kotsampopoulos, P., Eltahawy, B., ... & Strebko, J. (2021). State of the art in cybersecurity and smart grid education. In *IEEE EUROCON 2021-19th International Conference on Smart Technologies* (pp. 571-576). IEEE. https://doi.org/10.1109/EUROCON52738.2021.9535627. ©2022 IEEE. Reprinted with permission.

4. Eltahawy, B., Valliou, M., Kamsamrong, J., Romanovs, A., Vartiainen, T., & Mekkanen, M. (2022). Towards a massive open online course for cybersecurity in smart grids–a roadmap strategy. *In 2022 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)* (pp. 1-6). IEEE. https://doi.org/10.1109/ISGT-Europe54678.2022.9960630. ©2022 IEEE. Reprinted with permission.

5. Berg, P., Berlijn, S. M., Eltahawy, B., Hilber, P., Karimi, M., Klepper, K. B., ... & Xu, Q. (2024). Towards a Model for Assessing the Effects of Social-Cyber-Physical Threats on the Future Power Grid – Review and Workshop Results. In *2024 International Workshop on Artificial Intelligence and Machine Learning for Energy Transformation (AIE)* (pp. 1-6). IEEE. https://doi.org/10.1109/AIE61866.2024.10561312. ©2024 IEEE. Reprinted with permission.

6. Eltahawy, Bahaa. (2025). Industrial Systems and Industrial Data Privacy – A Comprehensive Review. [Submitted to *The International Journal of Information Security*]

7. Eltahawy, B., Dang, D., Bu-Pasha, S. & Kuusniemi, H. (2025). Realizing Cyberprivacy: A Comparative Study and Implementation Roadmap Based on Privacy by Design Framework, GDPR, and ISO 27701. [Unpublished]

8. Eltahawy, B., Berg, P., Turtola, L., & Karimi, M. (2025). Resilient or Vulnerable Twin Transition? A Multi-System Perspective on the Intersection of Sustainability and the Electricity-Based Digitalized Energy System. [Submitted to The *Energy Research and Social Science journal*]

Author's Contribution

Bahaa Eltahawy is the main author as well as the corresponding author in articles I, II, IV, VI, and VII; the second author in article VIII; and a co-author in articles III and V. The contributions of the author are described below:

1. Eltahawy is the main and corresponding author. Eltahawy reviewed the included publications, constructed the suggested unified privacy preserving model, wrote, and edited the article. Virrankoski edited the article and guided Eltahawy through his writing, and also provided the funding for supporting this article.

2. Eltahawy is the main and corresponding author. Eltahawy reviewed the included publications, performed the analysis, developed the suggested definitions, wrote, and edited the article. Duong edited the article and refined the suggested definitions.

3. Eltahawy is a co-author. Eltahawy participated in the project, provided ideation and discussions, and participated in writing the report that was converted into this article. Romanovs, Bikovska, and Peksa wrote and edited the article. Other authors participated in the project, provided ideation and discussions, and participated in writing the report that was converted into this article.

4. Eltahawy is the main and corresponding author. Eltahawy reviewed the included publications, crafted the research methodology, designed the course and exercises, wrote, and edited the article. Valliou reviewed the instructional design methods and MOOC types. Other authors participated in the project, provided ideation and discussions, and participated in writing the report that was converted into this article.

5. Eltahawy is a co-author and the corresponding author. Eltahawy reviewed the different energy models, participated in developing the suggested analysis model, wrote, and edited the article. Other authors participated in developing the suggested analysis model, wrote, and edited the article.

6. Eltahawy is the sole and corresponding author. Eltahawy collected the data, performed the research, reviewed the publications included in the review, conducted the analysis, wrote, and edited the article.

7. Eltahawy is the main and corresponding author. Eltahawy reviewed the included directives and standards, performed the analysis, developed the

suggested integration roadmap, wrote, and edited the article. Duong and Bu-Pasha edited the article and refined the roadmap. Kuusniemi guided Eltahawy and provided the funding to support this article.

8. Eltahawy is the first and corresponding author. Eltahawy reviewed the included publications, performed the analysis, applied the framework, drew the insights, wrote, and edited the article. Berg, also a main author, conducted the analysis, suggested the framework, collected data, wrote, edited, and provided the funding to support this article. Other authors participated in writing and reviewing the article.

1 INTRODUCTION

1.1 Background and research gap

The current technological landscape, shaped by the rapid advances in computation and communication systems and the rise of social and market platforms, has brought drastic changes across many levels, including organizational structures, personal interactions, rights, societal norms, behavioral patterns, economic systems, and legal frameworks (Vial, 2019; Plekhanov *et al.*, 2023; Eltahawy & Virrankoski, 2016). While these advancements and associated changes bring about numerous benefits, such as connectivity, greater efficiency, system optimization, improved decision-making, and new business opportunities, they also introduce new risks and challenges that must be addressed to sustain those gains (Schwertner, 2017; Brunetti, 2020).

The Internet and cyberspace are among the most advanced concepts we have encountered. Although they – as we know them today – have rapidly evolved over the past two decades, we continue to experience their impacts and adapt to the ongoing changes they bring. Security, in particular, has undergone significant transformation (Vial, 2019; Admass *et al.*, 2024). With the proliferation of connected devices and vast data transfers, data has become increasingly critical due to its substantial value. This has contributed to a rise in cyber threats and crimes targeting data and its owners for different motives, ranging from basic mischief to state-sponsored, structured attacks aimed at causing greater harm. As a result, cybersecurity has become a critical concern for governments, the public, and businesses, especially within the context of digital transformation (Admass *et al.*, 2024; Chidukwani *et al.*, 2022).

Privacy is another critical concern that has been significantly impacted by these changes too. The right to privacy, which involves safeguarding one's data and information, has long been fundamental and protected by laws and authorities (Warren & Brandeis, 1890). However, with digitalization and the increasing reliance on data for operations, services, insights, and targeting users, protecting and maintaining privacy in cyberspace and its interconnected spheres has become an extremely complex issue (Agre & Rotenberg, 1998; Loch *et al.*, 1998; Foxman & Kilcoyne, 1993). The challenge with cyberprivacy is that it is not merely a technical issue like information security and cybersecurity; rather, it is a broader concept that encompasses norms, cultures, behavior, and societal values, with conflicts arising among personal rights, organizational rights, and the benefits of data usage (Eltahawy & Dang, 2022). While this issue has not existed for long, the capabilities of current technologies in profiling data (Berghel, 2001; 2014), extracting Personally

Identifiable Information (PII) (Levit, 2009), revealing patterns about private behavior and activities (Thuraisingham, 2002; Hayes, 2006), make addressing cyberprivacy both urgent and necessary.

Finally, critical infrastructure has also undergone drastic changes driven by digital transformation and digitalization initiatives (Bouwmans *et al.*, 2006). The energy sector, in particular, exemplifies this shift, now resembling ICT firms in its operations and business models (Shomali & Pinkse, 2016). Efforts towards electrification, broader smart grid implementations, and the shift to electricity-based energy systems have brought various benefits (Fang *et al.*, 2011; Ding *et al.*, 2022). However, as noted earlier, these developments have also exposed the energy system to a wide range of cyber threats (Wang & Lu, 2013). As a core component of critical infrastructure supporting other essential services and systems, protecting the energy sector is vital. Alongside cybersecurity threats, smart grids and advanced metering systems also raise concerns about data privacy, as they handle sensitive personal, organizational, and operational data that must remain secure and confidential (Fang *et al.*, 2011; Wang & Lu, 2013; Nweke & Wolthusen, 2020a). This is critical, as the exposure of such data could lead to serious consequences, such as reputational damage, financial harm, and the loss of competitive advantage, among others (Lehto, 2022).

Given the growing cyber threats and expanding data-privacy challenges, there is a substantial need to move beyond fragmented approaches and develop integrated solutions that comprehensively address the risks affecting critical infrastructure (Nweke & Wolthusen, 2020b; Roshanaei, 2021). Although cybersecurity, cyberprivacy, and smart-grid protection have each been studied extensively, e.g., Fang *et al.* (2011), Hasan *et al.* (2023), and Ferrag *et al.* (2018), they remain treated as separate domains, often overlooking their interconnectedness and interdependencies within modern energy systems, critical infrastructure, and broader societal contexts. This fragmentation limits how effectively existing strategies protect critical infrastructure against multifaceted cyber threats and privacy risks. To fill this gap, a holistic, multidisciplinary, and multi-perspective approach is required, integrating models, standards, frameworks, and strategies across these fields (Poleto *et al.*, 2023; Eltahawy, 2025). This dissertation addresses this need by offering an integrated framework and insights to enhance the protection of critical infrastructure in today's digital landscape.

1.2 Objectives and scope

The main objective of this dissertation is to develop a unified framework to enhance the protection critical infrastructure. This framework integrates cybersecurity, cyberprivacy, and smart grids by drawing on existing and emerging conceptual and practical approaches, including frameworks, standards, and strategies related to these areas. The framework is developed by integrating research that addresses these topics mostly separately.

The specific objectives are as follows:

1. To conduct a comprehensive review of the literature on cyberprivacy, to identify conceptual foundations and emerging challenges.

2. To critically analyze cybersecurity approaches in the context of critical infrastructure, with an emphasis on smart grids and the energy sector.

3. To identify systemic and technical gaps in existing cybersecurity measures for smart grids and propose targeted approaches for addressing them.

4. To develop and disseminate a knowledge base that bridges conceptual and practical gaps in cyberprivacy and cybersecurity through awareness and educational tools.

5. To explore the evolution of future energy systems and assess the security and privacy implications of their transformation.

6. To contribute to energy transition studies by integrating digital transformation and sustainability within a unified socio-technical framework.

7. To examine key cyberprivacy standards and directives, evaluating their applicability and proposing mechanisms for their practical implementation.

The scope of this dissertation encompasses the analysis of scientific literature, industry reports, standards, and legal directives; qualitative and quantitative research methods; and an integrative interpretative synthesis of findings. The dissertation draws on work from multiple research tasks and projects, such as Smart

Energy Systems Research Platform (SESP)[1], Nordic Telemedicine Center (NTC)[2], Cybersecurity Curricula Recommendations for Smart Grids (CC-RSG)[3], Resilient Digital Sustainable Energy Transition (REDISET)[4], Vaasa-IoT[5], Robocoast[6], and others, each with different scopes and aims. By mapping connections across these studies, the dissertation builds a holistic perspective on protecting critical infrastructure.

1.3 Research question

The main research question of this dissertation is as follows:

RQ. *How can models and strategies for cyberprivacy, cybersecurity, and smart grids be integrated into a unified framework to enhance critical infrastructure protection?*

This question was further refined using the Mutually Exclusive Collectively Exhaustive (MECE) problem solving approach (Lee & Chen, 2018) into the following sub-questions:

- ***RQ1.*** *What are the key challenges and requirements for ensuring cyberprivacy in critical infrastructure and smart grids?*
- ***RQ2.*** *How do cyber threats affect smart grids and critical infrastructure, and which mitigation strategies are most effective?*

[1] SESP – Smart Energy Systems Research Platform is a project in the AIKO-program relating to the theme ”digitalization and innovation environment” in the growth agreement made between government and Vaasa region. The project is executed by the University of Vaasa in cooperation with Svenska handelshögskolan (Hanken) at Vaasa. More information at: https://www.uwasa.fi/en/tutkimus/hankkeet/sesp

[2] NTC is a project that aims to create an interdisciplinary competence center in telemedicine to gather knowledge and promote joint learning among healthcare professionals, researchers and companies. More information at: https://www.botnia-atlantica.eu/about-the-projects/project-database/nordic-telemedicine-center

[3] CC-RSG is a European Erasmus+ project that developed cybersecurity curricula recommendations for smart grids, aiming to define skills, roles, and learning outcomes while providing tools and strategies for higher education and professional training. More information at: https://www.uwasa.fi/en/research/projects/cybersecurity-curricula-recommendations-smart-grids-cc-rsg

[4] REDISET is a Nordic project that aims to look at descriptions of future energy systems and expected threat scenarios related to these. More information at https://www.uwasa.fi/en/research/projects/rediset-resilient-digital-sustainable-energy-transition

[5] Vaasa-IoT project aims to support the City of Vaasa’s strategic goal of achieving carbon neutrality by 2029 by developing a system that enables the monitoring, measurement, and verification of the need, impact, and progress of climate actions. More information at: https://www.uwasa.fi/en/research/projects/carbon-neutral-vaasa-202x-creation-data-platform-real-time-monitoring-testing-and

[6] Robocoast is a non-profit European Digital Innovation Hub (EDIH) whose mission is to provide companies with services to implement the digital transition. More information at: https://robocoast.eu/?lang=en

- ***RQ3.*** *How can existing cyberprivacy, cybersecurity, and smart grid protection schemes be combined into a coherent, actionable framework to protect critical infrastructure?*

Figure 1 illustrates how the research questions are addressed in the compiled articles and the dissertation's analysis.

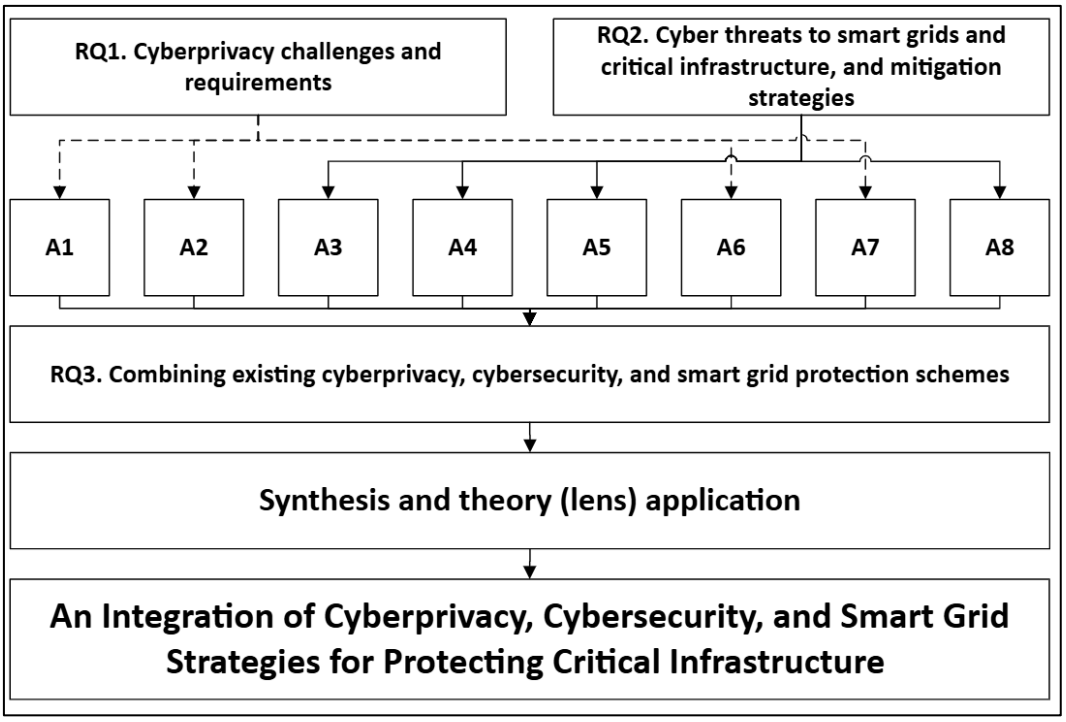


Figure 1. Overview of the dissertation's components.

1.4 Research approach

This dissertation adopts a multidisciplinary, multi-perspective methodology to develop a unified framework that integrates cybersecurity, cyberprivacy, and smart grid protection schemes for critical infrastructure. Given the interconnected nature of these topics, a mixed-methods design was employed, combining reviews, qualitative inquiry, quantitative analysis, and interpretative synthesis.

Research activities include:

- Systematic review and analysis of academic publications, industry and technical reports, and legal directives.

- Workshops and semi-structured interviews with experts and stakeholders.

- A case study on smart grid and cybersecurity education.
- A case study on NORDIC energy systems.
- Quantitative surveys examining future energy systems.

1.5 Research contributions

The contributions of this dissertation and the compiled articles are as follows:

1. Development of a unified framework that integrates cybersecurity, cyberprivacy, and smart grid strategies for critical infrastructure protection.
2. Identification and analysis of key cybersecurity and cyberprivacy challenges in smart grids and broader critical infrastructure systems.
3. Generation of insights into the evolution of future energy systems, emphasizing an integrated and holistic perspective.
4. Contribution to the advancement of standards, directives, and regulatory discourse related to cyberprivacy and infrastructure protection.

1.6 Dissertation Structure

This dissertation is structured as follows:

Chapter 1 introduces the research topic and provides background on the main concepts discussed in this work, along with the objectives, scope, central research question, research approach, and main contributions.

Chapter 2 lays the theoretical foundation by reviewing cyberprivacy standards and directives, cybersecurity standards and frameworks, and smart grid systems. It then covers critical infrastructure and resilience topics, concluding with a preliminary conceptual framework that integrates the introduced concepts and models, establishing a foundation for their use throughout the dissertation and analysis.

Chapter 3 outlines the philosophical orientation and methodology adopted, highlighting the integrative interpretive conceptual framework synthesis approach. It then details the specific research methods and data collection techniques employed.

Chapter 4 summarizes the articles included in this dissertation.

Chapter 5 presents the synthesis of findings by introducing the integrative approach, core elements, their interconnections and interdependencies, and identified challenges and gaps. It then updates the earlier model to propose a unified framework for critical infrastructure protection and discusses its implications.

Finally, Chapter 6 discusses the overall contributions and results, concluding with limitations and directions for future research.

2 LITERATURE REVIEW AND THEORETICAL BACKGROUND

This chapter lays the theoretical foundation for the dissertation by reviewing the key topics and concepts it addresses before presenting existing conceptual frameworks for Critical Infrastructure Protection (CIP), which form the basis for the dissertation's analysis and the development of the unified CIP model.

2.1 Cyberprivacy

Cyberprivacy, cyber privacy, or privacy in the cyberspace, is a set of concepts and solutions that collectively aim to protect personal and organizational data against leakage and misuse of information and data (Bartholomew, 2013). With the introduction of cyberspace and its interconnected spheres, several threats were introduced, among which privacy breaches and data misuse were some of the most prominent and critical (Breaux *et al.*, 2014a; Breaux *et al.*, 2014b) . Cyberprivacy is a multidisciplinary topic that is interconnected with several fields, with implications across several domains, including legal, technical, social, and ethical (Biselli & Reuter, 2021). Cyberprivacy is mainly a technical issue, as current technologies – with their unprecedented capabilities – have contributed to several privacy risks, including identification, monitoring, tracking, discovery, profiling, and revealing patterns about personal activities and behavior without explicit consent or awareness of these actions (Magnani, 2011; Magnani, 2007; Cooper *et al.*, 2010). However, the impacts of cyberprivacy risks are multifaceted, as they could affect basic and fundamental rights, businesses and economies, and result in severe and unwanted societal, behavioral, psychological, as well as moral and ethical consequences (Yadin, 2016; Demchak & Fenstermacher, 2009).

The main issue with cyberprivacy centers on the conflict between data usage and rights, since data provides the foundation for many benefits, including system optimization and insights about users (Cranor *et al.*, 2016), while individuals simultaneously retain the right to protect and control their own data (Warren & Brandeis, 1968). This was particularly emphasized by Eltahawy & Dang (2022), who provided four definitions for cyberprivacy to cover the required level of protection from different perspectives, i.e., technical, socio-technical, rights, and legal. Regarding protection, cyberprivacy as a concept relates significantly to cybersecurity, as it also addresses data in the cyberspace and utilizes cybersecurity concepts and protection measures (Philips, 2002). However, cyberprivacy differs from both cybersecurity and data privacy in the way it addresses data and protection, as it emphasizes holistic and comprehensive measures that go beyond technical ones to include non-technical

aspects such as risk management and control mechanisms, laws and rights, morality, ethics, and sociology, in addition to applying the right amount of privacy depending on the field of application (Eltahawy & Dang, 2022). The layers of cyberprivacy are shown in Figure 2 below.

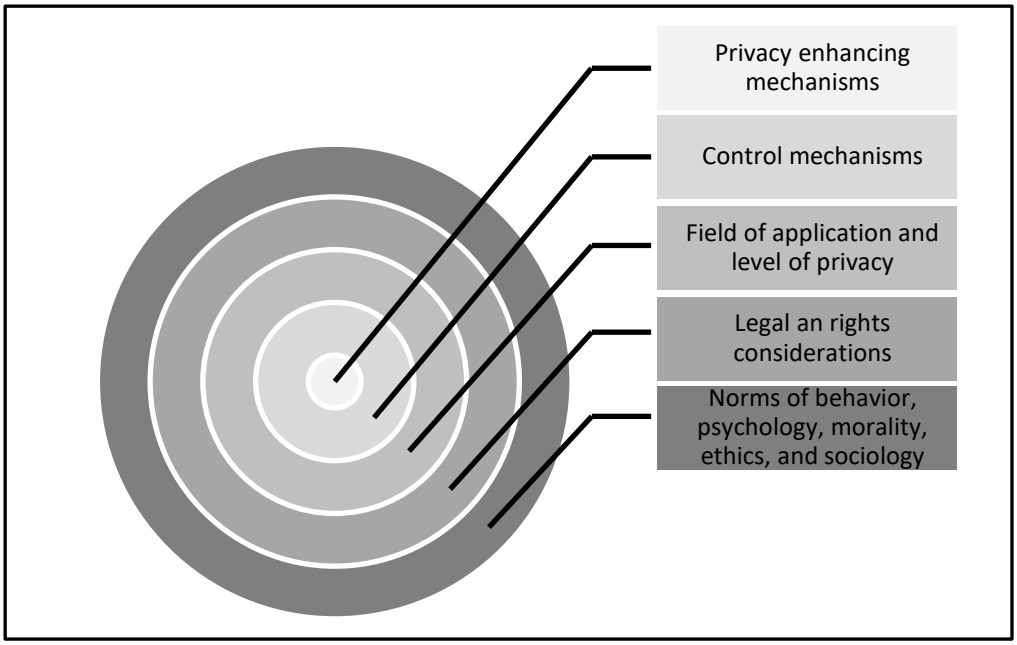


Figure 2. Layers of cyberprivacy [adopted from Eltahawy & Dang, 2022].

Finally, regarding application, to effectively achieve cyberprivacy, the literature has identified several technologies and solutions that can provide adequate level of privacy protection. These include, but are not limited to, k-anonymity, obfuscation, end-to-end encryption, differential privacy mechanisms, and blockchain implementations (Elmaghraby & Losavio, 2014; Froomkin, 1999; Knapp & Samani, 2013; Kumar *et al.*, 2016; Monti *et al.*, 2017). However, as emphasized, these are mere technical implementations that should be combined with the other protection layers to ensure full cyberprivacy protection.

2.1.1 ISO/IEC 27701:2019

ISO/IEC standards are universally adopted standards developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). These standards aim to provide guidance for implementation and support regulatory compliance, to enable consistency across practices, compatibility between systems, and coordinated efforts across sectors (Boiral, 2011). Regarding protection, ISO/IEC 27001 Information Security Management System (ISMS) and ISO/IEC 27002 Code of practice for information security controls have been the

standardized protection schemes for long, providing applicable information security measures and recommendations (Disterer, 2013). However, with the aforementioned privacy risks, ISO/IEC 27701:2019 was introduced to standardize privacy protection practices and provide controls for Privacy Information Management System (PIMS) (Lachaud, 2020). The standard builds on ISO/IEC 27001 and 27002, provides additional requirements, enhanced controls, and focuses on privacy by providing guidance for protecting PII.

In addition to ISO/IEC 27701, ISO/IEC 29100 Privacy Framework provides privacy principles and concepts, offering a foundation for designing privacy policies and systems (Ferrão *et al.*, 2024). ISO/IEC 29134 Privacy Impact Assessment (PIA) provides guidance on conducing impact assessments and help identify and manage privacy risks (Christofi *et al.*, 2020). ISO/IEC 29151 Code of Practice for PII Protection specifies security controls to protect PII and helps organizations implement measures for confidentiality, integrity, and availability (Lindquist, 2023). ISO/IEC 27018 Protection of PII in Public Clouds offers the same while focusing on cloud service providers handling PII (Hert *et al.*, 2016). ISO/IEC 27750 Privacy Engineering prvoides guidance for integrating privacy into the design and development of systems and services (Kalogeraki & Polemi, 2024). And, ISO/IEC 31700 Consumer protection: Privacy by Design, focuses on embedding privacy in the design of systems, devices, applications, and services (Valoggia *et al.*, 2024). In Figure 3, the relationship between these standards, highlighting the central role of ISO/IEC 27701, is shown.

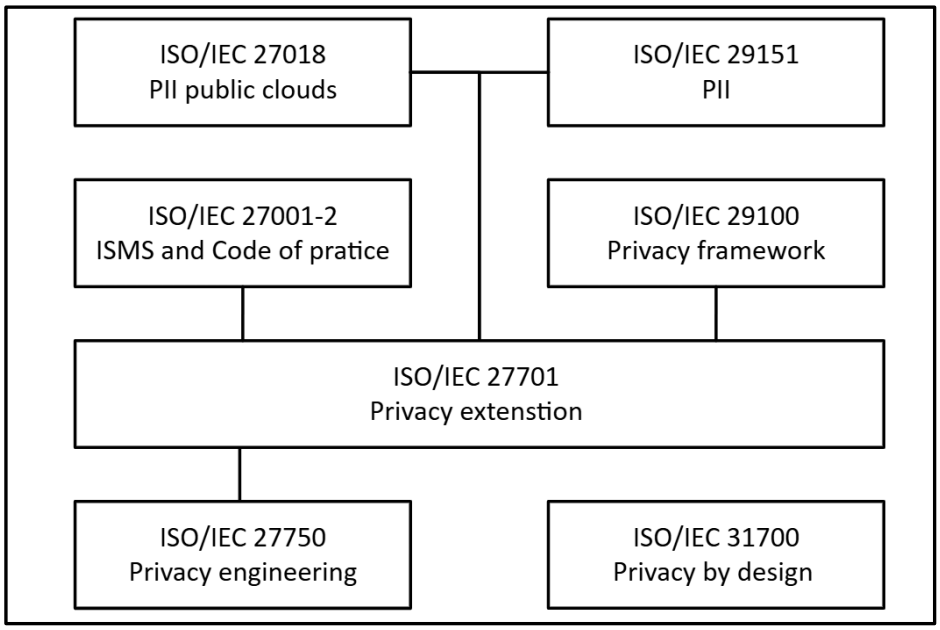


Figure 3. ISO/IEC 27701 privacy extension and related ISO/IEC standards [adopted and edited from Eltahawy *et al.*, 2025].

2.1.2 The General Data Protection Regulation

To address data privacy risks associated with the Internet and digital platforms, the General Data Protection Regulation (GDPR) was introduced by the European Union (EU) and came into application in 2018 (Voigt & Von dem Bussche, 2017) . Similar to ISO/IEC 27701, the GDPR was shaped by earlier regulations, including the EU Data Protection Directive, the EU Charter of Fundamental Rights, the Network and Information Systems (NIS) Directive, and others (Markopoulou *et al.*, 2019). The GDPR expanded on existing data protection principles and introduced specific measures for protecting PII. These measures include requirements for transparency, consent, accountability, and responsibility for compliance. Figure 4 presents the general architecture of the GDPR.

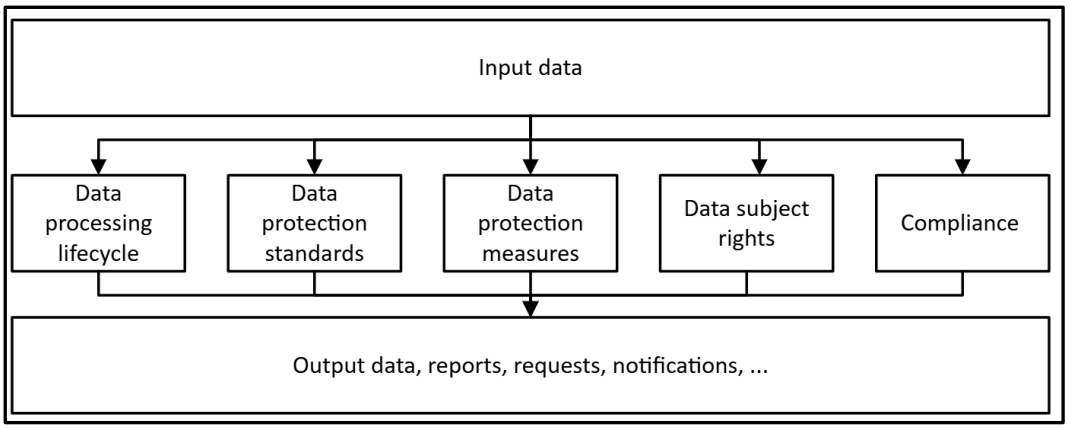


Figure 4. GDPR architecture [adopted from Eltahawy *et al.*, 2025].

2.2 Cybersecurity

Cybersecurity is defined as "*the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights*" (Craigen *et al.*, 2014). Traditionally, the conceptual measures of Information Security (InfoSec) and Computer Security (COMPUSEC), including Confidentiality, Integrity, and Availability (CIA Triad), provided an adequate level of protection for systems and data within isolated environments (Eltahawy & Dang, 2022). However, these measures had a narrow scope, focusing primarily on protecting individual systems and processes without addressing their rapid evolution and growing interconnectedness.

With current technological changes, increasing connectivity, the emergence of the Internet, and the exponential growth of data, the nature of cyberspace has evolved significantly. This evolution has brought about new complexities and challenges that

extend beyond isolated security concerns. As a result, cybersecurity has become the standard for information and data security, as it provides a comprehensive approach to protecting interconnected systems, networks, and digital assets against a wide range of threats and accidental failures. Moreover, cybersecurity's scope now extends beyond technical defenses to include organizational and procedural measures to manage and mitigate risks (NIST, 2018). This is discussed in the following subsections in more detail.

2.2.1 ISO/IEC 27001 and 27002

ISO/IEC 27001 and 27002 establish the foundation for information security management and a code of practice for implementing security controls (Disterer, 2013). Together, they provide a comprehensive framework and a set of requirements to plan, establish, implement, operate, monitor, review, maintain, and improve information systems and processes. In practice, ISO/IEC 27001 outlines the structure of an ISMS, while ISO/IEC 27002 provides detailed guidance on the implementation of controls. The controls are grouped into four categories: organizational, people, physical, and technological. The measures specified by the standards include access control, authentication and authorization, cryptographic protection, physical security, vulnerability and patch management, monitoring and logging, incident response, data backup and recovery, security awareness, education and training, and governance policies. Although widely adopted and relied upon, the standards do not prescribe specific systems, tools, or technical solutions for implementation (Al-Ahmad & Mohammad, 2013). Instead, they provide general guidance, leaving the choice of implementation methods to the organization based on its context, risk environment, and established best practices.

2.2.2 NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) defines three domains for protection, namely, people, technology, and processes (NIST, 2018). These domains represent the foundational elements of a comprehensive cybersecurity strategy, each addressing a distinct yet interdependent layer of defense. In this framework, people encompass users, operators, administrators, and all entities whose actions, awareness, and behavior influence system security. Technology refers to the hardware, software, and components that require protection against access, manipulation, or disruption. Finally, processes include the policies, procedures, and governance mechanisms that guide security implementation and development. In this view, NIST offers a socio-technical perspective on security rather than a purely technical one. In its Cybersecurity Framework (CSF), NIST further introduces five

core principles that cover the entire security landscape: Identify, Protect, Detect, Respond, and Recover (IPDRR) (Sulistyowati *et al.*, 2020). Figure 5 illustrates these principles along with their associated security measures.

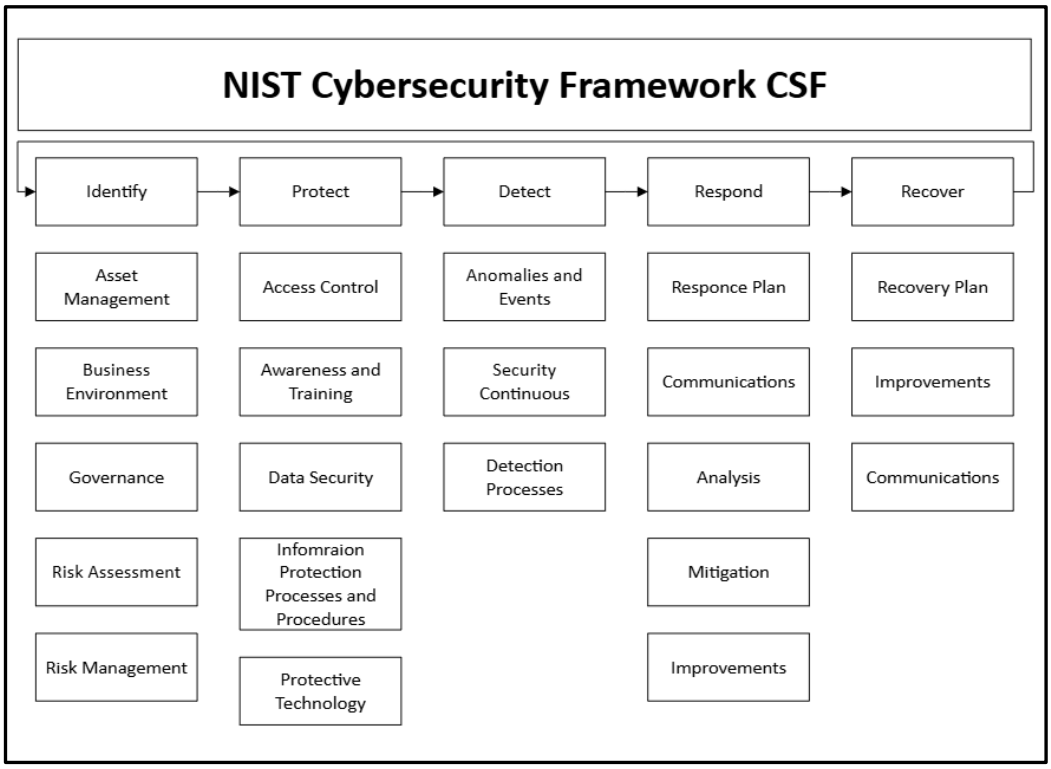


Figure 5. NIST CSF principles and measures [adopted and edited from Sulistyowati *et al.*, 2020].

2.3 Smart grid systems

Previously, energy systems operated in a largely unidirectional manner, delivering electricity – or other forms of energy – from utilities to end-users with minimal intervention, limited optimization, and primarily manual control (Delboni *et al.*, 2018). Similar to above, the energy sector has also witnessed drastic changes driven by advances in automation and the widespread implementation of ICT (Erlinghagen & Markard, 2012). These developments have introduced intelligence into the energy system, which resulted in the emergence of the concept of smart grids. As defined, "*a smart grid is an electricity network that can intelligently integrate the behavior and actions of all users connected to it, such as generators, consumers, and those that do both, to efficiently deliver sustainable, economic, and secure electricity supplies*" (European Technology Platform, 2010; Elzinga, 2015). This shift has transformed energy systems into complex, dynamic, socio-technical ecosystems where real-time data, bidirectional flows of electricity and information, and adaptive control

mechanisms enable enhanced reliability, resilience, and the coordinated integration of renewable resources. However, this evolution also introduced cyber risks into the energy sector, increasing its fragility and susceptibility to various types of vulnerabilities, such as privacy, connectivity, and security management (Ghelani, 2022). As a core component of critical infrastructure, smart grids require not only advanced technologies but also robust governance, regulatory frameworks, and cybersecurity measures to mitigate these risks and ensure the secure operation of their interconnected domains (Pardini *et al.*, 2017; Campbell, 2011).

Several models exist for describing power systems and their functions, for modeling, development, analysis, and integration, among which the most prevalent are the ISO/IEC Smart Grid Architecture Model and NIST's Smart Grid Conceptual Model, described below in more detail.

2.3.1 ISO/IEC 63200 – Smart Grid Architecture Model

The Smart Grid Architecture Model (SGAM) is a hierarchical framework that represents modern power systems and associated smart grids from a general perspective through five interactive layers, each reflecting different operational domains, their functionalities, and objectives (Uslar *et al.*, 2019). These layers include the business, function, information, communication, and component layers. The last of these – the component layer – is where energy operations take place, encompassing the physical infrastructure and energy sector domains, such as generation, transmission, distribution, Distributed Energy Resources (DER), customer premises, and utilities. The layer is further divided into several zones that address varying system demands, such as market, enterprise, operation, station, field, and process to support seamless integration and adaptability. The SGAM model is highly abstract and flexible, making it well-suited for illustrating system scenarios, explaining different operations and dependencies, simulating performance across domains, and implementing a wide range of use cases necessary for development and planning. Figure 6 shows the architecture of the SGAM model.

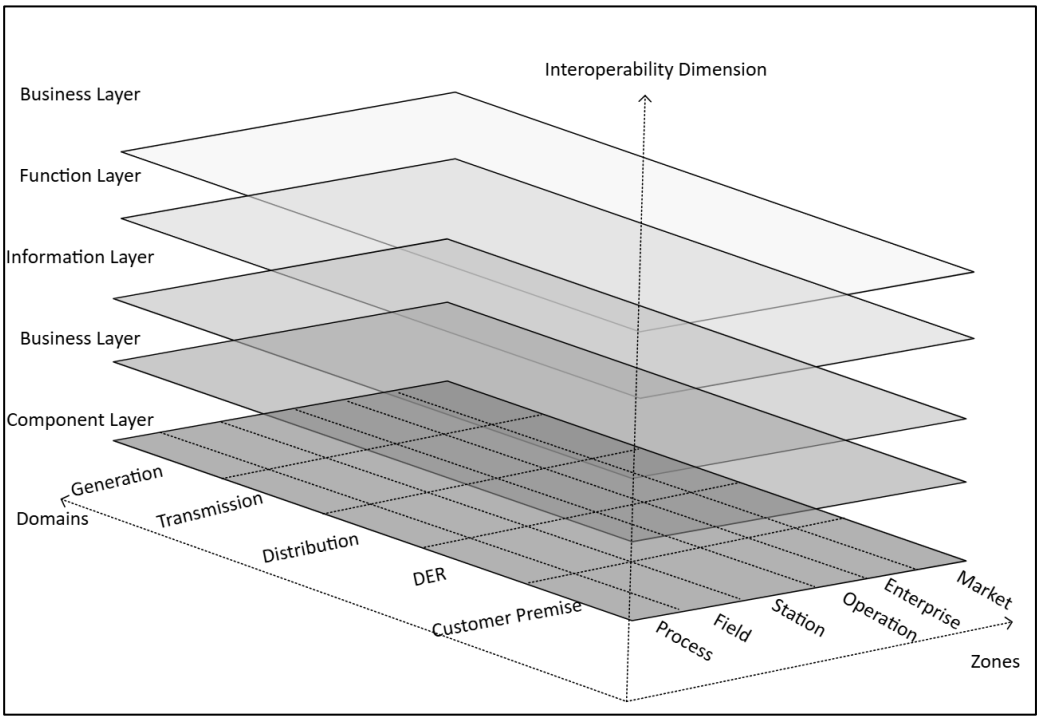


Figure 6. ISO/IEC SGAM model [adopted and edited from Uslar *et al.*, 2019].

2.3.2 NIST Framework and Roadmap for Smart Grid – Smart Grid Conceptual Model

Similarly, NIST's Smart Grid Conceptual Model (SGCM) offers a high-level alternative for illustrating the power system and smart grids by grouping domains, highlighting their associated roles and responsibilities, and emphasizing the interaction and interconnections between these domains (Gopstein *et al.*, 2021). SGCM encompasses the domains of operations, markets, transmission, generation, distribution, customer, and service provider. The model identifies the key points where information exchange occurs and where energy flows take place across the system. With these clearly defined domains and roles, SGCM serves as a practical guideline for understanding the grid from the perspective of different stakeholders, as well as being used for system analysis, strategic planning, and aligning stakeholder requirements within a common reference framework. Moreover, SGCM supports the development of standards that promote interoperability and smooth communication across grid components, thereby improving the overall efficiency, dependability, sustainability, and adaptability of the modern power system. Figure 7 shows SGCM model and its domains.

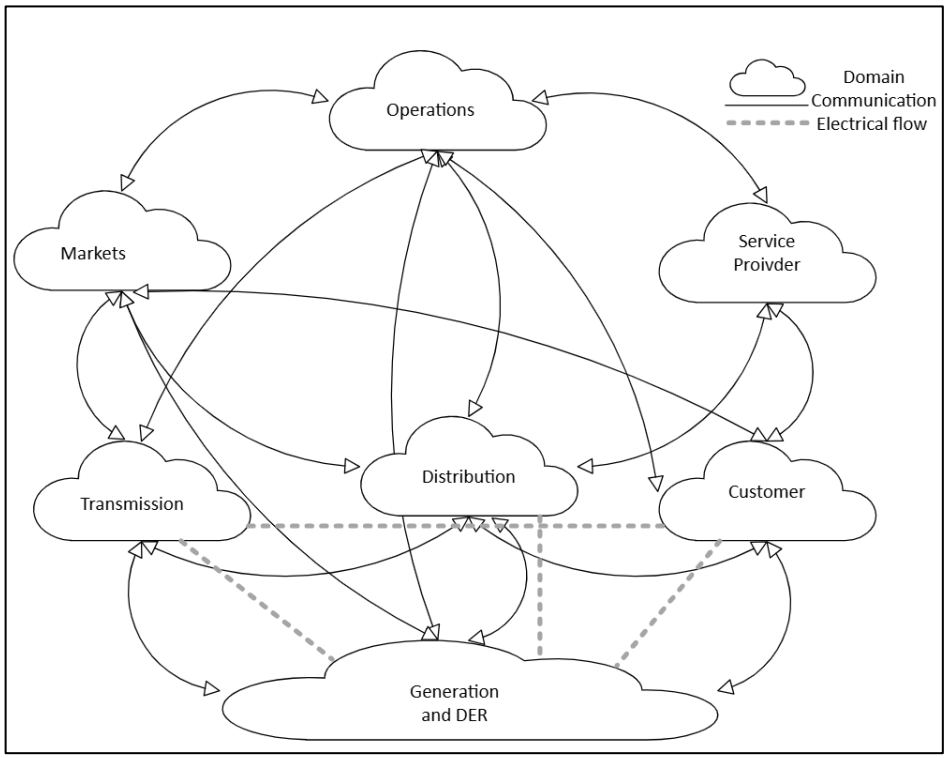


Figure 7. SGCM model [adopted and edited from Gopstein *et al.*, 2021].

2.4 Energy as critical infrastructure and current challenges

Critical infrastructure refers to the assets and systems essential for vital social functions, health, safety, security, economics, and overall social well-being (Moteff, 2004). This encompasses a range of sectors and key services, such as energy, utilities, emergency response, transportation, health, food supply, and communication. Recently, attention has been increasingly focused on these sectors, particularly on the essential functions they support, due to the significant consequences that can result from their disruption. Such disruptions, whether accidental or intentional, can trigger major cascading effects that spread beyond the affected domain and impact other interdependent sectors as well.

Central to critical infrastructure is the energy sector, as it plays a vital role not only in supporting everyday societal functions but also in enabling the operation of other critical domains (Rinaldi *et al.*, 2001). Without reliable energy supply, most other sectors would face immediate interruption, compromising their ability to operate and threatening overall societal stability. This highlights the importance of the energy sector and its role as a foundational element in maintaining national stability. Figure 8 shows the interdependencies and interfaces between the energy sector and other

critical infrastructure domains, emphasizing the extent to which they rely on its continuous and secure functioning.

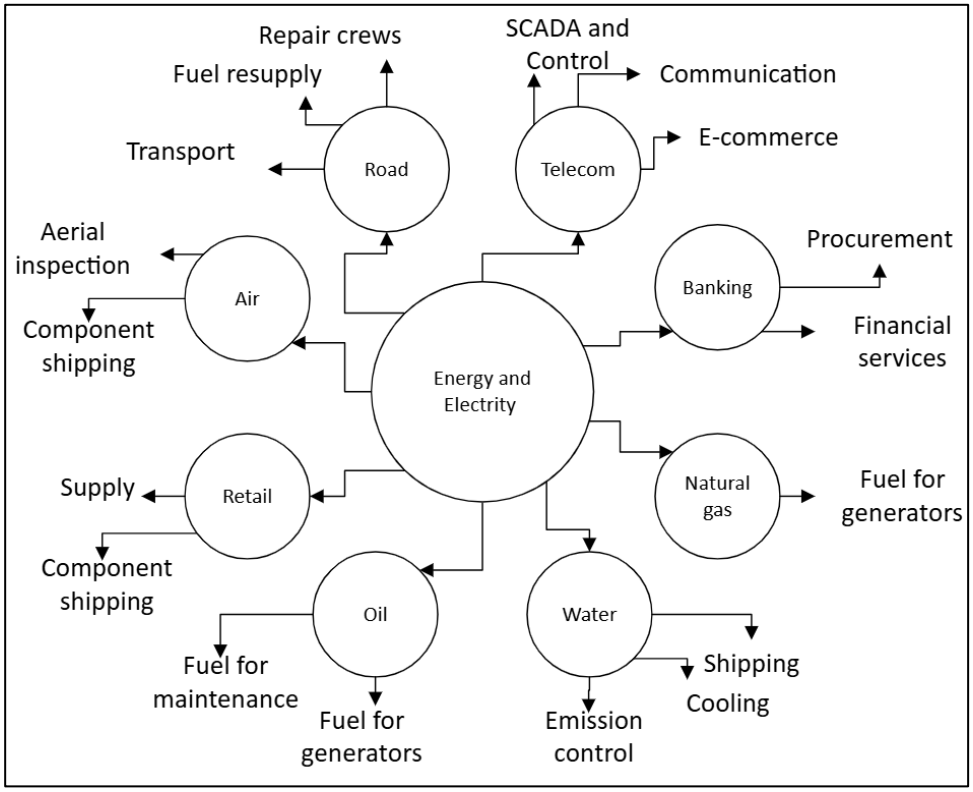


Figure 8. Critical infrastructure dependencies on the energy sector [adopted and edited from Rinaldi *et al.*, 2001].

Despite its critical role, the energy sector currently faces a number of pressing challenges that undermine its ability to remain secure, resilient, and responsive. First, the changing landscape and growing dependence on digitalized energy systems make the sector a prime target for cyberattacks, with adversaries seeking to exploit its vulnerabilities to disrupt operations on a large scale. For example, Alcaraz & Zeadally (2015) highlighted the rise in incidents targeting critical infrastructure, with the energy sector and its control systems being among the most affected. This was also confirmed by Roshanaei (2021), who noted that the energy and transportation sectors experienced the highest number of targeted cyber incidents. Second, the sector is undergoing several technological and systemic shifts, including increased digitalization, integration of ICT, expansion of distributed energy resources, and growing interdependencies with other sectors and supply chains. Moreover, existing models for energy systems such as SGAM and SGCM – though widely used – show limitations in addressing evolving needs, especially in terms of flexibility, integration of emerging technologies, cybersecurity, privacy, and human-centric concerns (Berg *et al.*, 2024).

2.5 Critical infrastructure protection

Finally, building on the challenges outlined in the previous section, it is clear that ensuring the protection of critical infrastructure – particularly as represented by the energy sector – is essential. This requires structured and adaptive approaches, rather than narrowly focusing on individual threats or specific incidents. The required protection must be comprehensive, taking into account evolving technologies, complex interdependencies, the dynamic risk landscape, and human factors and needs as well. The following are some of the existing frameworks that support this need.

1. The US's National Infrastructure Protection Plan (NIPP) (Hemme, 2015): similarly, the NIPP provides a strategic framework for strengthening the security and resilience of critical infrastructure and key resources across the physical, cyber, and human domains. Rather than following a fixed cycle, the NIPP promotes a dynamic and iterative risk management process. This process includes: setting security goals and objectives; identifying critical assets, systems, and networks; assessing risks based on threats, vulnerabilities, and potential consequences; prioritizing protective efforts and investments; implementing corresponding protection and resilience programs; and finally, measuring effectiveness and refining strategies as needed. This flexible, evolving structure allows for continuous adaptation to emerging risks, evolving technologies, and shifting threat landscapes.

2. CIP Strategy: in their work on the same topic, Mosadeghi et al. (2018) proposed a five-domain cyclic strategy for protecting critical infrastructure. The strategy includes: identifying critical infrastructures and the essential assets to be protected; conducting cross-sectoral analysis of interdependencies; performing vulnerability and risk analysis to uncover existing and anticipated risks, to inform better protection planning; implementing resilience measures; and finally, establishing response and recovery procedures. The strategy operates as a continuous cycle, revisiting each phase and evolving to address emerging challenges.

3. Holistic approach for enhancing CIP: in their work on the same topic, Nweke & Wolthusen (2020) propose a holistic approach for enhancing critical infrastructure protection, structured around three interconnected components. The first focuses on organizational measures and includes policies, procedures, and processes that govern the management and oversight of the infrastructure in question. The second focuses on technical measures, addressing system vulnerabilities, potential threats, and attack

mechanisms, while aiming to understand their sources, impacts, and broader implications. The third component combines both technical and strategic dimensions, emphasizing the need for integrated detection, prevention, and mitigation plans that not only respond to incidents but also anticipate and adapt to evolving risks and challenges. **This approach is adopted in this dissertation as a foundation for developing the proposed unified model for protecting critical infrastructure.** Figure 9 illustrates the components of this holistic CIP approach.

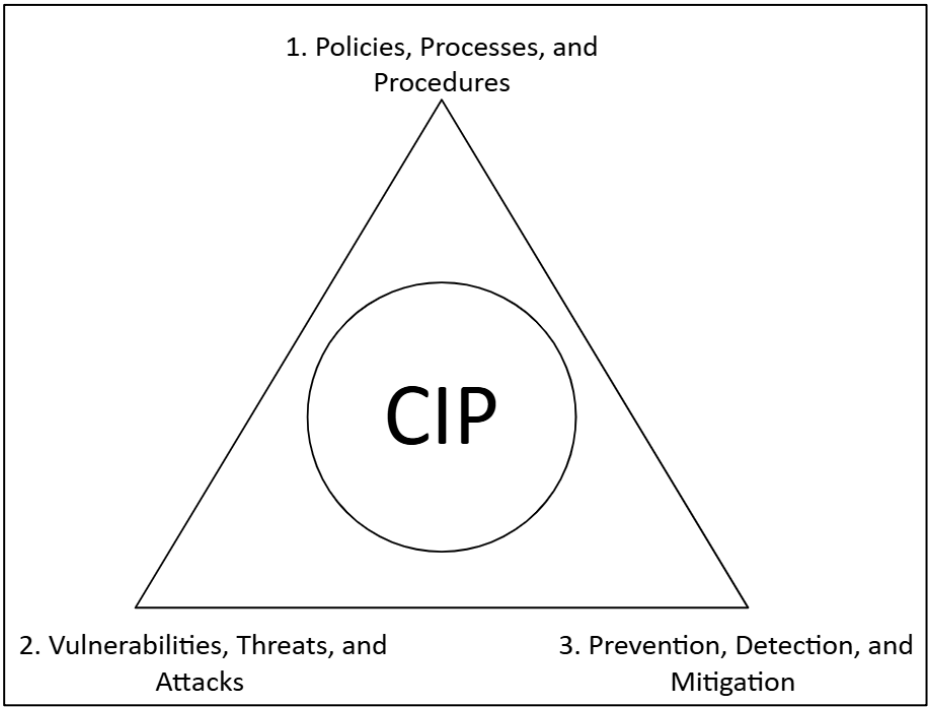


Figure 9. Holistic approach for enhancing CIP [adopted and edited from Nweke & Wolthusen, 2020].

4. Finally, NIST's Cybersecurity Framework (CSF): as shown in Figure 5, NIST's CSF, structured around the core functions of Identify, Protect, Detect, Respond, and Recover, is among the most widely adopted frameworks for CIP (Sulistyowati et al., 2020). The framework provides a structured yet flexible approach for managing cybersecurity risks, since each function addresses a different aspect of risk management. The framework proceeds with: identifying critical assets and vulnerabilities; implementing measures to ensure protection of services; detecting incidents and cybersecurity events; responding to incidents; and enabling timely recovery. While the framework was originally developed for managing risks to critical information and operational systems, the CSF has been increasingly used in CIP contexts due to its adaptability across sectors.

3 RESEARCH PHILOSOPHY, APPROACH, AND DATA COLLECTION

This chapter outlines the overall research method employed in this dissertation, as well as the specific methods used in the individual articles. It begins by examining the field of information systems, followed by an overview of relevant philosophical research paradigms and their components. The chapter then presents the research approach adopted in this study and describes the methods used for data collection, analysis, and synthesis.

3.1 Information systems

Information Systems (IS) – as systems for managing and utilizing information – involve Information Technology (IT) systems such as computers, software, databases, communication systems, the Internet, and mobile devices, as well as processes that support operations and inform actors in various organizational and societal contexts (Boell & Cecez-Kecmanovic, 2015). IS focuses on the development, implementation, use, and impact of such systems in organizations and society. IS systems can be described as "*social systems that are technically implemented*" (Gregg *et al.*, 2001; Hirschheim *et al.*, 1995). On the other hand, IS as a scientific research discipline differs significantly from the narrow perspective that views it merely as a collection of technical systems. Rather than focusing on technical and computational aspects only, IS research goes beyond to examine how technologies are embedded and utilized to fulfil informational needs and requirements. In this context, IS is a socio-technical field that concerns the development, use, and effects of systems involved in the generation, processing, handling, and retrieval of data to support organizational and societal actors with information, insights, understanding, and decision-making capabilities. It also addresses the integration of technological and social systems, and the interactions and transitions that occur within them. IS can thus be viewed and described as the intersection between organizational, societal, and IT domains (Hasan, 2018), shaping theories of socio-technical dynamics and practical innovations in system design, while addressing evolving challenges related to data management, system integration, and organizational and societal needs. The core focus of IS includes studying the application of IT to support organizations, the processes of systems development, the management of information systems, their organizational value, and their broader societal impact (Avgerou, 2000).

3.2 Philosophical research paradigms

According to research scholars, research is one of the different approaches used to build knowledge and enhance understanding about a certain topic or issue (Kerlinger, 1966; Mertens, 2019). Research is a process of systematic inquiry that is conducted following established theoretical frameworks and guidelines (Gregg *et al.*, 2001). The main purpose of research and the use of theories and frameworks is generating knowledge artifacts that can be transferred to other settings, making the process of research distinct from evaluation, which also uses systematic inquiry but targets decision making. That being said, research can be simplified as the systematic process of learning (Rossman & Rallis, 2011). Following this, to do research – or to learn – different components, including ontology (the nature of reality), epistemology (the nature of knowledge), and methodology (the approach of obtaining knowledge and understanding), exist to properly address different problems, issues, and topics with the mindset and tools needed (Guba & Lincoln, 1994; Gregg *et al.*, 2001). Based on how these components are interpreted and combined, different paradigms emerge. These include – but are not limited to – positivism, post-positivism, interpretivism, constructivism, pragmatism, critical realism, and socio-technical/developmentalism. Following is a brief description of these components and paradigms:

- Ontology is the branch of philosophy that concerns the nature, structure, and properties of reality – what is assumed to exist, and the basic building blocks that make up phenomena or objects to be investigated (Iivari *et al.*, 1998). It seeks to establish understanding by describing facts and meanings objectively in a realistic manner. In IS, ontology relates to phenomena such as information and data, information systems, and human beings in their roles in development, use, and interactions with technology, organizations, and society. Ontology is commonly interpreted through two perspectives: realism and idealism. In realism, the focus is on describing "*things*" as they are – as structures and agents. In contrast, idealism adopts a constructivist view, aiming to describe meanings, intentions, and interactions.

- Epistemology concerns exploring the nature of cognition, processes of understanding, and methods of inquiry and obtaining knowledge (Iivari *et al.*, 1998; Pretorius, 2024). It seeks to establish understanding by examining how knowledge is acquired and justified. Three epistemological positions exist for understanding and generating knowledge. The first emphasizes objective empirical observation, using the right tools and methods. The second suggests that reality is partially known and can be understood subjectively through individual lenses and perspectives. The third assumes that reality is

constantly evolving, making it impossible to capture full knowledge or understanding at any given moment. In the context of IS, epistemology concerns the type of knowledge obtained by academic and scientific IS community and its limitations. Two primary approaches are followed: the first aims to produce highly generalizable methods and approaches, while the second focuses on providing constructs or metaphorical templates to support IS development with useful insights.

- Methodology is the procedure and detailed description of the steps involved in the approach used to acquire knowledge about a particular topic. It includes the tools, canons, and principles related to the methods of inquiry used to develop, evaluate, and justify goals, concepts, interpretations, and actions (Iivari *et al.*, 1998). It serves as a bridge between philosophical assumptions, human processes, and research capabilities, supporting the use of information and ensuring alignment with research objectives and questions (Gregg *et al.*, 2001). Two primary research methodologies exist – each encompassing various subtypes: qualitative and quantitative methods. Qualitative approaches focus on interpretative techniques to understand context-specific experiences, while quantitative approaches emphasize structured techniques to build hypotheses and theories, and to generate generalizable results and insights.

- Positivism is an objective research paradigm based on ontological and epistemic realism, assuming that reality and facts are singular, follow universal laws, exist independently of subjective experiences and perspectives, and can be systematically observed and understood through scientific inquiry and experimentation (Avenier & Thomas, 2015; Pretorius, 2024). Its goal is to discover certain objects and phenomena using tools and methods that minimize personal bias and subjectivity. Positivism enables the generalization of facts and results for developing theories and models that can be applied across different contexts.

- Post-Positivism, as a research paradigm, is similar to positivism in its commitment to objectivity and its ontological and epistemological realism. However, it places greater emphasis on the research process and the role of induction, acknowledging the existence of different values – such as culture, experience, and history – that influence and affect the interpretation of results. Post-positivists accordingly stress this complexity, highlighting the need for reflectivity and arguing that absolute objectivity is unfeasible, as research is never entirely free from the researcher's influence. For these

reasons, post-positivism promotes minimizing bias through transparency and by openly addressing potential value implications.

- Constructivism is a research paradigm that emphasizes subjectivity, where reality is partially understood through individual perspectives and subjective perceptions, making each person's reality unique and reflective of personal experiences and interactions. Social interaction is central to constructivism, as it contributes to shaping different realities, with knowledge being co-constructed through ongoing interactions and contexts. In constructivism, bias and differences in shared experiences are not eliminated, but are recognized, understood, and acknowledged. In contrast to other paradigms, inquiry in constructivism is context-driven, qualitative, collaborative, and involves flexible and adaptive approaches to research design.

- Interpretivism is a subjective research paradigm that, similar to constructivism, holds that reality is partially known as its constructed in individuals' minds. Interpretivists emphasize that we cannot fully understand other experiences objectively, but we can try to interpret and make meaning of them. Interpretivism highlights the importance of recognizing diverse experiences and accepts that multiple realities can coexist, depending on the perspectives and conditions of the involved observers. The paradigm's inquiry focuses on understanding and interpreting experiences, their origins, and impacts rather than directly analyzing statistical data or assessing policies. The main difference between constructivism and interpretivism lies in the role of the researcher. Constructivism considers the researcher inherently part of the research process, actively influencing it and co-creating knowledge. In contrast, interpretivism emphasizes the researcher as a more detached, passive observer who seeks to understand meaning without co-constructing knowledge. That being said, interpretivists strive to maintain a degree of separation while interpreting subjective experiences as objectively as possible.

- Pragmatism is a flexible research paradigm that is neither entirely objective nor subjective, based on the belief that reality is constantly changing or debated, and therefore does not rely on a single reality or method of inquiry (Pretorius, 2024). In pragmatism, research methods should be chosen and adapted to address the research questions. This allows for using a mix of qualitative and quantitative methods as necessary to investigate a certain topic and to draw a comprehensive understanding of complex issues. Pragmatism focuses on practical outcomes, holding that the value of research lies not in producing abstract theories, but in generating knowledge and

solving problems. In simpler terms, pragmatism emphasizes implications and creating actionable solutions.

- Critical realism is a research paradigm that views subjectivity and objectivity as interconnected across different levels of reality. It assumes the objectivity of reality, which exists independently of human perception, but argues that this reality cannot be directly observed. Instead, reality can be understood through a layered approach, uncovering the deeper structures and mechanisms that influence it (Avenier & Thomas, 2015; Pretorius, 2024). Critical realism aligns with positivist and interpretivist ontological assumptions in acknowledging both an objective reality and the coexistence of multiple realities and interpretations. However, it argues that empirical methods alone are insufficient, and explanations must also account for unobservable structures (Mukumbang, 2023). Like interpretivism, critical realism recognizes the role of meaning, ideas, and experiences, but further emphasizes that the world functions as an open system with groups of structures, contexts, and mechanisms, making critical realism suitable for developing open systems theories. A key concept in critical realism is its stratified reality, which distinguishes between the real (structures with generative power and potential to produce something), the actual (phenomena and events that actually occur), and the empirical (what is observed and experienced). Epistemologically, critical realism rejects the notion of a final truth, encouraging researchers to be value-aware when selecting inquiry methods to collect experiences. It supports the use of diverse sources and methods to generate a group of answers that help address complex realities. Finally, while critical realism acknowledges the differences and backgrounds of researchers, it strives for a deeper, objective understanding of the structures and knowledge.

- Finally, socio-technical/developmentalism is a new research paradigm proposed and emphasized by Gregg *et al.* (2001) to bridge the gap between positivist and interpretivist practices and address the specific needs of software engineering research by focusing on the creation of new systems and related knowledge processes (Kroeze, 2011). Unlike the paradigms it links, the socio-technical/developmentalism paradigm is considered objective, subjective, and interactive in nature. Ontologically, it views reality as technologically created, where multiple social realities coexist, influenced by the need, acceptance, and extent of technology used. Epistemologically, it emphasizes the objectivity of reality but frames it interactively, through the researchers' experience of system behavior as interactions occur and the creation of contexts that reflect their own values and priorities. What

distinguishes this paradigm is its alignment with the developmental methodology, a product- or model-oriented approach focused on generating ideas, designing, testing hypotheses through prototypes and proofs-of-concept, developing early implementations, and providing formal mathematical and logical descriptions of systems.

Figure 10 below visualizes the paradigms discussed above, showing their placement in terms of relative subjectivity, objectivity, rigor, and openness.

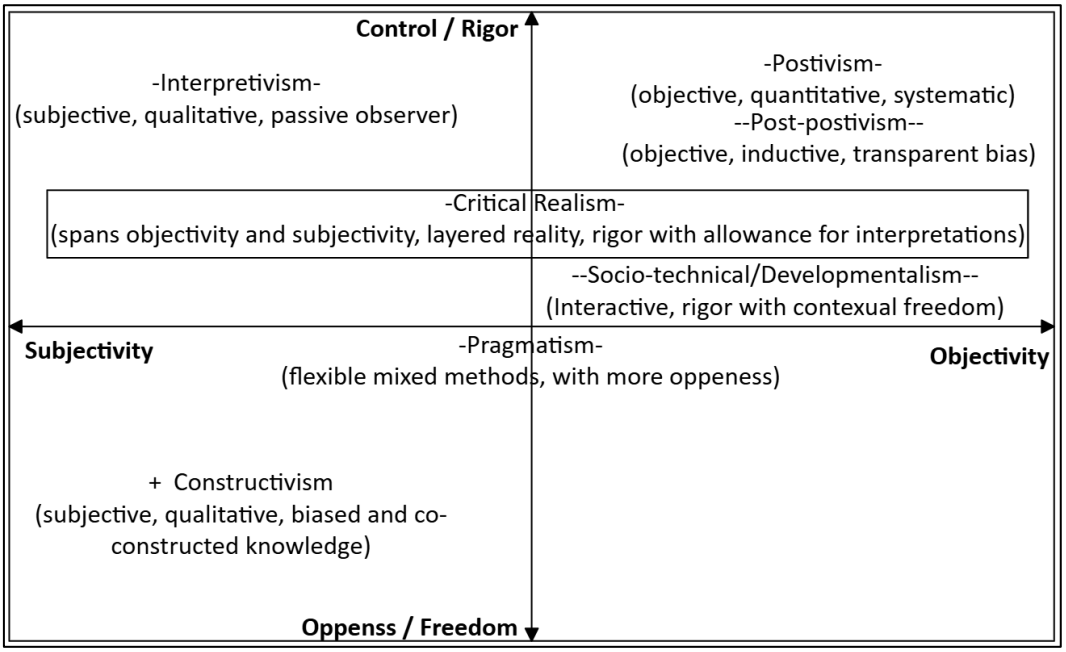


Figure 10. Major research paradigms explained [adopted from Hirschheim & Klein (1989) and modified with own understanding and elaboration].

3.3 Research approach and methodology

This dissertation follows the themes, objectives, and guidelines of IS research. It focuses on specific IS systems phenomena – cyberprivacy, cybersecurity, smart grids, and critical infrastructure – aiming to build knowledge and enhance understanding of them by examining their socio-technical aspects, including development, use, effects, and associated data processes. The research adopts the interpretivist research paradigm, guided by its beliefs and positioning, and follows an interpretive research approach to achieve its objectives. The rationale behind the adoption of this paradigm and approach is discussed below.

As outlined earlier, interpretivism (Avenier & Thomas, 2015; Pretorius, 2024) addresses the nature of reality and the ways of acquiring knowledge. As the name

implies, it does so in an interpretative manner, focusing on how meanings are constructed through human experience. In this paradigm, reality is understood as partially known and is interpreted based on experiences and an understanding of the factors shaping it. This means that, depending on the observers, their interpretations of the same reality can vary, which indicates the coexistence of multiple versions of that reality – or rather, multiple realities – simultaneously. Although this suggests a subjective research perspective, interpretivism seeks to obtain knowledge objectively by viewing the researcher's role solely as an observer. Interpretivists accordingly must recognize their biases and acknowledge the factors influencing their thinking before reporting final results based on their observations.

Interpretivism was chosen as the research paradigm and main umbrella governing this research for two key reasons: its flexibility and its acceptance of mixed-research methods. First, interpretivism provides the flexibility needed to explore emerging issues related to specific research problems, as it supports the coexistence of multiple realities, stances, and perspectives (Ponelis, 2015). Second, despite being a structured qualitative paradigm and the incompatibility between general qualitative and quantitative research approaches (Dawadi *et al.*, 2021; Smith, 1983), interpretivism allows for the integration of quantitative and statistical methods with qualitative methods to form interpretation (Wiggins, 2011). This, in fact, may offer a more robust approach than relying on a single-research method, as it provides a more comprehensive understanding and coverage of the phenomena under investigation while addressing the limitations of a single-method approach (McChesney & Aldridge, 2019). Interpretivism, thus, can be used to frame a mixed-method study, which is particularly important for this dissertation, since the compiled articles employ various research methods, approaches, and methodologies, making a comprehensive research paradigm essential for integrating them and forming a coherent understanding of their collective insights.

An interpretative research approach is therefore employed for this objective. Here, the practices and principles outlined by Walsham (1995; 2006), Rowlands (2005), Yin (2009), and Klein & Myers (1999) for conducting interpretative research, are adopted. The general practices of this approach involve, first, selecting the study area, defining the research problem, addressing the "*what*," "*why*," and "*how*," and creating a loose hypothetical conceptual model to be investigated and reflected upon later. Second, identifying and selecting cases and designing data collection protocols. At this stage, it is recommended to adopt a theory as an initial guide for designing and collecting data, which can be qualitative through interviews, observations, and documents, or also quantitative data, as emphasized earlier. For this dissertation, data are drawn from reports in the form of articles, presenting various methodologies and approaches, including reviews and standards studies, qualitative interviews and

analysis, and framework applications. However, no theory was adopted for the design and data collection phase as recommended, since the reports and associated data were derived from different project tasks, addressing diverse topics and concerns, and often not following the same theme or methodology. Third, after collecting data and conducting case studies, the analysis phase follows with iterative processes and hermeneutic reflection. This includes drawing cross-case insights and conclusions, and performing within-case analysis; shaping and adjusting propositions while confirming, extending, and refining the theory presented in the initially created hypothetical conceptual model; and assessing findings, ensuring their applicability, and identifying final patterns. Similarly, at this stage, it is recommended to follow a specific type of theory or framework to guide the analysis. For this, a comprehensive synthesis of the individual outcomes from the compiled articles is conducted.

Regarding synthesis, synthesizing is considered the most important part of reviews, as it provides a complete representation of the literature being investigated and studied (Okoli, 2012, Wyborn, 2018). According to Rowe (2012), a good synthesis involves not only summarizing research findings, but also applying novel interpretations through appropriate analytical and semantic classifications to provide abstraction and make sense of pieces of research addressing specific problems at a particular level. Synthesizing is a qualitative process that can be conducted in an ad-hoc and flexible manner (Snyder, 2019); however, in practice, certain approaches and types of synthesis are commonly used in IS, with the most prevalent including: narrative, theoretical, interpretive, framework, meta-analysis, meta-synthesis, realist, comparative, and thematic synthesis (Skinner *et al.*, 2022; Barnett-Page *et al.*, 2009). These methodological approaches can be applied in different styles or through various analytical lenses to serve specific purposes. These include conceptual for developing theory and refining concepts, integrative for combining perspectives and methodologies, argumentative for constructing interpretive arguments, explanatory for explaining causal and contextual dynamics, and descriptive for organizing existing knowledge (Rowe, 2012; Sovacool & Hess, 2017; Elbardan *et al.*, 2017). For this dissertation, a conceptual framework synthesis approach is the most fitting, as it supports the integration of cyberprivacy, cybersecurity, and smart grid models and strategies, and enables the development of a unified framework for protecting critical infrastructure. Following the guidelines and recommendations of Carroll *et al.* (2013) and Schryen (2015), and incorporating the main elements of a conceptual framework synthesis, the synthesis proceeds in six steps as follows:

1. Identifying and choosing a suitable IS framework or model. Here, the Socio-Technical Systems (STS) framework is selected as the general synthesis model, as it combines technical subsystems (hardware and software, content,

and Human-Computer Interface (HCI)), social subsystems (people, workflow and communication, organizational policies and culture, and external environment), and joint optimizations (measurements and monitoring) (Baxter & Sommerville, 2011; Sittig & Singh, 2010).

2. Defining a priori constructs by breaking the model into key dimensions, such as privacy controls, grid resilience, threat vectors, and policies.

3. Deductively coding studies and mapping findings to the a priori constructs – applying top-down reasoning (Okoli, 2023)

4. Inductively analyzing findings and insights not covered in the deductive phase to generate new themes, relationships, and sub-constructs – using bottom-up reasoning (Okoli, 2023)

5. Refining and extending the framework by merging constructs and elements and integrating emerging sub-constructs to reflect both a priori and inductively derived concepts.

6. Examining and interpreting the expanded framework by mapping relationships and explaining how the resulting conceptual model addresses the phenomena of interest.

In Figure 11, the entire adopted research approach is illustrated.

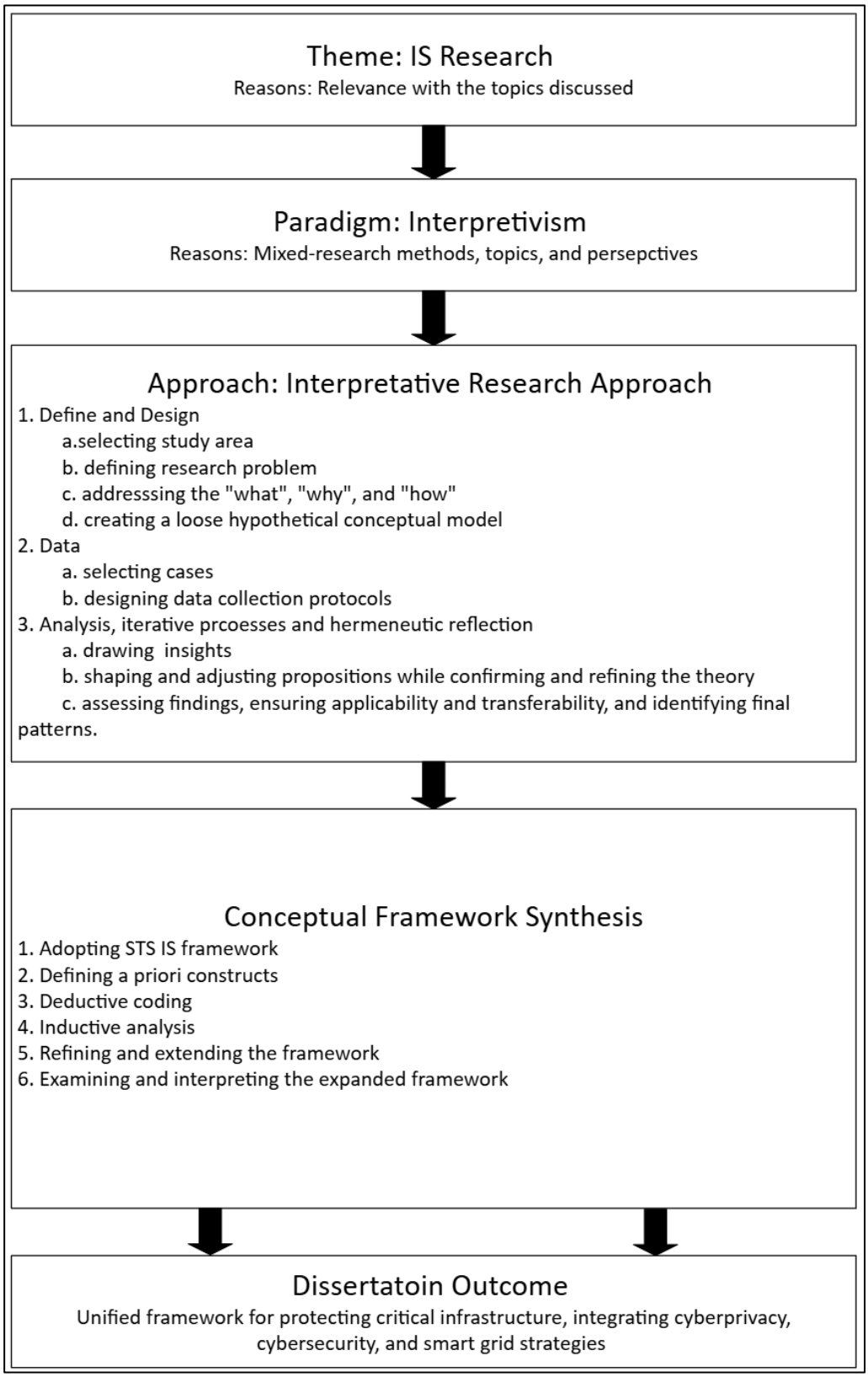


Figure 11. Overview of the detailed research approach and methodology adopted.

3.4 Research methods

This dissertation comprises articles that employ various research methods. An overview of these methods follows.

3.4.1 Literature review

A literature review is a fundamental part of the research process, used for gathering existing knowledge relevant to a topic under investigation, helping researchers become familiar with prior work and identify gaps for future directions (Cronin *et al.*, 2008; Randolph, 2009). According to Hart (2018), a literature review can be defined as "*the selection of available documents (both published and unpublished) on the topic, which contain information, ideas, data and evidence written from a particular standpoint to fulfill certain aims or express certain views on the nature of the topic and how it is to be investigated, and the effective evaluation of these documents in relation to the research being proposed*".

Different types of literature review exist, with the main ones employed in this work are as follows:

1. Narrative (also called traditional or conceptual) review: it is a process that aims at summarizing a synthesizing body of literature and secondary data sources to draw conclusions without being systematic or following a strictly structured approach (Cronin *et al.*, 2008; Tshabangu *et al.*, 2020; Nundy *et al.*, 2022). The review is typically selective and may reflect author bias and the criteria for selecting sources are not always clear to the reader. This type of review does not always start from a specific research question, only a topic of interest, as the primary purpose is to provide a comprehensive background and highlight the significance of the topic or selected points.

2. Systematic review: it is a rigorous and well-defined process that investigates a large body of literature comprehensively by employing strict structures and protocols, including narrowly defined research questions, assessed data sources, detailed time frames, explicit criteria for inclusion and exclusion, and clear methods for evaluating and synthesizing findings (Cronin *et al.*, 2008; Grant & Booth, 2009). This approach helps avoid any personal and subjective biases while covering the topic of interest. Several protocols already exist for conducting a systematic literature review, in which Kitchenham *et al.*'s (2009), Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) reporting protocol (Moher *et al.*, 2010), and Okoli & Schabram's (2015), each with their detailed checklists and flowcharts, provide structured

guidance and help ensure transparency and rigor throughout the entire review process.

3. Rapid review: it is a process that adapts the systematic review process but in a faster and more flexible form by omitting certain steps and simplifying strict criteria for searching literature, assessing quality, and applying multiple screenings (Smela *et al.*, 2023; Hamel *et al.*, 2021; Grant & Booth, 2009). Rapid reviews are mainly intended for producing timely evidence and general conceptual understanding, rather than offering an exhaustive or deeply detailed coverage of a topic. Still, by clearly outlining the method used, the approach manages to address bias and selectivity in a structured way, even if not as thoroughly as in systematic review.

3.4.2 Design science

Design science is an approach that focuses on the conceptualization and creation of innovations, ideas, practices, and technical capabilities through the analysis, design, implementation, management, and use of information systems (March & Smith, 1995; Hevner *et al.*, 2004). It follows a problem-solving methodology in which the created artifacts are developed to address specific problems and improve existing conditions within a defined context. Design science is inherently iterative, involving a cycle of structured steps: problem identification, definition of objectives, design and development, demonstration, evaluation, and finally, communication of the solution (Peffers *et al.*, 2007). These steps are repeated as needed, allowing the solution to emerge and gradually converge through refinement until it becomes implementable and effective.

3.4.3 Qualitative research

Qualitative research is a methodology that focuses on understanding complex phenomena and providing in-depth meaning through the contextual study of experiences, events, and cases (Lim, 2025). According to Aspers and Corte (2019), qualitative research is an "*iterative process in which improved understanding to the scientific community is achieved by making new significant distinctions resulting from getting closer to the phenomenon studied*." The approach employs various data collection and analysis methods, including interviews, observations, workshops, panel sessions, document-based comparisons (Greckhamer *et al.*, 2018), and similar formats, to generate rich, detailed data that support pattern identification and theme interpretation (Thoring *et al.*, 2020). The main characteristics of qualitative research include attention to data quality, a multi-phase process with iterations between

theory and evidence, and direct engagement with the phenomena under study, which together contribute to an improved understanding of the underlying conditions and outcomes.

3.4.4 Reasoning

The articles included in this dissertation apply different forms of reasoning that guide how data is analyzed and knowledge is built (Okoli, 2023), as follows:

1. Inductive (bottom-up) reasoning involves combining specific cases, observations, conclusions, or pieces of literature to draw a general rule or create collective insights. This approach is widely used in research; however, induction does not guarantee that the final conclusion is true or valid, only that is probable.

2. Deductive (top-down) reasoning, in contrast, applies general cases, rules, theories, or principles to specific instances to generate applicable insights. This approach relies mostly on established and validated knowledge and does not create predictions or new knowledge, yet guarantees that conclusions are logically sound and true.

3. Abductive reasoning (Thagard & Shelley, 1997) uses existing knowledge or theories alongside incomplete observations or poorly defined cases to form explanatory hypothesis that aid understanding and decision-making. Abduction is a "*may be*" process and often leads to the creation of new ideas.

3.5 Data collection and articles methodologies

Finally, data were collected in various formats and settings depending on the specific focus of each article or project task. To summarize, Table 1 shows the data sources for each article, the methodologies adopted, and associated reasoning.

Table 1. Data collection, methodologies, and reasoning.

Article	Data sources	Methodology	Reasoning
1	Secondary data, from reports, standards, and scientific publications	Narrative review	Inductive
2	Secondary data, from reports, standards, and scientific publications	Systematic literature review	Inductive

Article	Data sources	Methodology	Reasoning
3	Primary data, from university courses and curricula	State of the art (Systematic literature review)	Inductive (assessing courses) and deductive (applying educational frameworks)
4	Primary and secondary data, from reports, standards, scientific publications, workshops, and discussions	Design science	Inductive (assessing requirements) and deductive (applying design science principles)
5	Primary and secondary data, from reports, standards, scientific publications, workshops, and discussions	Multi-method qualitative (Rapid review + Qualitative workshops)	Inductive
6	Secondary data, from reports, standards, and scientific publications	Multi-method qualitative (Narrative review + Systematic literature review)	Inductive
7	Secondary data, from reports, standards, and scientific publications	Qualitative (Narrative comparative analysis)	Inductive (deriving broad directions and thematic insights) with abductive elements (crafting the roadmap)
8	Primary and secondary data, from reports, standards, scientific publications, workshops, and a panel session	Multi-method qualitative (Narrative review + Qualitative case study)	Inductive (assessing case studies) and deductive (applying frameworks)

4 SUMMARY OF ARTICLES

This chapter briefly summarizes the articles compiled for this dissertation. Each of the following sections presents the main research goals, conducted methodology, key findings, results, and contributions of the scientific article. As a reminder, please refer to Figure 1 in Chapter 1 for the specific research sub-questions and their relationship to each article.

4.1 Overview on how to preserve privacy

The first article, titled "*Unified Information Privacy Preserving Model,*" examines security and privacy frameworks, using a narrative and conceptual analysis approach. The article stresses the importance of privacy to individuals and organizations, highlights the growing reliance on communications and digital technologies, and emphasizes the need for a robust unified security and privacy standardization to keep systems safe and well-secured while ensuring functionality, controllability, and the users' right to privacy. The article reviews key concepts related to security and privacy, pointing out the main shortcomings in current deployments. It then broadly describes privacy and associated complexities and proposes a set of solutions addressing various aspects discussed. The main outcome of this work is the introduction of a unified information privacy preserving model, accompanied by a set of technical recommendations to support its implementation.

Safety, security, and privacy are three related concepts that fall under the broader umbrella of protection. Safety concerns keeping systems free from unintentional harm and accidents, while security deals with intentionality – ensuring systems remain free from danger and threat. Security is categorized into personal, operational, communications, networks, and information security, which is the main focus of this article. To secure information, classical security models emphasize confidentiality, integrity, and availability measures, while the Parkarian Hexad model introduces additional measures such as utility, possession, and Authentication, Authorization, and Access control (AAA) concepts. The ISO model further includes non-repudiation, supported by logging, as an essential parameter for communication and the security of operations. These factors collectively – if well implemented – can ensure information security. However, existing security implementations suffer from fragmented standardizations and best practices, compatibility issues with legacy and outdated systems, and that the security structure is independent of the end-user. On a higher level, privacy concerns protecting entities' data from being disclosed or connected, revealing private details and activities that should be kept private. Privacy elements include identity, time, location and mobility, type of activity, exchanged

traffic, involved parties, and other identifiers. Privacy is about determining who is allowed to access an entity's data and under what conditions that access is permitted. The article presents three theories on protecting privacy: control theory, which relies on individuals managing their own information; restricted access theory, which enforces privacy through secrecy, anonymity, and isolation; and control/restricted access theory, which argues that complete control of information in cyberspace is unfeasible, and that privacy should rather be ensured by allowing the right entity to access information at the right time.

The article then discusses the main privacy relationships, including pseudonymity, anonymity, unlikability, unobservability, and undetectability. These relationships define different privacy levels, ranging from level 1 (provably exposed) to level 6 (absolute privacy). The latter, however, is unrealistically achievable, and most implementations aim for level 5 (beyond suspicion) or at least level 4 (probable innocence). The article further examines key challenges to information privacy, including the rights and responsibilities of different parties involved in communication (first – senders, second – receivers, third – operators, and fourth – the public), as well as cultural, organizational, structural, legal, and operational conflicts related to privacy protection. These include issues related to crime prevention, standardization inconsistencies, efficiency trade-offs, complexity, and increased costs associated with privacy systems and enforcement.

The article concludes by proposing a conceptual framework for protecting information privacy, structured around three core principles. First, ensuring security, which involves applied security measures, standardizations, compatibility, and basic and essential responsibilities such as policies, transparency, accountability, and safety measures. Second, ensuring privacy, which builds on security while incorporating privacy relationships and control mechanisms, i.e., configurability, anonymity, and traceability. Third, enhancing information privacy by integrating privacy-enhancing tools and embedding privacy and security into the core design of devices and applications.

4.2 Cyberprivacy and its elements

The second article, titled "*Understanding Cyberprivacy: Context, Concept, and Issues,*" focuses on the concept of cyberprivacy, breaking it down to its core elements through conducting a systematic literature review of the topic and closely related ones. The article raises concerns about cyberprivacy and the importance of protecting privacy in digital environments, highlighting that the literature on this topic is fragmented due to its multidisciplinary nature and that it is often confused with cybersecurity. It

emphasizes the need for a thorough understanding of cyberprivacy to better address its issues. The article reviews and analyses 79 selected articles on the topic published between 2008 and 2021, showing that cyberprivacy is centered around eight contexts and revealing the issues associated with each. Finally, it proposes four meta-level definitions to better reflect on cyberprivacy. In addition to these definitions, the main contribution of this work is enhancing and supporting the understanding of cyberprivacy by covering it collectively and holistically. The article also identifies gaps and suggests future research directions, including digital transformation practices, ICT and cyberprivacy in the energy sector, and cyberprivacy in education.

With rapid digitalization, the distinction between individuals as physical organisms with their own rights and their digital identities and capabilities is blurring. The right to privacy is a fundamental right recognized by laws and constitutions. Yet, there is no universal agreement on its scope and context. Similarly, there is no common understanding of the term cyberprivacy and what it entails. Entities have the right to protect their data, but data also brings benefits such as improving efficiency, system optimization, and user experience. This creates a dilemma regarding what should be private and what can be shared publicly. The key issue lies in how data is handled and the capabilities of existing technologies in extracting PII and identifying patterns about users' behavior and their activities against their will. Even with cybersecurity measures in place, cyberprivacy extends beyond security practices, encompassing technical, legal, societal, and cultural dimensions.

The analysis of the reviewed publications reveals eight contexts associated with cyberprivacy: technology, legislation and right, ethics and morality, business and economy, risk and insurance, behavior and psychology, societal, and medical. Each context addresses cyberprivacy differently, sometimes leading to conflicting views. The technology context challenges cyberprivacy through advances in tracking, processing, knowledge discovery, sensing, and mixed reality technologies. The legislation context presents dilemmas such as balancing personal and governmental rights in accessing data and emphasizes that consent, control mechanisms, accountability measures, and law enforcement are the key to achieving cyberprivacy. The ethical context debates that cyberprivacy is a personal right, yet too much privacy could lead to misuse and unethical activities, hence the need for balancing cyberprivacy rights and adopting the concept of moral mediators. The economic context sees data as essential for business operations to optimize services and meet demands, emphasizing data ownership rights and the broader concept of trust. For the risk context, cyberprivacy is an intangible risk, which makes it difficult to address. However, attempts to frame cyberprivacy as intellectual property and quantify privacy risks by assigning them monetary value help address these risks more effectively. The psychological context focuses on shifts in cyberspace related to

identity, self-expression, and behavior, redefining harm and violence more in emotional and social terms. Accordingly, emphasis is placed on raising awareness and the use of psychological mediators to shape reasoning about actions and behavior. From a societal perspective, individuals have the right to be left alone and the right to social interaction. Societal norms should balance these rights while recognizing that privacy may have different meanings in different contexts. Finally, in the medical sector, data is vital as it drives improvements and accurate diagnosis, making trust and authorization critical factors to protect cyberprivacy.

The article proceeds by proposing four definitions of cyberprivacy from technical, sociotechnical, rights-based, and legal perspectives. It then highlights key cyberprivacy challenges related to technological advancements in storage, processing and recognition, communication, and knowledge discovery techniques. To address these, the article introduces a five-layer model comprising behavior, law, field of application, security and risk management, and privacy-enhancing mechanisms. The article concludes by emphasizing that cyberprivacy solutions must be considered holistically rather than separately.

4.3 Cybersecurity and smart grid education

The third article titled, "*State of the Art in Cybersecurity and Smart Grid Education,*" investigates the status of cybersecurity in smart grid education through a systematic literature review combined with educational study offering analysis. The article highlights the significance of smart grid skills and the need for specialized training in the field of cybersecurity to support ongoing development initiatives. It reviews policies and strategic directions, industry requirements, and ongoing research. It then examines education in smart grids and cybersecurity within higher education study programs, continuing education programs, and Massive Open Online Courses (MOOCs) available on these topics. Finally, it provides a set of recommendations to enhance knowledge and awareness of cybersecurity and technological advancements. The main contribution of this work is building insights into cybersecurity education and its requirements to support the development of the energy sector.

Cybersecurity is recognized by the EU as a strategic digital capability due to its critical role in IT and OT systems. However, a major shortage of expertise and skills covering this capability remains. Recommendations emphasize strengthening cyber resilience, establishing common cybersecurity frameworks, supporting certification schemes, ensuring regulatory compliance, and promoting education and research in this field. Regarding energy, modern energy systems rely on IT and advanced technologies and

are connected to data networks. This creates new cyber threats that require upskilling operators to make them ready to handle these challenges. The article investigates these issues by assessing current strategic directions, available educational curricula, and identifying gaps that need to be addressed.

Research indicates that the EU is committed to enhancing its Digital Education Action Plan to foster a high-performing digital education ecosystem and develop the competencies needed for digital transformation. In the energy sector, EU research highlights that beyond standard cybersecurity measures, knowledge of real-time requirements, a combination of advanced and legacy technologies, and cascading effects is essential. The article stresses that awareness and education are key to meeting these needs. This includes training courses for C-level executives and managers, classical training, hands-on exercises, and online learning. It also reviews industry studies and recommendations, highlighting NIST's efforts in developing cybersecurity curricula and Body of Knowledge covering eight areas: data, software, component, connection, system, human, organization, and societal impacts.

From a research perspective, studies on cybersecurity education remain relatively limited, with existing work primarily relying on online learning platforms for delivering cybersecurity training. Key topics include: cyber infrastructure in energy systems, monitoring and awareness, privacy in the smart grid, critical infrastructure security, and robust control systems. The article examines how these topics are integrated in current educational offerings, showing that undergraduate programs provide basic cybersecurity courses, master programs offer more specialized training, while at the doctoral level, cybersecurity education is scarce. In continuing education programs, cybersecurity topics in smart grids are also limited, with only a few certifications covering them. Finally, MOOCs are gaining popularity and are already in use, but their coverage of cybersecurity differs drastically and often lacks the depth required by employers.

The article concludes with a set of recommendations to address the shortage of cybersecurity competencies, particularly in the energy sector. These include: designing curricula tailored to different needs and career levels, expanding online and distance learning courses to facilitate accessibility, addressing both general and industry-specific cybersecurity topics, integrating theoretical and hands-on training, collaborating with industrial partners, covering all cybersecurity domains equally – including advanced topics such as privacy, mandating cybersecurity courses in energy programs, and incorporating innovative learning approaches such as gamification and flipped learning to improve retention.

4.4 An educational strategy supporting cybersecurity in smart grids

The fourth article, titled "*Towards a Massive Open Online Course for Cybersecurity in Smart Grids – A Roadmap Strategy,*" continues investigating the skill gap of cybersecurity in smart grids through a design science research approach to support teaching and educational curricula addressing the topic. The article highlights the changes the energy sector has witnessed and the challenges facing smart grid development, including the lack of cybersecurity professionals and the shortage of cybersecurity training and education. It reviews educational methodologies and learning approaches to address this gap. It then investigates MOOC design approaches and instructional design models to find the most suitable way of addressing this educational gap for the greatest number of participants. Finally, it offers a detailed course design approach to cover the gap in cybersecurity knowledge related to smart grids. The main contribution of this work is providing a detailed MOOC structure and handy roadmap strategy for addressing this knowledge gap – and other knowledge gaps in other fields as well. An outcome of this article was the development of a MOOC course following the design approach presented in this article.

The energy sector has witnessed major changes, moving towards smart grids and digitalization. This, accordingly, has led to the sector being exposed to various threats related to data and the manipulation of its connected assets. Cybersecurity is recognized as one of the EU's critical digital capabilities due to its importance and role in protecting systems. Although tools and technology exist to counter threats, the issue remains prominent, mainly because specific issues related to the energy sector are not well-addressed, there is a lack of specialists and professionals in this field, and there is a lack of educational offerings that provide proper skills to fill this gap. The article emphasizes the need for upskilling and building knowledge through an educational approach, especially considering that 50% of cyber incidents, at least, result from human errors and a lack of adequate knowledge to apply concepts properly.

Educational methodologies and learning approaches play a key role in building knowledge and raising awareness. Traditionally, these were simple and few. However, with the current changes and the variety of topics and needs, these have evolved drastically. Currently, these include, but are not limited to, lecture-based, experiential, active learning, cooperative learning, flipped learning, inquiry-based, problem- and project-based learning, and gamification. Each of these methodologies differs in the targeted group, resources, delivery method, and level of retention aimed for. The article then discusses MOOCs as a means for course delivery that is easily

accessible and requires minimal resources to operate after its design, facilitating the dissemination of knowledge. MOOCs come in different types, the main ones being: extended – aiming for knowledge duplication; connective – aiming for knowledge creation; social – aiming for active participation and engagement; and transfer – aiming for learning and pedagogical transformation. The article moves on to discuss ways to design educational materials and curricula by applying learning theories of behaviorism, cognitivism, constructivism, and connectivism. Several instructional design models exist on this, including Bloom's taxonomy, Gagne's nine events model, the ADDIE model, Merrill's principles, and the system approach model. These models can be combined and used together as they mostly share the same core principles, with only minor differences in scope and application criteria. The article complements its approach by providing detailed elements and a syllabus to design a MOOC course for cybersecurity in smart grids. This includes learning objectives, the projected level of retention, approaches used, criteria to increase attention and engagement, assessment criteria, and much more. This is supported by the design of real-time simulation exercises as an innovative approach that could offer the hands-on training criteria that are highly required by the industry. Finally, a detailed strategy was provided to facilitate course delivery.

The article concludes with a discussion of the challenges faced during course design and implementation. These mainly involve matching resources, adjusting retention rates and accordingly the weight of the course, retaining students, ensuring engagement, and addressing technical challenges depending on the deployed environment and systems utilized. All in all, technical and specialized MOOCs offer a feasible and practical way to deliver knowledge in an accessible manner, as long as a careful and detailed structure is adopted.

4.5 Towards a social-cyber-physical model for the future power grid

The fifth article, titled "*Towards a Model for Assessing the Effects of Social-Cyber-Physical Threats on the Future Power Grid – Review and Workshop Results,*" focuses on threats targeting power grid systems through a rapid review and qualitative analysis approach. The article discusses ongoing changes in the energy system, highlighting increasing vulnerabilities, disruptive events, and the critical role of the power grid in society and the economy. It then argues for a future electrical power system model that considers threats and social factors alongside cyber and physical aspects. The article reviews existing power system models, identifying their applicability and limitations, before proposing a seven-domain system-of-systems framework for modelling the future power grid, its subsystems, and influencing factors. The main

contribution of this work is the proposed framework, which includes a detailed description of its subsystems and components, while also shedding light on behavioral and social aspects of power systems.

As the energy system transitions into a fully digitalized cyber-physical infrastructure, driven by evolving demands and sustainability incentives, its complexity and vulnerability increase. Disruptive events are a major concern, with energy systems becoming more attractive targets due to their critical social and economic roles and the current shifts in political power dynamics. Several models of power grid systems exist to understand, analyze, and model grid dependencies. However, when it comes to disruptive events, these models lack thorough consideration of the human and social factors, as well as challenges emerging from integrating cyber-physical systems with social networks and advanced technologies. The article addresses this gap by introducing a third social layer into current cyber-physical models, analyzing how future power systems and their associated risks are addressed.

The article then reviews key power grid system models, including ISO's SGAM, NIST's SGCM, and the Cyber-Physical Power Model. Among the limitations of existing models are their complexity, limited flexibility, segmented layered structures, weak interfacing and testing tools, interoperability constraints, and concerns related to cybersecurity, privacy, and regulation, as well as human error and behavioral factors. The article also examines the geopolitical landscape and how conflicts increasingly target critical infrastructure and energy systems to cause disruptions and interrupt services. Based on these challenges, it proposes a social-cyber-physical grid model that takes these issues into consideration, integrating seven interconnected domains of supply, demand, market, transmission-distribution infrastructure, control, social-cultural, and disruption systems. These domains are interdependent, each influencing the others through two-way interactions. The article further provides remarks and insights into adopting this model for future power grid development.

The article concludes by emphasizing the need to consider all contributing domains and factors when modelling power grid systems to enhance resilience and mitigate possible disruptions. Future work suggestions include examining intra- and inter-dependencies between infrastructure environments, analyzing cascading failures of critical components, and refining system descriptions within the proposed model.

4.6 Insights into industrial systems and industrial data privacy

The sixth article, titled "*Industrial Systems and Industrial Data Privacy – A Comprehensive Review,*" explores industrial systems and associated privacy issues

through a combination of narrative and systematic review methodologies with an explanatory synthesis approach. The article first examines industrial systems, highlighting their common types, features, and significance, before shifting to industrial data and its value. It then reviews and synthesizes 34 selected publications between 2017 and 2023, identifying key focus areas of industrial data and prominent issues and solutions emphasized in the literature. The main contribution of this work is categorizing industrial systems within different contexts, proposing a comprehensive definition of modern industrial systems, and developing comprehensive insights into industrial data privacy by addressing existing challenges and feasible solutions.

Manufacturing has undergone a major transformation in recent decades, driven by the convergence of advanced IT and OT technologies, efficiency incentives, and the strategic utilization of industrial data. Industrial systems play a critical role in this transition, providing the intelligence and control needed to meet these objectives. Examining the literature on industrial systems, the article finds a lack of a unified definition describing these systems, with existing definitions varying significantly by context and sector. The article proceeds by investigating the types of industrial systems, identifying ten broad types that most industrial systems fall within, and highlighting key characteristics shared by modern industrial systems, including integration, connectivity, complexity, distributed control, data driven operations, and a focus on efficiency, reliability, scalability, and resilience. Based on these insights, it proposes a comprehensive definition of modern industrial systems, addressing their evolving role in industrial environments.

Industrial data is central to advancing these systems, providing the foundation for their capabilities and holding significant value in maintaining consistency, utility, and competitiveness. However, its importance also makes maintaining the security and preserving the privacy of industrial data critical concerns. The reviewed publications indicate increasing attention to industrial data privacy since 2017, particularly in relation to emerging technologies such as IoT, Big Data, and Cloud computing. The article categorizes privacy research into eight interconnected themes, including privacy technology, security technology, Industry 4.0 and cyber physical Systems, cloud computing, Internet of Things, data analysis, artificial intelligence, and federated learning, showing the interdisciplinary and interconnected nature of the topic. It then highlights key challenges facing industrial data, such as data leakage, handling sensitive records, model learning, regulatory gaps, real-time performance limitations, scalability issues, the growing number of devices and data volumes, third-party risks, and increased costs. The article also underscores governance and technical solutions proposed in the literature, including regulatory enforcement, anonymization, data minimization, differential privacy techniques, decentralized

architectures, access control and encryption mechanisms, and technologies such as blockchain, edge computing, and federated learning.

The article concludes by synthesizing these challenges and solutions, highlighting open issues such as the continuous evolution of industrial systems and knowledge extraction techniques, the need for privacy-by-design measures, cost-effective privacy solutions, operator upskilling, and privacy-centric manufacturing approaches. It finally suggests that future research should focus on Privacy Enhancing Technologies (PETs), adaptive privacy frameworks, and addressing operational and computational constraints in privacy-preserving solutions.

4.7 Realizing cyberprivacy through privacy-by-design, GDPR, and ISO/IEC 27701

The seventh article, titled "*Realizing Cyberprivacy: A Comparative Study and Implementation Roadmap Based on Privacy by Design Framework, GDPR and ISO/IEC 27701,*" examines the GDPR and ISO/IEC 27701 through a combination of narrative review and qualitative comparative analysis. The article explores the concept of cyberprivacy and emphasizes the need for approaches that support its realization. It first outlines the theoretical background surrounding cyberprivacy, then examines the Privacy by Design (PbD) framework and establishes a connection between cyberprivacy and PbD principles. Finally, it analyzes how PbD is addressed in both the GDPR and ISO/IEC 27701 privacy extension, offering insights into their similarities, potential overlaps, and ways to navigate conflicts in application. The main contribution of this work is identifying a set of features and differences between the GDPR and ISO/IEC 27701 to guide application and decision-making and presenting a twelve-step implementation roadmap for achieving cyberprivacy.

As the technological landscape continues to evolve, new technologies and methods have introduced various benefits, yet have also intensified risks. These include monitoring, aggressive marketing, and the processing of personal data without agreement or consent. Previously, InfoSec measures guided by major cybersecurity standards, such as those from ISO/IEC, NIST, and ENISA, have long addressed data security and the CIA Triad. However, under current developments, personal and data privacy have remained only partially addressed. This is because InfoSec and cybersecurity approaches typically deal with raw data without considering its context and due to the rise of digital identity and its associated rights. Several efforts have been made to address data privacy, such as the EU Data Protection Directive, but these have proven outdated and insufficient. In response, the GDPR was introduced to modernize privacy controls and provide stronger protection, drawing

on legal and foundational concepts including PbD. Still, the GDPR remains broad and primarily compliance-oriented. ISO/IEC 27701 was then released to standardize privacy technologies and enhance ISMS through better data control and effective PIMS. However, this standard has seen limited adoption and offers only minimal guidance. The article focuses on these two standards to foster a more comprehensive understanding that can support their adoption and, in turn, the realization of cyberprivacy.

The article proceeds by introducing the dimensions of cyberprivacy, including its relevance to cyberspace, cybersecurity, data privacy, and PII. To reduce ambiguity and avoid terminology confusion, it presents definitions of cyberprivacy from technical, socio-technical, rights-based, and legal perspectives. It then explores the PbD framework and how it is addressed within the GDPR, building a hypothetical model that utilizes GDPR principles to achieve cyberprivacy. The article continues with a closer review of the GDPR, followed by an overview of the ISO/IEC 27xxx series, including ISO/IEC 27001 – ISMS, 27002 – code of practice for security controls, 27701 privacy extension, and related standards. A comparative analysis is then conducted, identifying detailed similarities and overlaps between the GDPR and ISO/IEC 27701. In line with this, the article highlights key features and differences between the two, along with potential challenges that may hinder adoption.

The article concludes by building on this combined understanding and proposes an implementation roadmap for cyberprivacy that incorporates elements from the GDPR and ISO/IEC 27701, outlining twelve detailed steps that integrate these concepts. Finally, the article emphasizes that realizing cyberprivacy requires additional supporting approaches and stresses that the GDPR and ISO/IEC 27701 are not interchangeable, but should be adopted together. Moreover, it recommends the integration of socio-technical theory and related approaches to address privacy in a more comprehensive manner than through technical and managerial perspectives alone.

4.8 Transitions of cybersecurity and sustainable energy

The eighth article, titled "*Resilient or Vulnerable Twin Transition? A Multi-System Perspective on the Intersection of Sustainability and the Electricity-Based Digitalized Energy System,*" examines the transformation of the energy sector through the twin transition by combining narrative and qualitative review approaches with a multi-system perspective analysis. The article investigates how cybersecurity and energy systems are represented in transitions research, explores the changing landscape and

its implications, and emphasizes the need to expand existing transition frameworks to address these changes. The article first examines existing transition literature, frameworks, and practices of both IT and OT. It then considers a multi-system perspective, drawing insights from a Nordic case study on the Electricity-Based Digitalized Energy System (EBDES). Finally, it complements the analysis with insights from semi-structured workshops and discussion sessions. The main contribution of this work is supporting transition research by addressing the intersections of digitalization and security in energy systems, and examining the role of system interactions in shaping the twin transition.

As the European Union focuses on sustainability and green transition goals, it recognizes the importance of digitalizing energy systems and shifting towards electricity-based energy. This twin transition – combining sustainability and digitalization – has been reshaping the energy sector, introducing new technologies, capabilities, and opportunities while also creating new risks. This transition is not only a technical transition, but rather a socio-technical one that blends societal norms with technical practices. Despite the wide implications of this shift, the role of cybersecurity in socio-technical energy transitions remains underexplored. The article addresses this gap by examining system-wide changes and new dynamics within the energy system to understand such a socio-technical transformation. It emphasizes that this transformation occurs along with the simultaneous evolution of various interconnected STS, thus requiring a comprehensive and holistic approach to address it. The article then analyzes the contributing factors of this transformation, emphasizing the growing importance of energy and digitalization in transition research and introducing Geels' Multi-Level Perspective (MLP) framework to visualize the emergence of innovations, pressure impacts, and established regime transformations. It then highlights the role of IT and OT convergence, driving the evolution of energy systems, and explores the shift towards EBDES. Following this, it discusses the changing cybersecurity landscape, underscoring the importance of energy system cyber resilience while recognizing the new risks being introduced.

The article proceeds by introducing Breitschopf's Multi-System Interactions (MSI) framework to explore how STS interactions influence transitions. The framework involves identifying system interfaces, defining relationships, assessing system impacts, and evaluating interaction intensities over time. For the application of the framework, the Nordic EBDES case, including studies of the Nordic energy sector and workshops with energy experts, was used. The analysis reveals a range of insights, including – but not limited to – interfaces involving actors, institutions, infrastructure, technologies, knowledge, and resources; structural, functional, and competitive relationships; intensifying interactions; and inter-, intra-, and transformative impacts. These findings highlight how EBDES is reshaping electricity systems and the

whole energy sector in ways that increasingly resemble ICT structures. Workshop and semi-structured discussion sessions reinforced findings and provided empirical insights, focusing on the evolving technical and legal dimensions, growing regulatory complexity, emerging risks from IT and OT convergence, and socio-cultural challenges such as fairness, human-related risks, and awareness needs.

The article concludes by discussing the findings and building a shared understanding of the transition based on the applied framework and empirical insights. It emphasizes the complexity of the transformation and the importance of multi-perspective research that addresses its various components in depth. Finally, it suggests future research directions, including technological developments and studying the implications of the new NIS2, Critical Entities Resilience (CER), and Cyber Resilience Act (CRA) for the energy sector.

5 CYBERPRIVACY, CYBERSECURITY, AND SMART GRIDS – AN INTEGRATIVE APPROACH

This chapter applies the conceptual framework synthesis approach introduced in Chapter 3 to integrate the domains of cyberprivacy, cybersecurity, and smart grid strategies into a unified model for protecting critical infrastructure. The synthesis follows a structured six-step process (Carroll *et al.*, 2013; Schryen, 2015), involving: 1) choosing a framework as the main analysis lens, 2) defining a priori constructs, 3) performing a deductive coding and mapping of literature to the constructs, 4) conducting an inductive analysis to identify new insights and themes, 5) refining the framework by merging constructs with the new findings, and, 6) examining and interpreting the expanded framework. The chapter is structured around this process, beginning with the analytical lens and progressing through the synthesis stages to the presentation of the integrated model.

5.1 Step 1 – Choosing a framework: Socio-Technical Systems Theory

As highlighted in Chapter 3, the Socio-Technical Systems model (STS) is chosen as the main lens for guiding the analysis and synthesis of findings. STS is a framework within the IS field that facilitates understanding of the relationships and interactions between technical subsystem, e.g., technology, systems, and processes, and the social subsystem, e.g., people, organizations, cultures, and structures (Baxter & Sommerville, 2011; Sittig & Singh, 2010). Figure 12 shows the STS framework and how its different dimensions are interrelated (Dang & Vartiainen, 2024). STS suggests that the social and technical domains are not distinct but rather interdependent. The theory emphasizes the dynamic and continuous interactions and the mutual influences between social and technical dimensions. In practice, the theory suggests that the design of the technical subsystem should take social considerations into account to reflect human and organizational needs. Likewise, it suggests that the social subsystem should be structured around technical capabilities to leverage technology effectively, support social processes, and avoid conflicts or disruptions. Figure 13 illustrates the main characteristics of the social and technical domains (Militello *et al.*, 2014). As shown in Figure 13, the area where both domains overlap is where joint optimization occurs, supported by measures as well as continuous evaluation and adaptation of both social and technical elements.

Clearly, STS is chosen as the analytical lens for its integration of social and technical dimensions, which aligns with this dissertation's focus on cybersecurity and cyberprivacy as socio-technical phenomena. This framework provides a useful

perspective for analyzing these topics, framing cybersecurity not merely as a technological issue but as a socio-technical challenge involving user behavior, organizational practices, and system design (Malatji *et al.*, 2019), and positioning cyberprivacy at the intersection of social norms, legal standards, and digital architectures (Knijnenburg *et al.*, 2022).

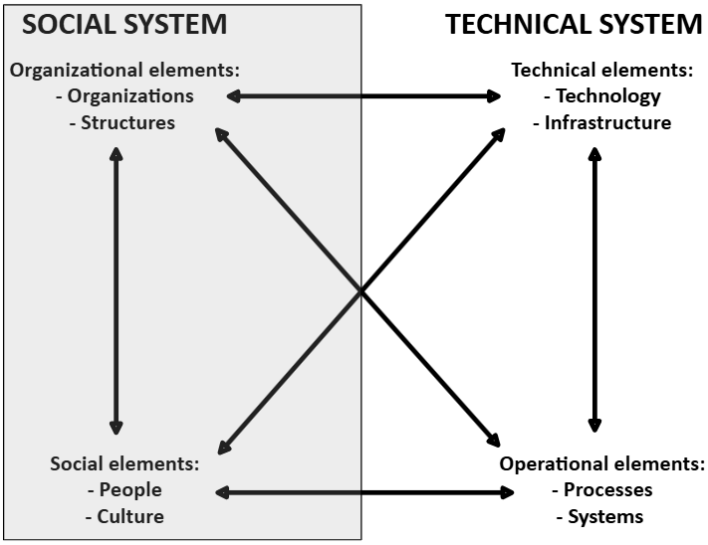


Figure 12. STS framework dimensions and their interconnections [adopted and edited from Dang & Vartiainen, 2024].

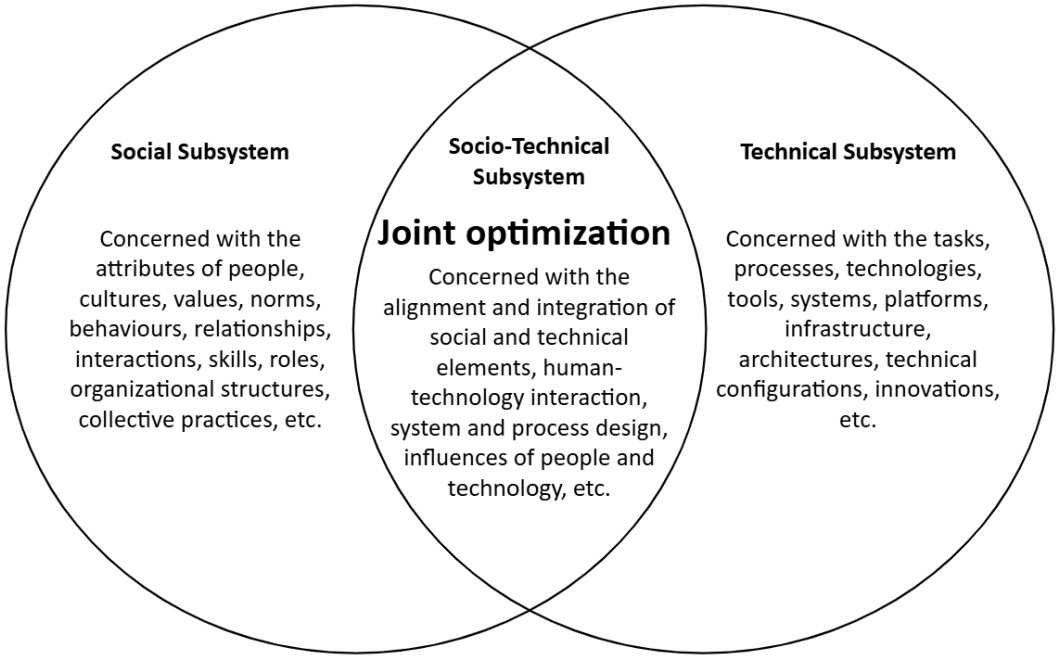


Figure 13. Key characteristics of the social, technical, and socio-technical domains [adopted and edited from Militello *et al.*, 2014].

5.2 Step 2 – Core elements of cyberprivacy, cybersecurity, and smart grids

Applying the STS framework to offer a multidimensional perspective, the key components of cyberprivacy, cybersecurity, and smart grids – drawn from ISO/IEC standards, the GDPR, NIST, SGAM, and SGCM – are categorized into the technical subsystem, social subsystem, and socio-technical subsystem, which captures the interactions and alignments between the two to support effective critical infrastructure protection. It is worth noting that some components may appear as constructs across different subsystems with different meanings and roles or as part of other constructs, and therefore might not always be identifiable as separate entities.

- Technical subsystem:
    - Privacy by Design, privacy-preserving technologies, and data protection mechanisms
    - data encryption, access control, and identity management
    - intrusion detection and prevention
    - logs and event management
    - grid automation and control systems
    - communication protocols and network security standards
    - hardware and software management
    - analytics and advanced detection algorithms and tools
    - cyber-physical systems and human-computer interaction
    - resilience technologies
    - digital twins and simulation models
- Social subsystem:
    - user knowledge, awareness, training, skills, behavior, and digital literacy
    - organizational culture and ethical norms

- regulatory, compliance, and governance frameworks
- communication, collaboration, and stakeholder engagement
- incident response, roles, and coordination
- policy enforcement and accountability

- Socio-technical subsystem: these components correspond to those outlined above and are presented in more detail in Section 5.2.4 as the explicit a priori coding categories for deductive coding.

5.2.1 Cyberprivacy

As highlighted in Chapter 2 and Articles 1, 2, 6, and 7, cyberprivacy refers to the protection and control of personal and organizational information within cyberspace and interconnected environments. In the context of smart grids and critical infrastructure, it involves protecting sensitive personal and operational data against unauthorized access, monitoring, or misuse, while ensuring transparency, consent, and control over data collection, use, sharing, processing, dissemination, and storage. This protection operates across legal, societal, technical, and socio-technical levels. For the deductive coding process, cyberprivacy is realized through a set of well-established theoretical and technical constructs identified from the GDPR, ISO/IEC 27701, and ISO/IEC 27001 and 27002, as shown in Table 2.

Table 2. Cyberprivacy constructs, explained.

Code	Construct	Definition
CP1	Privacy by Design	A framework for embedding privacy protection into systems from the design phase
CP2	Data minimization	A privacy principle that targets collecting only the necessary amount of data
CP3	Encryption and anonymization	Technical methods for protecting data through coding and removing identifiers
CP4	User consent and access control	Processes that ensure agreement on data collection and that only authorized entities can access data
CP5	Regulatory compliance	Ensuring adherence to privacy regulations and standards
CP6	Organizational privacy culture	The shared attitudes, values, and behaviors that prioritize and support privacy protection

5.2.2 Cybersecurity

As highlighted in Chapter 2 and Articles 1, 2, 4, 5, 6, and 7, cybersecurity encompasses the measures, policies, and practices implemented to protect information systems, networks, and digital assets from unauthorized access, accidental damage, disruption, and compromise of data integrity (NIST, 2018). Within energy systems, these measures cover both IT and OT environments. For the deductive coding, constructs are drawn from NIST and ISO/IEC 27001 and 27002, as presented in Table 3.

Table 3. Cybersecurity constructs, explained.

Code	Construct	Definition
CS1	Threat identification and risk assessment	A Process for finding potential threats, evaluating their impacts, and prioritizing protection efforts
CS2	Access control mechanisms	A technique and tools to limit which entities can access data, systems, and resources based on assigned permissions
CS3	Intrusion detection and prevention	Systems and procedures that monitor for unauthorized activities and prevent or mitigate threats
CS4	CIA Triad: Confidentiality, Integrity, and Availability	A security model defining the core goals for keeping data private, accurate, and accessible when needed
CS5	Regulatory compliance and technical standards	A set of legal requirements and best practices to maintain security
CS6	Security culture and governance	An organizational approach to support ongoing security efforts and security management

5.2.3 Smart grid strategies

As highlighted in Chapter 2 and Articles 3, 4, 5, and 8, smart grid strategies refer to the approaches, technologies, and policies used to modernize energy systems by integrating communication, automation, intelligence, and real-time operations to enhance the reliability, efficiency, security, and sustainability of power systems. For the deductive coding, key constructs are identified from NIST SGCM, ISO/IEC SGAM, and ISO/IEC 62351 – "*Cybersecurity for Energy Systems*" (Hussain *et al.*, 2019), based on the interdisciplinary nature of smart grids, which integrate electrical engineering, information technology, and socio-technical aspects, as described in Table 4.

Table 4. Smart grid constructs, explained.

Code	Construct	Definition
SG1	Advanced Metering Infrastructure (AMI) security	A framework for protecting smart metering systems and exchanged data
SG2	Distributed Energy Resources (DER) integration	A process for securely connecting and managing decentralized energy sources
SG3	Grid automation and control	A system and tools for monitoring, managing, and adjusting grid operations
SG4	Resilience and recovery mechanisms	Strategies and tools for overcoming disruptions and restoring operations
SG5	Regulatory frameworks	A set of rules and policies that guide a secure and reliable energy system operations
SG6	Consumer engagement	An approach for involving users in energy-related decisions, behaviors, and data sharing
SG7	Education and workforce development	Efforts to build knowledge and skills for maintaining secure energy systems

5.2.4 Socio-Technical (Joint optimization) subsystem

Finally, to address the interactions, alignment, and interfaces across the domains of cyberprivacy, cybersecurity, and smart grid strategies and to ensure their coordinated adoption for protecting critical infrastructure, socio-technical constructs identified from selected literature are presented in Table 5 for joint optimization. It is worth noting that this list covers general themes and is not exhaustive, as additional relevant constructs may exist beyond those captured here.

Table 5. Socio-technical joint optimization constructs, explained.

Code	Construct	Definition
ST1	Privacy-security balance and trade-offs (Porcedda, 2023; Viganò *et al.*, 2020)	An approach for managing tensions between protecting privacy and ensuring system security and associated benefits
ST2	Integration of cyberprivacy and cybersecurity controls within smart grid operations (Fhom & Bayarou, 2011; Leszczyna, 2018)	A strategy for embedding privacy and security measures into the functions of energy systems

Code	Construct	Definition
ST3	Socio-technical risk assessment and resilience strategies (Montoya-Rincon *et al.*, 2023; Clarke *et al.*, 2022)	A framework for evaluating risks across technical and social domains and associated adaptive response plans
ST4	Human-technology interaction in operational contexts (Voordijk & Dorrestijn, 2021; Aaltola, 2021)	An area of focus examining how people work with and respond to different systems to enhance both user experience and system performance
ST5	Cross-functional collaboration in threat intelligence and vulnerability management (Miryala & Gupta, 2022; Daniel & Victor, 2024)	A practice that brings different roles, departments, and sectors to share knowledge, respond to security risks, and plan protection strategies.
ST6	Alignment of regulations and technical standards (Paravano *et al.*, 2024; Shameem, 2024)	A coordination effort to ensure the effectiveness of legal and technical requirements without conflict
ST7	Continuous monitoring to ensure coordination between technical systems and organizational policies and practices (Beridze & Lomidze, 2024; Adams, 2024)	A procedure for regularly checking that technical operations remain aligned with organizational policies and practices

5.3 Steps 3 and 4 – Interconnections and interdependencies

5.3.1 Deductive coding

This section applies the deductive coding process to the compiled set of articles, using the a priori constructs identified in the previous section, as presented in Table 6.

Table 6. Deductive coding process.

Code	A1	A2	A3	A4	A5	A6	A7	A8
CP1						✓	✓	
CP2		✓				✓	✓	
CP3	✓	✓				✓	✓	
CP4	✓	✓	✓			✓	✓	
CP5	✓	✓				✓	✓	
CP6		✓					✓	
CS1				✓	✓	✓	✓	✓
CS2	✓		✓			✓	✓	
CS3						✓		
CS4	✓	✓	✓			✓	✓	
CS5	✓	✓	✓		✓		✓	✓
CS6		✓			✓		✓	✓
SG1			✓					✓
SG2					✓			✓
SG3			✓		✓			✓
SG4	✓		✓			✓		✓
SG5		✓	✓		✓			✓
SG6					✓			✓
SG7		✓	✓	✓		✓	✓	✓
ST1	✓	✓				✓	✓	
ST2	✓	✓	✓		✓	✓	✓	
ST3		✓			✓		✓	✓
ST4			✓	✓	✓			✓
ST5						✓	✓	✓
ST6	✓	✓					✓	✓
ST7		✓					✓	✓

The deductive coding of the eight articles against the a priori constructs reveals a clear emphasis on technical protection measures, while higher-order design and governance dimensions remain underexplored and require more consideration. Across the cyberprivacy domain, encryption and anonymization techniques, along with consent and access-control mechanisms, receive the most attention, indicating a consistent focus on protecting data confidentiality at the transaction level. However, foundational principles such as Privacy by Design and Data minimization are notably absent and governance-oriented constructs – including Regulatory compliance and Organizational privacy culture – remain under-addressed. This gap suggests that privacy protection has relied more on operational controls than on embedding privacy considerations into system lifecycles and corporate policies.

Similarly, in the cybersecurity domain, Threat identification and risk assessment, the CIA Triad, and Regulatory compliance emerge prominently. Yet, constructs related to continuous monitoring, such as Intrusion detection and prevention and Security culture and governance are underrepresented. The deductive process also noted a lack of standardization and conflicts, as emphasized in the CS5 construct. This pattern indicates a strong theoretical grounding in assessing potential threats but relatively limited attention to the operational processes and human-centered practices required for real-time detection, response, and recovery. For a resilient critical-infrastructure framework, it will be essential to integrate both strategic risk assessment and tactical incident-management capabilities.

Analysis of smart grid strategies highlights considerable attention given to Resilience mechanisms and Recovery planning, including redundant architectures, alongside targeted Educational and upskilling initiatives. In contrast, core infrastructure technologies such as Advanced Metering Infrastructure, Distributed Energy Resources, and Grid automation and control did not receive the expected attention. This may be because these technologies are highly specific, while the articles covered broader topics. This suggests that while system reliability and stakeholder participation and knowledge have been central concerns, there is room to deepen the analysis of underlying grid technologies to enable both security and performance improvements.

Finally, the socio-technical constructs are unevenly addressed. Privacy-security balance and Integration of cyberprivacy and cybersecurity controls within smart grid operations receive considerable attention, reflecting their critical importance. However, Socio-technical risk assessment and Alignment of regulations and standards could be examined more thoroughly. Human-technology interaction as in OT emerges as a significant topic, whereas Cross-functional collaboration and

Continuous monitoring receive the least attention, indicating a need for greater attention on these areas.

Taken together, the analysis highlights the necessity of integrating socio-technical constructs into the unified framework, as well as of embedding design-stage and governance constructs, such as Privacy by Design and Organizational privacy culture, to balance the focus on technical controls. The findings also reveal that the gap between strategic and operational risk assessment must be bridged and that the analysis should extend beyond resilience to include foundational and emerging technologies. Addressing these gaps will help ensure the final STS-informed model captures the full complexity of CIP from both technical and social dimensions.

5.3.2 Inductive coding analysis

Following the deductive coding process, it was clear that the a priori constructs covered most of the topics discussed in the articles. However, thorough inductive coding identified a few overlapping and additional patterns that extend beyond the a priori constructs, as presented in Table 7.

Table 7. Inductive coding process.

Theme	Coverage	Article
Architectural complexity beyond encryption	New	A1
End-user involvement in security architectures	New	A1
Protected zones as context-specific privacy domains	New	A2
Cyber-insurance for intangible privacy and cyber risks	New	A2
Emerging privacy-enhancing methods and technologies	New	A6
Sustainability and twin-transition nexus in cybersecurity and cyberprivacy	New	A5, A8
Privacy as user configurability and transparency	New	A1
Trust, transparency and ethics	Overlapping	A1, A2
Multi-perspective governance and social-cyber-physical risk	Overlapping	A2, A5
Education and training innovations	Overlapping	A3, A4
Multi-domain privacy conflicts	Overlapping	A1, A2
User-centric configurability and design	Overlapping	A1
Terminology ambiguity and taxonomy gaps	Overlapping	A2, A7

The inductive coding of the eight articles reveals several themes that extend beyond the a priori constructs, bringing novel dimensions and deepening the synthesis.

First, a set of new themes emphasizes emerging concerns around how architectural and contextual factors shape privacy and security. For example, Architectural complexity beyond encryption (A1) highlights that system heterogeneity introduces risks not captured by standard cryptographic measures. Similarly, End-user involvement in security architectures (A1) and Privacy as user configurability and transparency (A1) emphasize that concrete resilience and trust depend on interactive, user-centric controls rather than on back-end mechanisms. The notion of Protected zones as context-specific privacy domains (A2) further suggests that privacy protections can be tailored at certain levels, which challenges the one-size-fits-all assumption of many frameworks.

Second, themes such as Cyber-insurance for intangible privacy and cyber risks (A2) and Emerging privacy-enhancing methods and technologies (A6) point to financial and technical innovations that are not yet embedded in traditional models. The appearance of Sustainability and twin-transition nexus in cybersecurity and cyberprivacy (A5, A8) highlights a growing recognition that environmental and digital transitions interact, creating hybrid risk landscapes where energy transition and data protection intersect. These insights call for expanding the framework to include risk-transfer mechanisms and the relationship between sustainability goals and socio-technical security.

Third, several overlapping themes highlight areas where existing constructs lacked sufficient detail. Trust, transparency and ethics (A1, A2) and Multi-perspective governance and social-cyber-physical risk (A2, A5) reveal that governance must span ethical considerations, multi-stakeholder viewpoints, and the full cyber-physical spectrum. Education and training innovations (A3, A4) restates the importance of upskilling but introduces novel approaches beyond standard workforce development. Multi-domain privacy conflicts (A1, A2) and Terminology ambiguity and taxonomy gaps (A2, A7) highlight persistent tensions when policies for different domains clash and when the field lacks a thorough consideration of a unified vocabulary.

Taken together, these emergent themes indicate that the unified framework must not only integrate technical, social, and joint-optimization constructs but also accommodate dynamic architectures, financial and insurance instruments, sustainability interdependencies, and evolving educational and ethical dimensions. Incorporating these insights will ensure that the suggested model remains adaptable to emerging technologies, contextual nuances, and the complex governance landscapes characteristic of CIP.

5.4 Step 5 – Current gaps and challenges – The need for a new conceptual framework for CIP

From the deductive analysis, it is clear that existing frameworks focus heavily on technical protection measures while giving limited attention to higher-level design, governance, and socio-technical aspects – even though these were emphasized as important. This creates a noticeable gap between strategic risk assessment and operational incident management that remains unaddressed. The deductive phase also revealed a lack of consideration for foundational and emerging technologies, which could lead either to missed opportunities or to increased exposure to new risks stemming from them. The inductive analysis further emphasized this point by introducing new themes that centered on architectural complexity, user configurability, and deeper user involvement. It also pointed to governance-related challenges that span ethics, multi-stakeholder perspectives, and ambiguity in terminology. These themes underscore the need for more adaptable, inclusive, and future-aware approaches to CIP.

Furthermore, earlier research confirmed that existing CIP models often overlook several of the key aspects identified here – namely, privacy, integration, comprehensiveness, and adaptability to modern and emerging technologies. This is particularly apparent in models used within the energy sector, such as SGAM and SGCM, where similar shortcomings were found. Moreover, while standards like ISO/IEC provide a base for cybersecurity practices, they tend to function more for compliance checklists, offering only the bare minimum, with limited guidance and oversight.

These insights emphasize the need for a comprehensive, holistic, STS model for CIP that expands beyond technical and operational controls to address the current complexities and demands emerging across critical infrastructure.

5.5 Step 5 (continued) and Step 6 – Towards a unified framework for critical infrastructure protection

Drawing on the deductive and inductive analysis, as well as the current gaps and challenges identified, an **abstracted, conceptual** unified framework for critical infrastructure protection that addresses the current needs and integrating cyberprivacy, cybersecurity, and smart grid strategies is presented in Figure 14.

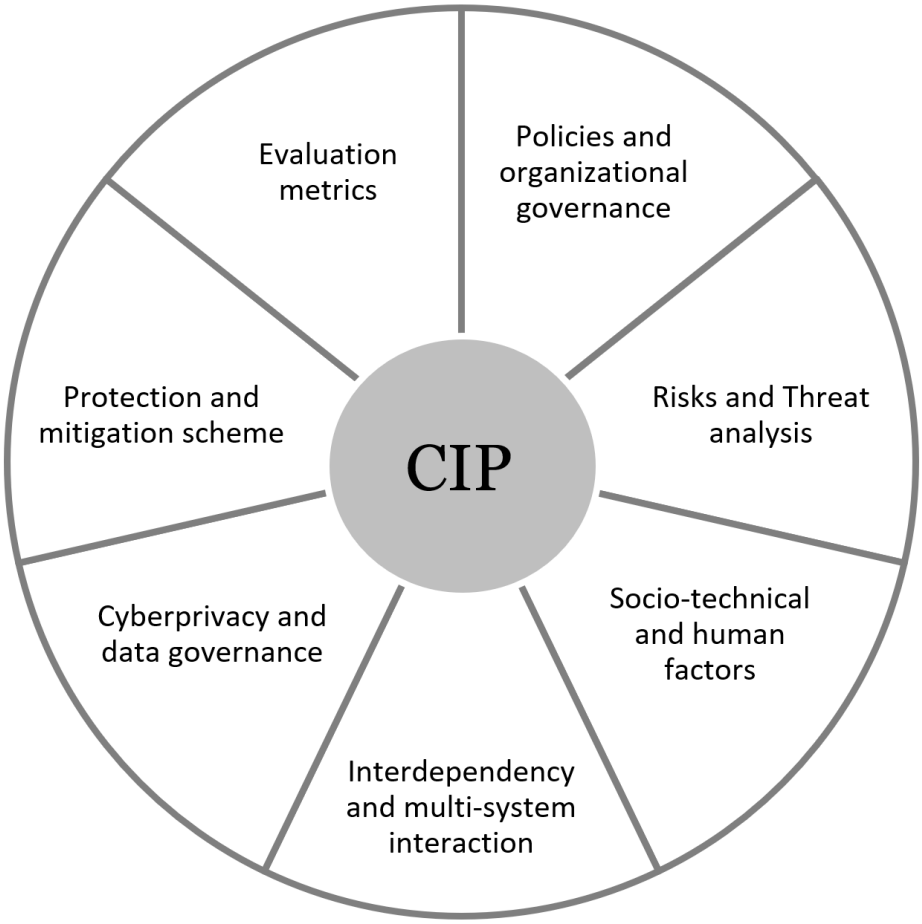


Figure 14. The proposed unified framework for critical infrastructure protection.

The proposed model builds on the holistic approach to enhancing CIP presented in Chapter 2 (Figure 9), incorporates the model developed in Article 5 for assessing social-cyber-physical threats of the future power grid, and draws on NIST's Cybersecurity Framework (CSF), the GDPR, and ISO/IEC 27001, 2, and 27701. It adopts the system-of-systems concept and spans seven domains, each of which may contain its own subdomains, as follows:

- Policies and organizational governance: This domain covers the formal rules, norms, commitment, and strategic directives shaping how an organization manages its obligations as well as risks.
    - Financial and insurance mechanisms: This reflects the need for risk-transfer strategies to complement internal controls and help absorb potential losses for recovery.

  - Sustainability nexus: This embeds environmental goals alongside resilience and digital security objectives to ensure supporting decarbonization and grid-stability requirements.

  - Ethics, transparency, and trust: This covers guiding principles and communication practices that help build stakeholder confidence and conformance through clear notices, ethical data handling, and accountability measures.

- Risks and Threat analysis: This domain provides systematic methods to identify, assess, and prioritize potential risks to proceed with the right controls.

  - Threat and vulnerability assessment: This combines identification of likely attack vectors, adversary capabilities, failure modes, gap analysis, and processes to uncover weaknesses.

  - Impact quantification and risk prioritization: This builds scenarios to quantify potential consequences and cascading effects to inform risk prioritization, adjust controls, as well as risk-transfer policies.

- Socio-technical and human factors: This domain explores the relationship between people, processes, and technology, reflecting on behavior and organizational culture affecting security, privacy, and protection outcomes.

  - Organizational security and privacy: This examines how organizational values and behavior influence adherence to controls and proactive risk practices.

  - Human-technology interaction and usability: This assesses ability to use OT systems effectively

  - Education and training innovations: This covers scenario-based education, micro-learning, and tools for upskilling and increasing engagement and retention.

- Interdependency and multi-system interaction: This domain provides understanding and insights on systems' connectedness and the transfer of attacks and failures to other systems

  - Dynamic architectural complexity: This addresses evolving system topologies and heterogenous components that may introduce new risk vectors beyond known ones.

- Cyberprivacy and data governance: This domain provides the policies, procedures, and controls for ensuring data is collected, stored, processed, and disposed of according to established legal requirements, privacy principles, and agreements.
    - Data lifecycle management: This ensures that that data is collected, stored, shared, archived, and deleted according to legal requirements, directives, and agreements.
    - Privacy-enhancing technologies: This provides advanced technical controls to protect data confidentiality while enabling data utilization and analytics.
    - Consent and user transparency: This provides mechanisms for configurability, consent, and data access-control.
- Protection and mitigation scheme: This domain provides the set of technical and operational controls designed to prevent, detect, and respond to risks and breaches.
    - Continuous monitoring and incident management: This involves real-time data, alert systems, and response actions that support swift detection, control, and recovery.
- Evaluation metrics: This domain provides the key performance indicators and measures used to track the effectiveness, efficiency, and resilience of overall the implemented framework, in addition to enabling continuous improvement.

5.6 Step 6 (continued)– Implications and Interpretation

The proposed model addresses the gaps in existing CIP approaches comprehensively by integrating concepts from cyberprivacy, cybersecurity, and operational continuity into a single socio-technical framework that spans governance, risk, human factors, and technical implementations. The model considers systemic and cross-sectoral interdependencies to ensure that both technical measures and human-organizational factors are well aligned for effective critical infrastructure protection. Rather than treating cyberprivacy, cybersecurity, and smart grid strategies separately, the model connects their concepts across seven interdependent domains. This integration enables a thorough understanding of the measures needed to protect critical

infrastructure and mitigate vulnerabilities that are not only systemic, but also organizational and behavioral, which are often overlooked.

While this model was built with smart grids and the energy sector as the core focus – given their central role in critical infrastructure – it was developed at a high level of abstraction. This was done to ensure that the concepts are clearly captured while remaining applicable across other critical infrastructure sectors. The intention was not to prescribe specific tools or solutions, but to maintain the model's comprehensiveness and adaptability. Lastly, although the framework does not explicitly show it, it is inherently cyclic, allowing for ongoing refinement and continuous improvement.

In summary, the proposed framework offers a practical foundation for researchers and practitioners seeking to examine and secure critical infrastructure in an increasingly digitalized and interconnected environment.

6 DISCUSSION AND CONCLUSIONS

This chapter completements the dissertation by discussing the work as a whole, presenting its contributions, limitations, future directions, and concluding remarks.

6.1 Discussion

This dissertation focused on implementing measures of cyberprivacy, cybersecurity, and smart grid strategies to protect critical infrastructure. It was designed to investigate threats and risks beyond the technical level, including human and organizational dimensions. Choosing cyberprivacy as a core concept provided a foundation for protection schemes, norms, legislation, and societal aspects. Cybersecurity, meaning technical security measures, was examined alongside the human factor, which clearly emerged as a gap across various studies. The smart grid strategies revealed the sector's reach across technical, social, legal, and organizational domains, showing that protecting critical infrastructure requires understanding their interconnections and interdependencies.

From these insights, a key takeaway of this dissertation is that fragmented solutions most likely will not work. In such interconnected environments, comprehensive, multidisciplinary, and multi-perspective approaches are needed to cover all protection aspects equally. The interpretative approach used in this dissertation gave the flexibility necessary for investigating such a complex topic. When combined with socio-technical systems theory, it provided insights and guidance unavailable from social or technical perspectives alone.

Building on this foundation, the integrative interpretative conceptual framework synthesis that guided the analysis and development of the proposed unified model proved effective. It offered insights into critical domains, their needs, and how to address them abstractly to allow reflection and generalization. The proposed model integrates seven interdependent domains, covering cyberprivacy, cybersecurity, operational continuity, governance, risk, human factors, and technical implementations, into a single socio-technical framework. This closes key gaps by bridging technical controls with organizational and behavioral factors. It supports a holistic understanding of critical infrastructure protection, highlighting systemic and cross-sectoral interdependencies that require adaptable, inclusive strategies capable of handling evolving risks and emerging technologies.

While built at a high level of abstraction, the model applies beyond the energy sector, supporting broader adoption and ongoing refinement. It shifts the focus from siloed solutions towards a cohesive and resilient approach aligned with current critical

infrastructure complexities. The dissertation shows that current protection initiatives often overlook these wider perspectives, focusing on specific risks without enough attention to interdependencies, cascading effects, or the people who operate or are affected by these systems.

In summary, this work offers a solid foundation for securing critical infrastructure in a digitalized and interconnected environment. It stresses the need for continuous improvement, cross-disciplinary collaboration, and approaches that go beyond technical fixes to include governance, human factors, and systemic complexity.

6.2 Results and overall contributions

This dissertation offers several theoretical and conceptual contributions:

- It provides a clear and systematic overview of the philosophy of science relevant to this research, including methods, paradigms, and stances, which clarifies the research process and enhances its rigor.
- It highlights the evolving dynamics of critical infrastructure protection, emphasizing the pressing need for comprehensive and integrated approaches that go beyond traditional technical solutions.
- It demonstrates the importance of cyberprivacy as a foundational concept, advocating for its inclusion in future protection schemes to address emerging challenges in digitalized infrastructures.
- It advances socio-technical systems research by systematically applying STS concepts to develop a more robust and context-aware model for critical infrastructure protection.
- It proposes a comprehensive, multi-domain model for critical infrastructure protection that addresses current challenges and fills significant gaps in existing frameworks, with potential applicability beyond the energy sector.
- It bridges conceptual theory with real-world challenges, opening new paths for future research and encouraging further exploration of integrated, adaptive protection strategies.

6.3 Limitations and future work

Although many limitations were addressed during this work, some remain:

- The focus was on the energy sector as a core critical infrastructure component. The proposed model was designed to be generalizable, but applying it to other critical infrastructure domains may require adapting technical descriptions to fit their specific nature and demands.
- The research primarily used qualitative methods aligned with the project tasks. Results would benefit from deeper statistical, numerical, and quantitative analyses. For example, conducting sensitivity analyses on cascading effects within specific critical infrastructures could strengthen findings.
- This work applied the socio-technical systems theory as its main theoretical lens. Incorporating additional theories could provide further insights to the synthesis. However, this should be approached carefully to avoid confusion or conflicting interpretations.

Future work includes:

- Studying privacy-enhancing technologies alongside advanced privacy methods, such as differential privacy.
- Applying Actor-Network Theory to better understand dependencies and interfaces between systems.
- Investigating the new ePrivacy directive in more detail to integrate it into the protection framework.
- Testing and refining the unified framework across different critical infrastructure domains to produce practical insights and adjustments.
- Developing further educational approaches beyond the current MOOC format and extracting insights from these initiatives.

6.4 Conclusion

This work addresses the urgent need for comprehensive critical infrastructure protection amid rapid digital transformation and increasing complexity. It demonstrates that conventional models, focused mainly on technical measures, fall

short in addressing the evolving interdependencies and socio-technical challenges inherent to sectors like energy. By developing a unified, multidisciplinary framework that integrates cyberprivacy, cybersecurity, and smart grid strategies across seven key domains, the work bridges critical gaps and offers a foundation for more resilient, inclusive protection approaches.

The framework's broad scope and abstraction make it applicable beyond the energy sector, supporting adaptable strategies that reflect real-world complexities and human factors. This approach shifts the focus to holistic protection that balances technical measures with governance, privacy, and organizational needs. Overall, the dissertation provides a foundation for ongoing research and practical advancements, emphasizing the need for continuous evolution in protecting critical infrastructure in an interconnected world.

POSTSCRIPT

First, I thought I was following an interpretivist approach, but I realized I might have mixed it with a constructivist approach without noticing. Luckily, that does not change any of the dissertation's results, since the two are closely related subjective approaches, with differences that are more philosophical than practical in this context.

Second, I planned to use the Actor-Network Theory to support the synthesis and generate further insights. However, while studying and trying to apply the theory, I realized it does not really fit the synthesis and analysis section, and that it probably should have been adopted much earlier, during the problem formulation phase. Since I was already at the final stage, and after realizing that the theory would not bring anything significant at this point, I had to discard it. Still, I have to admit that I learnt something useful from studying this theory, and I might – and should – apply it in future research, at the right phase this time.

That was it!

References

Aaltola, Kirsi. "Empirical study on cyber range capabilities, interactions and learning features." *Digital Transformation, Cyber Security and Resilience of Modern Societies* (2021): 413-428.

Adams, Ed. *See Yourself in Cyber: Security Careers Beyond Hacking*. John Wiley & Sons, 2024.

Admass, Wasyihun Sema, Yirga Yayeh Munaye, and Abebe Abeshu Diro. "Cyber security: State of the art, challenges and future directions." *Cyber Security and Applications* 2 (2024): 100031.

Agre, Philip, and Marc Rotenberg, eds. *Technology and privacy: The new landscape*. Mit Press, 1998.

Al-Ahmad, Walid, and Bassil Mohammad. "Addressing information security risks by adopting standards." *International Journal of Information Security Science* 2.2 (2013): 28-43.

Alcaraz, Cristina, and Sherali Zeadally. "Critical infrastructure protection: Requirements and challenges for the 21st century." *International journal of critical infrastructure protection* 8 (2015): 53-66.

Aspers, Patrik, and Ugo Corte. "What is qualitative in qualitative research." *Qualitative sociology* 42 (2019): 139-160.

Avenier, Marie-José, and Catherine Thomas. "Finding one's way around various methodological guidelines for doing rigorous case studies: A comparison of four epistemological frameworks." *Systèmes d'information & management* 20.1 (2015): 61-98.

Avgerou, Chrisanthi. "Information systems: what sort of science is it?." *Omega* 28.5 (2000): 567-579.

Barnett-Page, Elaine, and James Thomas. "Methods for the synthesis of qualitative research: a critical review." *BMC medical research methodology* 9 (2009): 1-11.

Bartholomew, Mark. "Intellectual Property's Lessons for Information Privacy." *Neb. L. Rev.* 92 (2013): 746.

Baxter, Gordon, and Ian Sommerville. "Socio-technical systems: From design methods to systems engineering." *Interacting with computers* 23.1 (2011): 4-17.

Berg, Petra, et al. "Towards a Model for Assessing the Effects of Social-Cyber-Physical Threats on the Future Power Grid – Review and Workshop Results." *2024 International Workshop on Artificial Intelligence and Machine Learning for Energy Transformation (AIE)*. IEEE, 2024.

Berghel, Hal. "Cyberprivacy in the new millennium." *Computer* 34.1 (2001): 132-134.

Berghel, Hal. "PII, the FTC, Car Dealers, and You." *Computer* 47.5 (2014): 102-106.

Beridze, Tamar, and Giorgi Lomidze. "A Policy-Centered Framework for Cybersecurity Management: Ensuring Information Assurance Through Governance and Oversight." *International Journal of Advanced Computational Methodologies and Emerging Technologies* 14.8 (2024): 1-13.

Biselli, Tom, and Christian Reuter. "On the relationship between it privacy and security behavior: A survey among German private users." *Innovation Through Information Systems: Volume II: A Collection of Latest Research on Technology Issues*. Springer International Publishing, 2021.

Boell, Sebastian K., and Dubravka Cecez-Kecmanovic. "What is an information system?." *2015 48th Hawaii International Conference on System Sciences*. IEEE, 2015.

Boiral, Olivier. "Managing with ISO systems: lessons from practice." *Long Range Planning* 44.3 (2011): 197-220.

Bouwmans, Ivo, Margot PC Weijnen, and Adrian Gheorghe. "Infrastructures at risk." *Critical Infrastructures at Risk: Securing the European Electric Power System*. Dordrecht: Springer Netherlands, 2006. 19-36.

Breaux, Ronald W., Emily Westridge Black, and Timothy Newman. "A guide to data protection and breach response-part 1." *Intellectual Property & Technology Law Journal* 26.7 (2014a): 3.

Breaux, Ronald W., Emily Westridge Black, and Timothy Newman. "A guide to data protection and breach response-part 2." *Intellectual Property & Technology Law Journal* 26.8 (2014b): 23.

Brunetti, Federico, et al. "Digital transformation challenges: strategies emerging from a multi-stakeholder approach." *The TQM Journal* 32.4 (2020): 697-724.

Campbell, Richard J. "The smart grid and cybersecurity: Regulatory policy and issues." Congressional Research Service, Library of Congress, 2011.

Carroll, Christopher, et al. ""Best fit" framework synthesis: refining the method." *BMC medical research methodology* 13 (2013): 1-16.

Chidukwani, Alladean, Sebastian Zander, and Polychronis Koutsakis. "A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations." *IEEE Access* 10 (2022): 85701-85719.

Christofi, Athena, et al. "Erosion by Standardisation: Is ISO/IEC 29134: 2017 on Privacy Impact Assessment Up to (GDPR) Standard?." *Personal data protection and legal developments in the European Union*. IGI Global, 2020. 140-167.

Clarke, Drew, et al. "Australian energy transition research plan: transition dynamics." (2022).

Cooper, Tom, Alex Faseruk, and Lewis D. Johnson. "IMPACT OF PRIVACY AND CONFIDENTIALITY ON VALUATION: AN INTERNATIONAL PERSPECTIVE." *Journal of Financial Management & Analysis* 23.2 (2010).

Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse. "Defining cybersecurity." *Technology innovation management review* 4.10 (2014).

Cranor, Lorrie, et al. "Towards a privacy research roadmap for the computing community." *arXiv preprint arXiv:1604.03160* (2016).

Cronin, Patricia, Frances Ryan, and Michael Coughlan. "Undertaking a literature review: a step-by-step approach." *British journal of nursing* 17.1 (2008): 38-43.

Cybersecurity, Critical Infrastructure. "Framework for improving critical infrastructure cybersecurity." *CSWP* 4162018.7 (2018). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST

Dang, Duong, and Tero Vartiainen. "Exploring Socio-technical Gaps in the Cybersecurity of Energy Informatics for Sustainability." *Adoption of Emerging Information and Communication Technology for Sustainability*. CRC Press, 2024. 288-304.

Daniel, Sontan Adewale, and Samuel Segun Victor. "Emerging trends in cybersecurity for critical infrastructure protection: a comprehensive review." (2024)

Dawadi, Saraswati, Sagun Shrestha, and Ram A. Giri. "Mixed-methods research: A discussion on its types, challenges, and criticisms." *Journal of Practical Studies in Education* 2.2 (2021): 25-36.

De Hert, Paul, Vagelis Papakonstantinou, and Irene Kamara. "The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection." *Computer Law & Security Review* 32.1 (2016): 16-30.

Delboni, Luiz FN, et al. "Electrical power systems: Evolution from traditional configuration to distributed generation and microgrids." *Microgrids design and implementation*. Cham: Springer International Publishing, 2018. 1-25.

Demchak, Chris C., and Kurt D. Fenstermacher. "Institutionalizing Behavior-Based Privacy." *Administration & Society* 41.7 (2009): 783-814.

Ding, Jianguo, et al. "Cyber threats to smart grids: Review, taxonomy, potential solutions, and future directions." *Energies* 15.18 (2022): 6799.

Disterer, Georg. "ISO/IEC 27000, 27001 and 27002 for information security management." *Journal of Information Security* 4.2 (2013).

Elbardan, Hany, et al. "An interpretive approach for data collection and analysis." *Enterprise resource planning, corporate governance and internal auditing: An institutional perspective* (2017): 111-165.

Elmaghraby, Adel S., and Michael M. Losavio. "Cyber security challenges in Smart Cities: Safety, security and privacy." *Journal of advanced research* 5.4 (2014): 491-497.

Eltahawy, Bahaa, et al. “Resilient or vulnerable twin transition? A multi-system perspective on the intersection of sustainability and the electricity-based digitalized energy system”. *Unpublished manuscript,* 2025.

Eltahawy, Bahaa, et al. “Realizing cyberprivacy: A comparative study and implementation roadmap based on privacy by design framework, GDPR, and ISO 27701”. *Unpublished manuscription,* 2025.

Eltahawy, Bahaa, and Duong Dang. "Understanding Cyberprivacy: Context, Concept, and Issues." *Wirtschaftsinformatik 2022 Proceedings*. 21. (2022). https://aisel.aisnet.org/wi2022/it_for_development/it_for_development/21

Eltahawy, Bahaa, and Reino Virrankoski. “Into a Unified Information Privacy Preserving Model”. *Proceedings of the International Conference on Communications, Computer Science and Information Technology (ICCCSIT)*, Dubai, United Arab Emirates, 12-14 Mar. 2016.

Eltahawy, Bahaa. “Industrial systems and industrial data privacy – A comprehensive review”. *Unpublished manuscript,* 2025.

Elzinga, David. "Electricity system development: A focus on smart grids. overview of activities and players in smart grids." *UNECE[Site]. URL: https://www. unece. org/fileadmin/DAM/energy/se/pdfs/eneff/eneff_h. news/Smart. Grids. Overview. pdf (accessed: 12.06. 2016)* (2015).

Erlinghagen, Sabine, and Jochen Markard. "Smart grids and the transformation of the electricity sector: ICT firms as potential catalysts for sectoral change." *Energy Policy* 51 (2012): 895-906.

Fang, Xi, et al. "Smart grid—The new and improved power grid: A survey." *IEEE communications surveys & tutorials* 14.4 (2011): 944-980.

Ferrag, Mohamed Amine, et al. "A systematic review of data protection and privacy preservation schemes for smart grid communications." *Sustainable cities and society* 38 (2018): 806-835.

Ferrão, Sâmmara Éllen Renner, et al. "Towards a taxonomy of privacy requirements based on the LGPD and ISO/IEC 29100." *Information and Software Technology* 168 (2024): 107396.

Fhom, Hervais Simo, and Kpatcha M. Bayarou. "Towards a holistic privacy engineering approach for smart grid systems." *2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE, 2011.

Foxman, Ellen R., and Paula Kilcoyne. "Information technology, marketing practice, and consumer privacy: Ethical issues." *Journal of public policy & marketing* 12.1 (1993): 106-119.

Froomkin, A. Michael. "The death of privacy." *Stan. L. Rev.* 52 (1999): 1461.

Ghelani, Diptiben. "Cyber security in smart grids, threats, and possible solutions." *Authorea Preprints* (2022).

Gopstein, Avi, et al. *NIST framework and roadmap for smart grid interoperability standards, release 4.0*. Vol. 10. Gaithersburg, MD, USA: Department of Commerce. National Institute of Standards and Technology, 2021.

Grant, Maria J., and Andrew Booth. "A typology of reviews: an analysis of 14 review types and associated methodologies." *Health information & libraries journal* 26.2 (2009): 91-108.

Greckhamer, Thomas, et al. "Studying configurations with qualitative comparative analysis: Best practices in strategy and organization research." *Strategic organization* 16.4 (2018): 482-495.

Gregg, Dawn G., Uday R. Kulkarni, and Ajay S. Vinzé. "Understanding the philosophical underpinnings of software engineering research in information systems." Information systems frontiers 3 (2001): 169-183.

Guba, Egon G., and Yvonna S. Lincoln. "Competing paradigms in qualitative research." *Handbook of qualitative research* 2.163-194 (1994): 105.

Hamel, Candyce, et al. "Defining rapid reviews: a systematic scoping review and thematic analysis of definitions and defining characteristics of rapid reviews." *Journal of clinical epidemiology* 129 (2021): 74-85.

Hart, Chris. "Doing a literature review: Releasing the research imagination." (2018): 1-352.

Hasan, Forat Falih. "A review study of information systems." *International Journal of Computer Applications* 179.18 (2018): 15-19.

Hasan, Mohammad Kamrul, et al. "Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations." *Journal of network and computer applications* 209 (2023): 103540.

Hayes, Brian. "Connecting the dots." *American Scientist* 94.5 (2006): 400-404.

Hemme, Kris. "Critical infrastructure protection: Maintenance is national security." *Journal of Strategic Security* 8.3 (2015): 25-39.

Hevner, Alan R., et al. "Design science in information systems research." *MIS quarterly* (2004): 75-105.

Hirschheim, Rudy, and Heinz K. Klein. "Four paradigms of information systems development." *Communications of the ACM* 32.10 (1989): 1199-1216.

Hirschheim, Rudy, Heinz K. Klein, and Kalle Lyytinen. *Information systems development and data modeling: conceptual and philosophical foundations*. Vol. 9. Cambridge University Press, 1995.
https://doi.org/10.22541/au.173822597.78031676/v1

Hussain, SM Suhail, Taha Selim Ustun, and Akhtar Kalam. "A review of IEC 62351 security mechanisms for IEC 61850 message exchanges." *IEEE Transactions on Industrial Informatics* 16.9 (2019): 5643-5654.

Iivari, Juhani, Rudy Hirschheim, and Heinz K. Klein. "A paradigmatic analysis contrasting information systems development approaches and methodologies." *Information systems research* 9.2 (1998): 164-193.

Kalogeraki, Eleni-Maria, and Nineta Polemi. "A taxonomy for cybersecurity standards." *Journal of Surveillance, Security and Safety* 5.2 (2024): 95-115.

Kerlinger, Fred Nichols. "Foundations of behavioral research." (1966).

Kitchenham, Barbara, et al. "Systematic literature reviews in software engineering–a systematic literature review." *Information and software technology* 51.1 (2009): 7-15.

Klein, Heinz K., and Michael D. Myers. "A set of principles for conducting and evaluating interpretive field studies in information systems." *MIS quarterly* (1999): 67-93.

Knapp, Eric D., and Raj Samani. "Chapter 4—Privacy Concerns with the Smart Grid." *Applied Cyber Security and the Smart Grid; Knapp, ED, Samani, R., Eds* (2013): 87-99.

Knijnenburg, Bart P., et al. *Modern socio-technical perspectives on privacy*. Springer Nature, 2022.

Kroeze, Jan H. "Interpretivism in Information Systems: A Postmodern Epistemology?." (2011).

Kumar, Shipra Ravi, et al. "Data-mining a mechanism against cyber threats: A review." *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)*. IEEE, 2016.

Lachaud, Eric. "ISO/IEC 27701 standard: Threats and opportunities for GDPR certification." *Eur. Data Prot. L. Rev.* 6 (2020): 194.

Lee, Chia-Yen, and Bo-Syun Chen. "Mutually-exclusive-and-collectively-exhaustive feature selection scheme." *Applied Soft Computing* 68 (2018): 961-971.

Lehto, Martti. "Cyber-attacks against critical infrastructure." *Cyber security: Critical infrastructure protection*. Cham: Springer International Publishing, 2022. 3-42.

Leszczyna, Rafał. "Cybersecurity and privacy in standards for smart grids–A comprehensive survey." *Computer Standards & Interfaces* 56 (2018): 62-73.

Levit, N. "Family privacy bibliography." *Journal of the American Academy of Matrimonial Lawyers* 17 (2009): 183-255.

Lim, Weng Marc. "What is qualitative research? An overview and guidelines." *Australasian Marketing Journal* 33.2 (2025): 199-229.

Lindquist, Jan. "Introducing privacy receipts into DLT and eIDAS." *Journal of ICT Standardization* 11.2 (2023): 117-134.

Loch, Karen D., Sue Conger, and Effy Oz. "Ownership, privacy and monitoring in the workplace: a debate on technology and ethics." *Journal of Business Ethics* 17 (1998): 653-663.

Magnani, Lorenzo. "Chapter Seven Knowledge as a Duty: the ethical significance of the interest in information and knowledge." (2007).

Magnani, Lorenzo. "Structural and technology-mediated violence: Profiling and the urgent need of new tutelary technoknowledge." *International Journal of Technoethics (IJT)* 2.4 (2011): 1-19.

Malatji, Masike, Sune Von Solms, and Annlizé Marnewick. "Socio-technical systems cybersecurity framework." *Information & Computer Security* 27.2 (2019): 233-272.

March, Salvatore T., and Gerald F. Smith. "Design and natural science research on information technology." *Decision support systems* 15.4 (1995): 251-266.

Markopoulou, Dimitra, Vagelis Papakonstantinou, and Paul De Hert. "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation." *Computer Law & Security Review* 35.6 (2019): 105336.

McChesney, Katrina, and Jill Aldridge. "Weaving an interpretivist stance throughout mixed methods research." *International journal of research & method in education* 42.3 (2019): 225-238.

Mertens, Donna M. *Research and evaluation in education and psychology: Integrating diversity with quantitative, qualitative, and mixed methods*. Sage publications, 2019.

Militello, Laura G., et al. "Sources of variation in primary care clinical workflow: implications for the design of cognitive support." *Health informatics journal* 20.1 (2014): 35-49.

Miryala, Naresh Kumar, and Divit Gupta. "Data security challenges and industry trends." *IJARCCE Int J Adv Res Comput Commun Eng* 11.11 (2022): 300-309.

Moher, David, et al. "Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement." *International journal of surgery* 8.5 (2010): 336-341.

Monti, Matteo, et al. *An alternative information plan*. Technical Report, Working paper Santa Fe Institute, 2017.

Montoya-Rincon, Juan P., et al. "A socio-technical approach for the assessment of critical infrastructure system vulnerability in extreme weather events." *Nature Energy* 8.9 (2023): 1002-1012.

Mosadeghi, Razieh, Russell Richards, and Rodger Tomlinson. "Critical Infrastructure Protection and Uncertainty Analysis." *HANDBOOK OF DISASTER RISK REDUCTION & MANAGEMENT* (2018): 193-223.

Moteff, John D., Paul Parfomak, and Resources, Science, and Industry Division. "Critical infrastructure and key assets: definition and identification." Washington: Congressional Research Service, Library of Congress, 2004.

Mukumbang, Ferdinand C. "Retroductive theorizing: a contribution of critical realism to mixed methods research." Journal of Mixed Methods Research 17.1 (2023): 93-114.

Nundy, Samiran, et al. "Systematic, scoping and narrative reviews." *How to Practice Academic Medicine and Publish from Developing Countries? A Practical Guide* (2022): 277-281.

Nweke, Livinus Obiora, and Stephen D. Wolthusen. "A holistic approach for enhancing critical infrastructure protection: Research agenda." *The International Conference on Emerging Applications and Technologies for Industry 4.0*. Cham: Springer International Publishing, 2020b.

Nweke, Livinus Obiora, and Stephen D. Wolthusen. "A holistic approach for enhancing critical infrastructure protection: Research agenda." *The International Conference on Emerging Applications and Technologies for Industry 4.0*. Cham: Springer International Publishing, 2020.

Nweke, Livinus Obiora, and Stephen Wolthusen. "Legal issues related to cyber threat information sharing among private entities for critical infrastructure protection." *2020 12th international conference on cyber conflict (cyCon)*. Vol. 1300. IEEE, 2020a.

Okoli, Chitu, and Kira Schabram. "A guide to conducting a systematic literature review of information systems research." (2015).

Okoli, Chitu. "A critical realist guide to developing theory with systematic literature reviews." *Available at SSRN 2115818* (2012).

Okoli, Chitu. "Inductive, abductive and deductive theorising." *International Journal of Management Concepts and Philosophy* 16.3 (2023): 302-316.

Paravano, Alessandro, Giorgio Locatelli, and Paolo Trucco. "Creating and claiming social value by joining the governance of science-driven capital projects: an investigation in the New Space Economy." *IEEE Engineering Management Review* (2024).

Pardini, Daniel Jardim, Astrid Maria Carneiro Heinisch, and Fernando Silva Parreiras. "Cyber security governance and management for smart grids in Brazilian energy utilities." *JISTEM-Journal of Information Systems and Technology Management* 14 (2017): 385-400.

Peffers, Ken, et al. "A design science research methodology for information systems research." *Journal of management information systems* 24.3 (2007): 45-77.

Phillips, John T. "Privacy vs. cybersecurity." *Information Management* 36.3 (2002): 46.

Platform, S. G. E. T. "Smartgrids-strategic deployment document for european electricity networks of the future." *Available online, April* (2010).

Plekhanov, Dmitry, Henrik Franke, and Torbjørn H. Netland. "Digital transformation: A review and research agenda." *European management journal* 41.6 (2023): 821-844.

Poleto, Thiago, et al. "Information security applications in smart cities: A bibliometric analysis of emerging research." *Future Internet* 15.12 (2023): 393.

Ponelis, Shana R. "Using interpretive qualitative case studies for exploratory research in doctoral studies: A case of information systems research in small and medium enterprises." *International journal of doctoral studies* 10 (2015): 535.

Porcedda, Maria Grazia. "Cybersecurity, Privacy and Data Protection in EU Law." (2023): 1-352.

Pretorius, Lynette. "Demystifying research paradigms: Navigating ontology, epistemology, and axiology in research." *The Qualitative Report* 29.10 (2024): 2698-2715.

Randolph, Justus. "A guide to writing the dissertation literature review." *Practical assessment, research, and evaluation* 14.1 (2009).

Rinaldi, Steven M., James P. Peerenboom, and Terrence K. Kelly. "Identifying, understanding, and analyzing critical infrastructure interdependencies." *IEEE control systems magazine* 21.6 (2001): 11-25.

Roshanaei, Maryam. "Resilience at the core: critical infrastructure protection challenges, priorities and cybersecurity assessment strategies." *Journal of Computer and Communications* 9.8 (2021): 80-102.

Roshanaei, Maryam. "Resilience at the core: critical infrastructure protection challenges, priorities and cybersecurity assessment strategies." *Journal of Computer and Communications* 9.8 (2021): 80-102.

Rossman, Gretchen B., and Sharon F. Rallis. *Learning in the field: An introduction to qualitative research*. Sage, 2011.

Rowe, Frantz. "What literature review is not: diversity, boundaries and recommendations." *European journal of information systems* 23.3 (2014): 241-255.

Rowlands, Bruce H. "Grounded in practice: Using interpretive research to build theory." *Electronic Journal of Business Research Methods* 3.1 (2005): pp81-92.

Schryen, Guido. "Writing qualitative is literature reviews—guidelines for synthesis, interpretation, and guidance of research." *Communications of the Association for Information Systems* 37.1 (2015): 12.

Schwertner, Krassimira. "Digital transformation of business." *Trakia Journal of Sciences* 15.1 (2017): 388-393.

Shameem, A., et al. "Supply Chain Security in 6G Networks: Commerce's Critical Challenge." *6G Security Education and Multidisciplinary Implementation*. IGI Global, 2024. 191-211.

Shomali, Azadeh, and Jonatan Pinkse. "The consequences of smart grids for the business model of electricity firms." *Journal of Cleaner production* 112 (2016): 3830-3841.

Sittig, Dean F., and Hardeep Singh. "A new sociotechnical model for studying health information technology in complex adaptive healthcare systems." *BMJ Quality & Safety* 19. Suppl 3 (2010): i68-i74.

Skinner, Richard J., R. Ryan Nelson, and Wynne Chin. "Synthesizing qualitative evidence: a roadmap for information systems research." *Journal of the Association for Information Systems* 23.3 (2022): 639-677.

Smela, Beata, et al. "Rapid literature review: definition and methodology." *Journal of market access & health policy* 11.1 (2023): 2241234.

Smith, John K. "Quantitative versus qualitative research: An attempt to clarify the issue." *Educational researcher* 12.3 (1983): 6-13.

Snyder, Hannah. "Literature review as a research methodology: An overview and guidelines." *Journal of business research* 104 (2019): 333-339.

Sovacool, Benjamin K., and David J. Hess. "Ordering theories: Typologies and conceptual frameworks for sociotechnical change." *Social studies of science* 47.5 (2017): 703-750.

Sulistyowati, Diah, Fitri Handayani, and Yohan Suryanto. "Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss." *JOIV: International Journal on Informatics Visualization* 4.4 (2020): 225-230.

Thagard, Paul, and Cameron Shelley. "Abductive reasoning: Logic, visual thinking, and coherence." *Logic and Scientific Methods: Volume One of the Tenth International Congress of Logic, Methodology and Philosophy of Science, Florence, August 1995*. Dordrecht: Springer Netherlands, 1997.

Thoring, Katja, Roland Mueller, and Petra Badke-Schaub. "Workshops as a research method: Guidelines for designing and evaluating artifacts through workshops." (2020).

Thuraisingham, Bhavani. "Data mining, national security, privacy and civil liberties." *ACM SIGKDD Explorations Newsletter* 4.2 (2002): 1-5.

Tshabangu, Icarbord, Stefano Ba, and Silas Memory Madondo, eds. *Approaches and processes of social science research*. IGI Global, 2020.

Uslar, Mathias, et al. "Applying the smart grid architecture model for designing and validating system-of-systems in the power and energy domain: A European perspective." *Energies* 12.2 (2019): 258.

Valoggia, Philippe, et al. "Learning from the Dark Side About How (not) to Engineer Privacy: Analysis of Dark Patterns Taxonomies from an ISO 29100 Perspective." *Proceedings of the 10th International Conference on Information Systems Security and Privacy*. SCITEPRESS-Science and Technology Publications, 2024.

Vial, Gregory. "Understanding digital transformation: a review and a research agenda". *Journal of Strategic Information Systems* 28.2 (2019): 118–144

Viganò, Eleonora, Michele Loi, and Emad Yaghmaei. "Cybersecurity of critical infrastructure." *The ethics of cybersecurity* (2020): 157-177.

Voigt, Paul, and Axel Von dem Bussche. "The eu general data protection regulation (gdpr)." *A practical guide, 1st ed., Cham: Springer International Publishing* 10.3152676 (2017): 10-5555.

Voordijk, Hans, and Steven Dorrestijn. "Smart city technologies and figures of technical mediation." *Urban research & practice* 14.1 (2021): 1-26.

Walsham, Geoff. "Doing interpretive research." *European journal of information systems* 15.3 (2006): 320-330.

Walsham, Geoff. "Interpretive case studies in IS research: nature and method." *European Journal of information systems* 4.2 (1995): 74-81.

Wang, Wenye, and Zhuo Lu. "Cyber security in the smart grid: Survey and challenges." *Computer networks* 57.5 (2013): 1344-1371.

Warren, Samuel D., and Louis D. Brandeis. "The right to privacy." *Kingston L. Rev.* 1 (1968): 66.

Warren, Samuel D., and Louis D. Brandeis. "TheRight to Privacy." *Harv. L. Rev.* 4 (1890): 193-196.

Wiggins, Bradford J. "Confronting the dilemma of mixed methods." *Journal of Theoretical and Philosophical Psychology* 31.1 (2011): 44.

Wyborn, Carina, et al. "Understanding the impacts of research synthesis." *Environmental Science & Policy* 86 (2018): 72-84.

Yadin, Gilad. "Virtual Reality Surveillance." *Cardozo Arts & Ent. LJ* 35 (2016): 707.

Yin, Robert K. *Case study research: Design and methods*. Vol. 5. sage, 2009.

Into a Unified Information Privacy Preserving Model

Bahaa Eltahawy and Reino Virrankoski
University of Vaasa, Department of Computer Science, Communications and Systems Engineering Group
P.O.Box 700, FI-65101, Vaasa, Finland
{bahaa.eltahawy, reino.virrankoski}@uva.fi

***Abstract* –Privacy is a vital asset to individuals, where with it only they can possess control over their native information and data. The current dependency on the Internet, data networks, and cellular communication created the need for a robust unified security and privacy standardization that can keep these systems safe, and well-secured, while adopting the users' right to privacy. This required standardization should be ready within the 5G time frame. This would help the upcoming system to benefit from the power of full functionality and controllability offered by the complete security and privacy protection. This in turn will be potential for more data services and applications to become more common, since they are covered by the big umbrella of security and privacy. In this paper, we have concerned these issues. Here, we disassemble security and privacy to their main components, and we point out the main shortages in the current deployments. Then we provide a broad review to precisely describe privacy, and its associated complexities. After that, we bring a set of individual solutions for the different discussed factors. The main outcome of this work comes after, by introducing a unified model for information privacy preservation, which combines all discussed topics. As an addition, we also provide a set of technical recommendations regarding the way how the proposed model should be implemented.**

Keywords—privacy; safety; security; communication parties; conflict of interests and costs

I. INTRODUCTION

The rapid development of computation and communication systems has opened new opportunities that couldn't exist earlier. Currently, many services can be offered to users over different network devices such as table computers or smartphones. As a result, the combined use of local area networks and the Internet has created new concepts, such as industrial Internet, Internet of Things (IoT), converged networks, and many others. These advancements are not limited to the communication sector only, but they as well play an important role serving other technologies, and industries, e.g. smart grid in electricity, remote monitoring in the health sector, e-commerce, and online banking services. Once the communication systems have become such diverse, and broad, they become more complicated, and the amount and types of security risks as a result increase.

Safety, security, and privacy measures are in need to protect users and their assets. Telecommunications and data technologies can play a double role here. Deployments can opt to provide a means to protect users, or in contrast cause harm by revealing vital, personal, and private information. This later scenario can occur unintentionally or maliciously, also with or without users' awareness and permission. The current architecture of Internet and internetworks allows data to traverse through many networks in the way to its destination. These networks can differ in terms of trustworthiness, and acceptable security measures. The existing architecture provides many benefits in connectivity and reachability, but also allows many threats in data protection and data control. As a consequence, advanced measures for privacy are required to protect end users' data.

Privacy is an ethical requirement, a technology trend, and for advanced deployments it is a rule of thumb. This rather exists from the fact that privacy exceeds security to include controllability, configurability, transparency, and many advanced features. Unfortunately, for deployment the scope of privacy faces many conflicts and un-clarities, due to many factors, e.g. regulations, technical limitations, and legalization. There is also the conflict of interests between the different parties participating in the communication process, since different parties commonly have different interests, demands, procedures, and standards. Typically for end-users, they are the least involved in the system, and they are mostly enforced to follow certain policies with almost no options available. This case was accepted when services were limited, but with the current features and capabilities, this case became rather a threat. Another challenge for privacy is the resulted increases of systems' complexity and deployment costs.

In this paper, we are discussing all these parameters, and we run the required arguments to solve for these issues. Here, we disassemble security and privacy, point out the current shortages, and as an outcome we introduce a unified privacy preserving model with a set of technical recommendations for deployment.

The rest of this paper is organized as follows: Security is discussed in Section II, and Section III presents the security architecture. Privacy is discussed in Section IV, and then in section V we present the new unified privacy preserving model. Finally, conclusions come in Section VI.

II. SECURITY

Firstly, a secured system should firstly enjoy safety. Safety [1] is the practice to keep systems safe, which means freedom of harm, specifically the unintentional one. Systems can be vulnerable due to many reasons, and the unintentionality plays a role with incidents such as fire accidents, loss of vital assets and documents, outage incidents, etc. Safety is the practice to avoid such situations. By category, safety is either physical which protects assets in their physical form, or data safety, which concerns data to be maintainable, achievable, available, and intact when needed. Physical safety is a matter of the design phase, while data safety can be achieved using Data Loss Prevention (DLP) technologies as control over data, supervision, and filtering [2].

Secondly, security is the level up after maintaining systems' safety. Security is the freedom from danger or threat [3]. Security is divided into several categories, including personal, operations, communications, network, and information security [4]. Here we concern security by the meaning of information security. "Information security protects the availability, integrity, confidentiality, and authenticity of information and underpins such societal goods as privacy, the protection of digital identity, and the protection of intellectual property. This is performed by deploying a dynamic system of measures taken to protect data, information, and systems from unauthorized use or a disruption due to a human agency or a natural threat" [5]. The classical security model (CIA model) comprised of confidentiality, integrity, and availability measures [6]. The later Parkarian Hexad model included utility, possession, and authentication [7]. In the current applications and services, non-repudiation as well is a vital parameter to consider due to e-commerce and e-banking operations [8].

A. Utility

Utility refers to the usefulness, and worthiness of the exchanged data [9]. Utility depends on the deployed applications and the data formats applications utilize. For this reason, utility is not a concern for operators, because it is an abstract concept and a property of applications. Utility can be seen as the lack of standardization between peers, which rather can affect bandwidth and costs if not well addressed.

B. Availability

Availability is the readiness and reliability of resources to be accessible upon request [10]. Resources and identifiers have to be available and accessible to establish a session, e.g. IDs, addresses, locations, databases, privileges, etc. Availability is the foundation for security, since other measures tend to be meaningless when resources are not available. Systems must be able to handle incidents of unexpected failures by considering link redundancy and aggregation, and redundant standby infrastructure solutions. Also, intentional attacks targeting resources can be repulsed by isolating the sources of the attacks, and by hiding communication by means of anonymity.

C. Integrity

Integrity concerns the delivery of data in its original form. Information integrity refers to freedom, trustworthiness and dependability of information [11]. That is the consistency and the assurance of data against any sort of modification or alternation [12]. Integrity is achieved by means of the authentication procedures, which vary from simple checksums to sophisticated cryptographic algorithms as hashing methods. For robust security, integrity is imperative to both data and control frames. Separation between authentication and integrity mechanisms would significantly enhance the security practices. Another practice is the separation between the different domains as network access, user domain, and application [12].

D. Possession

Data possession or control protection concerns protecting and controlling data in the communication devices [13]. Devices typically store valuable data, once a device is lost, a significant amount of user's data can be compromised. Thus, possession shall be completely independent of the network and its security standards. Accordingly, passwords, tokens, biometrics, and other methods are mandatory to provide strict access, as well as data encryption, and automatic data erase.

E. Confidentiality

Confidentiality directly concerns the content and the access to user's data. Confidentiality is the property of information that is not made available or disclosed to unauthorized individuals, entities, or processes [14]. Confidentiality is protected by means of cryptography, and it is mostly deployed in the access layer since the core network is assumed to be trustworthy [15]. Compatibility is the main challenge confidentiality faces, since it prevents hybrid networks and devices from benefiting from advanced security mechanisms, thus leaving a hole for attackers to exploit system weaknesses.

F. Authentication

Authentication, Authorization, and Accounting (AAA) concepts provide means to identify users and to approve their permissible activities. Authentication validates the user's identity, authorization examines the user's privileges, services and resource permissions, and accounting keeps tracking of the user's activity for further considerations and security countermeasures [10] [16]. Authentication is performed along with integrity and ciphering procedures, since integrity provides a means to ensure the consistency of the authentication procedure, while ciphering protects the exchange of the authentication frame [17]. Unfortunately, most authentication mechanisms exchange unprotected messages during the key management phase. This case can be the gate for intruders to access the system. Public Key Infrastructure (PKI) deployments can overcome these situations, but they suffer from lack of sufficient standardization [18].

G. Non-repudiation

Repudiation is the denial by one of the entities involved in a communication of having participated in all or part of the communication [19]. Non-repudiation measures are required to prevent an entity from denying a communication activity, to prevent abandoning responsibility and accountability of own actions by means of verification. This can be performed by digital signatures with PKI systems.

H. Existing Shortages

Despite the precision of the deployed security measures, the system suffers from many shortages. Firstly, they lack standardization, as some parameters are let optional for operators' decision. Secondly, compatibility with weaker legacy system is a big issue to consider. Thirdly, the system's security can be compromised because of the initial authentication phase's current exchange of vital data in clear. Fourthly, the security structure is totally independent of end-users. Different attacks' scenarios and their risk to the network are given in [20].

III. Securtiy Domains

For implementation, the 3GPP has divided the security architecture into security domains [21]. We have adopted this architecture, and also introduced two extra domains, *device domain security* and *data domain secur*ity. This architecture can work as a security basis over all IP-based networks.

1) *Network Access Security:* Features between the user's device and the first node to the network. This is a relay to handle security functions, e.g. authentication.

2) *Network domain security:* Features between the different network nodes, e.g. tunneling, and secure routing protocols by means of cryptography.

3) *User domain security:* A means to validate the user to the device upon usage.

4) ***Device Domain Security****:* This extends the User domain security to include facilities for remote access, tracking and locating, erasing, accounts and permissions, functionality control, and all other policies concernig devices themselves.

5) *Application domain security:* Secure data exchange between applications.

6) ***Data Domain Security****:* This is the set of policies that ensure data protection within the device, e.g. using AntiVirus and AntiMalware, patching and updates.

7) *Visibility and configurability:* Information about the applied security level, encrypiton, network capabilities and services. It allows the user to participate to the security process so that he can choose his parameters, and accept or reject a service or a certain access.

IV. Privacy

It is well-known that even if the highest safety and security standards are applied, some information can still be leaked to outsiders. For example time, location, session activity, and many indicators to the communicating parties as well. This can enable the outsiders to extract valuable information using a method known as connect the dots. In a worse scenario, interception can be done internally, i.e. by a trusted service. This later exact case urges the need to answer the following questions: Who is allowed to access an entity's data? And what are the acceptable situations? This goes beyond the safety and security concepts discussed so far. To answer these questions, we go to the more generalized frame, privacy.

A. Privacy, Definitions and Theories

Research interests related to privacy have been growing rapidly since the beginning of computerization. Main reasons behind this development are the new demands and concerns in privacy caused by the digitalization, and the moral issues regarding technology and sciences. Privacy protects users' private data from being disclosed, or connected to draw a figure about their activities and their personalities [22]. Still, this is not absolute. There are some lines where privacy needs to be revealed under some criteria and by the right entities.

Privacy can be explained according to two theories: privacy control theory, and restricted access theory [23]. The privacy control theory proposes that privacy can be preserved if a person has control over his information and the way how it is spread. On the contrary, the restricted access theory relies on that the privacy can be preserved by restricting what others can access, based on secrecy, anonymity and solitude. Both theories were contradicted by the privacy control/restricted access theory [24]. It stated that controlling information in the cyberspace is unfeasible. However, according to privacy control / restricted access theory, it is a must that the right entity at the right time can access the information. This combines the advantages of both previous theories by stating that an entity can control information and restrict others from accessing it, while it is still accessible by the right entities whenever needed under the right conditions. Moreover, such a concept of privacy-policies was introduced, where they are flexible to be set according to the situation. The above mentioned theories summarize the privacy definition as: privacy is a right for individuals, as they hold the right to control their own information and the right to restrict others from accessing it, as long as no harm can be caused to others with this information.

B. Elements of Privacy

To preserve privacy, five elements need to be protected: data and traffic, identities, locations and mobility, time, and existence [25].

Traffic and exchanged data between entities should be protected against others. This can be achieved by using the cryptographic functions of the security procedures. Identity is how a person defines oneself to the world, describing his individuality, sort, and relation among others. An identity is used to relate a user to own activities, interests and privileges. Therefore, users' identities must be protected. This can be practically unfeasible since identities are used for session establishment. However, the use of temporal independent identities and a level of randomization can be a feasible solution for that. This generally is the concept of anonymity.

Related to privacy, location and mobility is a crucial concern. Many systems, services, and applications keep tracking records about users, to be used to provide services on demand. However, there is no enough transparency about this process and data usage. Location records can be used to draw a general picture about a person's behavior, and disclosure of

such information is a serious threat. Location Based Services (LBS) and other applications can use this data maliciously if they are not well trusted. Location privacy can be achieved by implementing blurring and obfuscation techniques, or by applying K anonymity servers and mix zones. These techniques will partly hide the exact locations of the users.

Time can be used with the other elements to precisely identify users' activities. Consequently, time privacy is required to protect against disclosure of activity times. Times of transactions can be hidden by randomly sending junk data at random instances to cause a sort of illusion about the exact times of events, though it will increase the amount of traffic.

The last factor to consider is the existence privacy, which protects entities by hiding them from surveillance. This task is not easy due to the nature of communication and its limitations. A strict control of node visibility and the use of pseudonyms can still provide an adequate level of existence privacy.

C. Privacy Relations

Privacy as a set of relations comprises anonymity, unlinkability, unobservability and undetectability [26]. These relations maintain privacy by hiding users' identities, as well as any indication, relation or connection about their activities, to protect them from information leakage.

Briefly, pseudonymity is the use of traceable anonymous identities rather than the real ones. Anonymity is the ability to combine an anonymous identity with a recognizable one in such a way that the identity cannot be identified from a set of identities. Anonymity can be achieved by the continuous use of pseudonyms or by providing less information than the amount what is needed for identification. Unlinkability is the inability to detect a link or relation between two identities or between two activities. Undetectability is the inability to detect the existence of an identity or its participation to certain activity. Finally, unobservability is the inability to observe a user and its activities. This rather implies undetectability and anonymity. Anonymity itself comprises sender and receiver anonymity to protect the communicating peers, as well as relationship anonymity to rather hide any information about the communication and the involved active users, i.e. unlinkability. These elements and their relations can be written as follows:

Unobservability → Undetectability
Unobservability → Anonymity → Pseudonymity
Sender/Receiver Anonymity → Relationship Anonymity.
Sender/Receiver Unobservability → Relationship Anonymity.

It is clear that the maintaining of unobservability is the sufficient condition to preserve privacy. The drawback is that it requires systems with high complexity. As a consequence, it is difficult to achieve unobservability in practice. A better easy to implement mechanism is to provide anonymity, in addition to spread dummy meaningless traffic to enable undetectability. Still, deploying these elements collectively is more conceptual than applicable, and in any way absolute privacy can be achieved in reality only up to certain levels [27]. If privacy levels span on a scale from 1 to 6 as presented in Table 1, then level 5 indicating beyond suspicion would be the best achievable deployment in reality. In contrast, exposed or provably exposed are the worst cases, which are common in web and in some of the VoIP applications.

Table 1. Privacy levels span on a scale from 1 to 6 [27].

6	5	4	3	2	1
Absolute Privacy	Beyond Suspicion	Probable Innocence	Possible Innocence	Exposed	Provably Exposed

D. Parties, Rights and Responsibilities, Conflict and Costs

Within a communication session, four parties with different rights and responsibilities are included [28]. The first and second parties are individuals or entities establishing the communication session. They are users who use the provided services and typically they do not hold control on any of the communication factors. The third party is the one managing the communication environment. This party can be the operator network, a monitoring organization, or the governmental authorities and policy officials. The fourth party consists of all other entities, which do not participate in the communication session and do not get any information about it by default. This can include the public, or in a worst case a malicious attacker.

Parties have different rights and responsibilities, which is the main reason behind the conflict of interests. The first party has the right to privacy, to hold control over their own information, and to restrict others access. This party has to take into account the spreading of their own information, and the responsibility associated with it. The first party also holds the right to acquire the level of privacy that suits for them, according to the benefits they gain or the threats they might face [29]. However, as a part of the society, the first party holds the responsibility not to cause harm with the rights they hold, because the privacy can be broken by any suspicious harm or danger. The second party is a replicate of the first one, with the same rights as they are sharing a communication relation. By default, the first party trusts the second party, which gives the second party responsibility against spreading information.

The third party (the one managing the communication environment) has an important role in privacy since it has access to the resources of the communication facility. Third party has the responsibility to protect the communication between communicating parties, also to protect other parties' data, including the stored personal information. Similarly, third party holds a right to protect the society from any sort of danger that other parties might cause. The fourth party on contrast to the previous ones has the least responsibilities and rights, as they have the right to access the authorized data only.

Conflicts do not arise only because of the differences between these four parties associated with the communication session. There are also other conflicts regarding the meaning of privacy itself, including [30]:

1) Cultural conflicts: The culture and its understanding and acceptance for privacy values, for individuals and society.

2) Organizational conflicts: Different places have different perspectives regarding privacy.

3) *Individual conflicts:* No common view about privacy.

4) *Structural conflicts:* The structure of privacy systems might conflict with safety, security and other modules.

5) Communication conflicts: Tracking, mobility and other services will face difficulties as well.

6) Price conflicts: Increased costs due to complexity.

7) *Efficiency and quality conflicts:* Data collection and extraction for evaluation processes conflicts with privacy.

8) Operational conflicts: Limitation of shared resources and information affect operations and increase difficulties.

9) *Standardization conflicts:* Different standards exist, but they do not currently cover the area of privacy that well. New standard development is a time consuming and difficult task.

10) *Expansion conflicts:* The standards should be forced across all networks, which might affect expansion plans.

In addition to these conflicts, it is necessary to consider crime fighting and privacy conflicts. Privacy, as all rights, can also be misused. That is because of the protection it provides against information collection, which in turn can encourage illegal actions and behavior. This later increases the criminal activities and certainly causes harm to the society [23]. It is a must while drawing the general lines for privacy to consider such cases, to allow lawful interception under the legal form.

V. Unified Privacy Preserving Model

Based on the presented discussion and analysis, we ended up formulating the following model as a basis for unified privacy preserving. The semantic architecture of the model is shown in Figure 1. In the proposed model, we could combine the essential components that are required to preserve privacy in the communication systems. The given model comprises both the theoretical and the practical perspectives. The theoretical perspective defines the main elements that should be considered to preserve privacy, and the practical perspective provides recommendations on how to implement these elements.

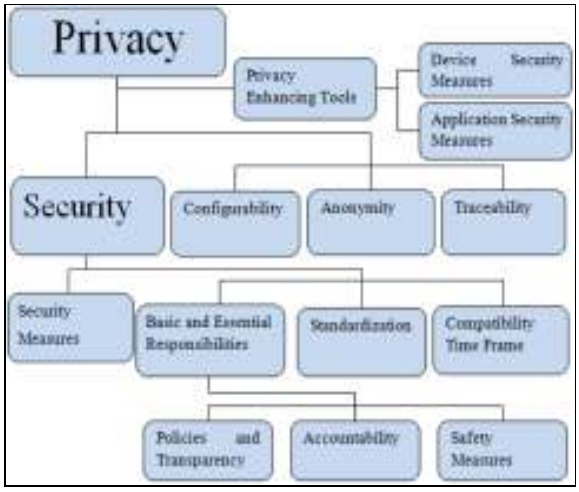


Figure 1. The proposed privacy preserving model.

A. Privacy from the Theoretical Perspective

The main elements that should be considered to preserve privacy are the following ones:

1) The transparency of the policies: Clear policies with well-defined procedures, functions, and actions are required. Policies have to clarify the disclosure situations, purposes and responsibilities upon disclosure. Also, the changes of the applied policies should be acknowledged and agreed upon applicaiton.

2) *Accountability:* Responsibility for own actions and behavior.

3) *Safety measures*: Operators' responsibility to maintain safety, which includes physical and data safety practices.

4) *Standardization:* Security measures and standards should be agreed. Applied mechanisms cannot be left as an implementation option for operators.

5) *Compatibility:* Upgrade time frame for legacy systems, applications, and protocols should be clearly declared.

6) *Security measures:* Considerations for actions targeting users, systems and data, also applying the main security measures discussed previously, will ensure secure communication. Authorities and governments on the other hand also hold a responsibility against the harm that might be caused to users or by users, thus to take the legal considerations.

7) *Configurability:* Ability to hold control over own data and security functions should be revised. Flexibility to configure and control the different privacy parameters according to users' preferences should be granted.

8) Anonymity: To protect users and to hide their activities.

9) *Traceability:* Unlike anonymity, linkage is allowed but only controlled by authorities under the legal form. This specefically restricts privacy so that society can provide its protection.

10) *Application Security measures:* Restricting applications from gathering, storing, or exchanging data about users without declaration and usage transparency. Also, anonymity should be applied upon collecting data.

11) *Device Security:* Mechanisms to restrict access to devices and stored data. Also rules to remotely control devices under the legal form.

B. Privacy Practical Perspective Recommendations

From the practical perspective, we provide here a set of general recommendations to consider in the implementation of the hypothetical elements:

1) Upgrading the non-standard algorithms and functions to the latest stable standard.

2) Time frame to upgrade legacy components. Also hybrid network compatibility capabilities should be revised.

3) Access network and AKM mechanisms are the weakest ones of the security phase, thus they need further consideration.

4) Digital Signatures are required to provide data origin authentication and non-repudiation guarantees.

5) PKI implementation to protect confidentialtity, and to provide lawful interception only for legal authorites.

6) Multi-homing solution is an acceptable to provide for anonymity and communication reliability.

7) IPv6 upgrade is required since it affords the means for multi-homing and also security services, that do not exist in IPv4.

8) Host Identity Protocol (HIP) implementation to provide anonymity, multi-homing, and also interception for legal authoroties.

9) IPSec,TLS/SSL, and/or other security protocols should be implemented to provide means for tunneling and application security.

10) Other security protocols should be considered, as Secure Real-Time Transport Protocol (SRTP), SRTP Control Protocol (SRTCP), Secure Distributed Anonymous Routing Protocol (SDAR), and Onion Routing mechnisms.

11) Application Security level is required to protect users from attacks targeting data within devices.

C. Case Scenario

According the presented model, this is the suggested application. The third party as the operator is responsible for maintaining the system's safety. The other third party as the authority body supervises and approves the operators' deployments, because they are going to take full responsibility with other implementations. Operators and authorities provide clear and transparent policies to users. Also, upon policy changes, an agreement should be established before policy application. End-users here will be responsible and maintain accountability on their own actions and use of the system. Operators will deploy all the possible security measures. On the other hand, cryptography procedures and PKIs are implemented by operators, but controlled only by authorities. This will keep operators' hands away from users' data, and possible malicious interception. When moving to other networks locally or within a roaming agreement, standardization will keep the system to its maximum security. If the new system doesn't meet the security level, the user will be notified about the security situation in prior. As well, this is the case when moving to networks with legacy deployments. Additionally, legacy deployments will be forced to upgrade within a specified time frame. Now, end-users enjoy the highest security deployment.

For the other matters regarding existence, routing, time, activity, and location protection, configurability should be allowed. This will let users to control the level of protection they seek, as well it will notify them about the accuracy of data upon their selection, and it is up to their preferences to choose whether to deploy it or not. Operators' systems by default will not be allowed to store data about users but only the required ones for successful communication. This rather will be connected to a central anonymity center, which connects real pseudonyms to anonymous ones. Only the real ones are accessible from the authorities' side. For the matter of legal situations, all identities can be connected under certain cases to provide for traceability or even taping. By now, end-users enjoy a protected privacy level, from operators, and any malicious tracking applications, since there is no connection to their real identities. On the other hand, since privacy is not absolute, the lawful interception is allowed and guaranteed.

The last issue will be to maintain devices' security, and application security. This will make sure that devices are not accessible by unauthorized ones, and that applications don't grant access to sensitive data.

In this scenario, we proposed that the first and second parties are end-users. The same exact scenario is applicable to all other applications as well. For instance, IoT, and Machine to Machine (M2M) deployments within the upcoming 5G network can benefit from this scenario. This works by performing the required separation between the application and the operator. In other words, the communication will be consistent and free of malicious incidents.

The only challenge that faces such deployment is the increased complexity and the heavy cryptographic deployments. Fortunately, 5G already is promising for Very High Throughput (VHT), which makes such overhead to be a minor one to consider.

VI. CONCLUSTION

In this paper, we gave a discussion about the issue of privacy, its related measures, and the difficulties that are faced to achieve privacy in the current communication systems. Based on that discussion, we provided a general privacy preserving model and a set of technical recommendations for its implementation. These results can be utilized when thinking about privacy solutions for the rapidly growing number of applications, either for industry or for private customers. We ended up the paper with a typical case scenario of the way to successfully achieve privacy in the communication system. Finally, "It is a necessity to protect individuals and the societal right to privacy, yet a complete privacy preserving system does not and cannot exist, because privacy is never absolute".

REFERENCES

[1] "safety." Dictionary.com Unabridged. Random House, Inc. 1 Oct. 2015. <Dictionary.com http://dictionary.reference.com/browse/safety>.

[2] Wang Xingkui; Peng Xinguang, "Research on data leak protection technology based on TPM," in *Mechatronic Sciences, Electric Engineering and Computer (MEC), Proceedings 2013 International Conference on* , vol., no., pp.2354-2358, 20-22 Dec. 2013

[3] security. Oxford Dictionaries. Oxford University Press, n.d. Web. 4 July 2013. < http://www.oxforddictionaries.com/definition/english/security>.

[4] Whitman, Michael E. & Herbert J. Mattord (2010). *Principles of information security*. Boston: Cengage Learning.

[5] Straub, Detmar W., Seymour E. Goodman & Richard Baskerville (2008). Information security: policy, processes, and practices. New York: M.E. Sharpe.

[6] Saltzer, Jerome H. & Michael D. Schroeder (1975). The protection of information in computer systems. Proceedings of the IEEE, 1975, 63.9: 1278-1308.

[7] Parker, Donn B. (1998). Fighting computer crime: A new framework for protecting information. New York: John Wiley & Sons, Inc.

[8] ISO (1989). ISO 7498-2, Information processing systems-Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture. ISO. Geneva, Switzerland.

[9] Andress, Jason (2011). The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Massachusetts: Elsevier.

[10] Stamp, Mark (2006). Information Security Principles And Practice. Hoboken, New Jersey: John Wiley & Sons.

[11] Geisler, Eliezer, Paul Prabhaker & Madhavan Nayar (2003). Information integrity: an emerging field and the state of knowledge. In: Management of Engineering and Technology, 2003. PICMET'03. Technology Management for Reshaping the World. Portland International Conference on. IEEE, 2003. 217-221.

[12] Lei, Wu & Song Xiao Ting (2009). Information integrity and its protection in networks. In: 2009 5th Asia-Pacific Conference on Environmental Electromagnetics. 2009. 238- 241.

[13] Ateniese, Giuseppe, Roberto Di Pietro, Luigi V. Mancini & Gene Tsudik (2008). Scalable and efficient provable data possession. In: Proceedings of the 4th international conference on Security and privacy in communication networks. ACM, 2008.

[14] IEEE (1998). IEEE standards for local and metropolitan area networks: standard for interoperable LAN/MAN security (SILS) specification; IEEE standard 802.10. IEEE Standard Press.

[15] Horn, Günther, Klaus Muellerand & Bart Vinck (1999). Towards a UMTS security architecture. ITG FACHBERICHT ,1999: 495-500.

[16] Convery, Sean (2007). Network Authentication, Authorization, and Accounting: Part One. The Internet Protocol Journal [online] 10:1 [cited 2 Oct. 2013] Available from Internet: <URL: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-1/101_aaa-part1.html>.

[17] Tanenbaum, Andrew S. & Maarten Van Steen (2007). Distributed systems principles and paradigms. Ed 2. New Jersey: Prentice Hall.

[18] Hsu, C. I., & Tung, Y. C. (2008). The benefits of PKI application and competitive advantage. *WSEAS TRANSACTIONS on COMMUNICATIONS*, *7*(7), 776-785.

[19] ISO (2009). ISO/IEC 13888-1: Information Technology Security Techniques-Non repudiation-Part 1: General. Available from World Wide Web: <URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:13888:-1:ed-3:v1:en>.

[20] Mobarhan, M. A., Mobarhan, M. A., & Shahbahrami, A. (2012). Evaluation of security attacks on UMTS authentication mechanism. *International Journal of Network Security & Its Applications*, *4*(4), 37-52.

[21] 3GPP. Security Architecture (3GPP TS version 33.102 Release 4). Available from World Wide Web: <URL: http://www.etsi.org/deliver/etsi_ts/133100_133199/133102/04.01.00_60/ts_133102v040100p.pdf>.

[22] Horniak, Virginia (2004). Privacy Of Communication-Ethics And Technology. Master Thesis, Mälardalen University, 2004. Available from World Wide Web: <URL: http://www.idt.mdh.se/utbildning/exjobb/files/TR0390.pdf>.

[23] Spinello, Richard (2006). Cyberethics: Morality and law in cyberspace. Massachusetts: Jones & Bartlett Learning.

[24] Moor, James H. (1997). Towards a Theory of Privacy I1', in the Information Age. Computers and Society, 1997, 27.3: 27-32.

[25] Candolin, Catharina (2005). Securing military decision making in a network-centric environment. Available on World Wide Web: <URL: http://lib.tkk.fi/Diss/2005/isbn9512279819/isbn9512279819.pdf>.

[26] Pfitzmann, Andreas & Marit Hansen (2005). Anonymity, unlinkability, unobservability, pseudonymity, and identity management-a consolidated proposal for terminology. Available from World Wide Web: <URL: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.28.pdf>.

[27] Chao, Gao (2009). Study on Privacy Protection and Anonymous Communication in Peerto-Peer Networks. In: Multimedia Information Networking and Security, 2009. MINES'09. International Conference on. IEEE, 2009. 522-525.

[28] Mason, Richard O. (2000). A tapestry of privacy, A meta-discussion.

[29] Graham, Ian (1999). Putting Privacy in Context--An overview of the Concept of Privacy and of Current Technologies. Retrieved June 13, 2013.

[30] Noam, Eli M. (1995). Privacy in Telecommunications: Markets, Rights, and Regulations. Part I. New Telecom Quarterly, 3.2: 52-59.

Understanding Cyberprivacy: Context, Concept, and Issues

Bahaa Eltahawy[1], Duong Dang[1]

[1] School of Technology and Innovations, University of Vaasa, Vaasa, Finland
{bahaa.eltahawy,duong.dang}@uwasa.fi

Abstract. Cyberprivacy has become one of the most worrisome issues in the age of digitalization, as data breaches have increased at an alarming rate, and the development of technology has changed privacy norms themselves. Thus, maintaining cyberprivacy is important for both academia and practitioners. However, the literature on cyberprivacy is fragmented, since the topic is multidisciplinary and often confused with cybersecurity and data privacy. In this study, we seek to understand cyberprivacy by conducting a comprehensive literature review and analyzing 79 selected articles on the topic between 2008 and 2021. Our analysis shows that there are eight contexts associated with cyberprivacy. We proposed concepts on cyberprivacy from different views and highlighted four issues related to cyberprivacy for future consideration. Taken together, the knowledge on cyberprivacy, its challenges and its practices does not seem to accumulate. Consequently, there is a need for more targeted research on the topic to cover different contexts.

Keywords: Cyberprivacy, Cyberspace, Cybersecurity, Literature Review

1 Introduction

Rapid information technology communications (ITC) advances have brought changes to values, norms, and privacy. For instance, individuals would choose to share their right to be unobserved [1] for services and other benefits [2]; yet, service providers and third parties would use monitoring technologies [3] to collect more data than allowed and agreed upon. Traditionally, computer security (COMPUSEC) and information security (InfoSec) measures [4] are used to protect individuals and systems from malicious activities. Three perspectives of protection are often considered, including confidentiality, integrity, and availability (CIA triad). However, although COMPUSEC and InfoSec target these issues, they have a narrow scope and limited practices as they only deal with confined and isolated systems [4]. With the involvement of the Internet, computing devices taking different forms, and the unprecedented proliferation of data, it is thus very difficult to cope with privacy in cyberspace, i.e. cyberprivacy in a digital environment [5]. This is because of the blurring between the individual as a physical organism with its own rights against digital identity and its capabilities [7, 8, 9] and cyberization [6]. As a result, it is argued that protection must go beyond traditional measures.

17th International Conference on Wirtschaftsinformatik,
February 2022, Nürnberg, Germany

Despite the importance of protecting digital identity rights and privacy, there is no general agreement on the exact scope of the term privacy [5]. In a similar vein, even though cyberprivacy is discussed in previous literature [10, 11, 12], there is a lack of a common understanding on cyberprivacy in terms of scopes, issues and context. Hence, in this study, we tried to address the topic of cyberprivacy and build an adequate understanding of it - which helps to improve protection of individuals, systems, and institutions in cyberspace - by answering the following research question: What is the context, concept and issues of cyberprivacy discussed in the literature? By answering this question, we determine the meaning of cyberprivacy in existing contexts, provide clear definitions of the key concepts of the topic, highlight the change that led to this issue, and in consequence emphasize on the actions needed to address it.

In the following sections background is presented (Section 2), followed by the methods (Section 3). Section 4 presents the findings, while Section 5 illustrates discussions. Finally, conclusions are drawn in Section 6.

2 Background

The "Right to Privacy" has been highlighted as a fundamental right since the early Harvard Law Review of 1890 [13]. Nowadays, this right has become one of the most complex issues to address [14, 15, 16] due to the paradoxical views and interpretations in dealing with personally identifiable information (PII) [17] of different stakeholders, such as the legislative perspective, the technical side, the commercial side, and the government side. According to [2], the dilemma of privacy arises from the benefits and transparency resulting from the use of data against the concerns of misusing sensitive personal information. With the help of [18] and [19], it is clear the need for dedicated privacy research that combines technical, human and social sciences, thus to address and understand implications of privacy to maintain trust, draw on what is or is not technically achievable, and suggest the right direction for privacy solutions.

There are two concepts related to cyberprivacy, namely, cyberspace and cybersecurity. First, cyberspace was considered as one of the most confusing terms in science over the past decade as the boundaries no longer exist, and the interaction is fast-paced with no control of any kind [20, 21]. According to [22], cyberspace refers to "the global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" [23]. Domains of cyberspace is, but not limited to the Internet; Internet-of-Things (IoT) technologies; Communication and Mobile technologies; Cloud Computing; data sciences and applications of Big Data (BD), Machine Learning (ML), Deep Learning (DL), Data Mining (DM), and Artificial Intelligence (AI); Blockchain; Virtual Reality (VR) and Augmented Reality (AR); Information Technology; Operational Technology (OT); and the human factor on top [22, 23].

Second, cybersecurity is defined as "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights" [24]. In [25], the

National Institute of Standards and Technology (NIST) defined three domains for protection, i.e. people, technology, and processes. NIST also provided detailed guidelines on the given domains and could provide adequate protection against most of the current issues. However, despite the existence of these guidelines, the issue is beyond typical security measures of cybersecurity. For example, PII associated with data, and the potential risks is one of the issues [17]. Another example is the issue related to traceability of involved parties [26], by connecting-the-dots [27, 28, 29] and similar mechanisms.

To our best knowledge, there is no common understanding of cyberprivacy, but rather mixed ones of cybersecurity, Internet and data privacy. However, cyberprivacy in our opinion, is a unique concept that addresses the issue of protection from a holistic perspective including security, persona, and legislative matters. Unfortunately, literature on these issues is scarce. Thus, we tried here to cover these topics and related ones, in favor of understanding the context, concept, and issues of cyberprivacy.

3 Methods

3.1 Methodology

The systematic research methodology practices of Okoli and Schabram [30] were adopted and followed by the recommendations given by Schryen [31], and Rowe [32]. As we consider cyberprivacy as privacy in cyberspace [33], we built our knowledge by searching articles in Information Systems (IS) and related disciplines. We searched in the specialized database Finna[1], and then in IEEEXplore and Google Scholar. Regarding search terms, searching the terms 'Cyber' and 'Privacy' was misleading as it returned results related to either privacy in general or cyber-related topics. Accordingly, we searched the term 'Cyberprivacy' and all combinations of its parent term 'Cyber Privacy'. The search yielded 191 and 1490 results for 'Cyberprivacy' and 'Cyber Privacy', respectively. We analyzed the term 'Cyberprivacy' and the term 'Cyber Privacy', articles were then categorized by year. From this initial analysis, the year 2008 was set as the lower limit of this study (four articles exempted from this criterion due to their importance), as it was noted that several technological breakthroughs occurred in the year 2008, e.g.: Google processed 1 trillion URLs [34]; Facebook reached 100 million users [35]; the first Android phone [36]; and Reality Mining [37], a system that uses cell phone data to extract patterns about users. Finally, we selected "peer reviewed" and scientific publications. As a result, we ended up with 78 articles on 'Cyberprivacy' and 564 articles on 'Cyber Privacy', which are the basis of this study.

[1] Finna is a search service that provides central access to material from Finnish libraries and all modern databases and content providers. Finna can be accessed online at: finna.fi

3.2 Scanning, Inclusion and Exclusion Criteria

Articles were assessed afterwards by examining keywords, abstracts, and summaries. Figure 1 shows the process of selecting the relevant articles.

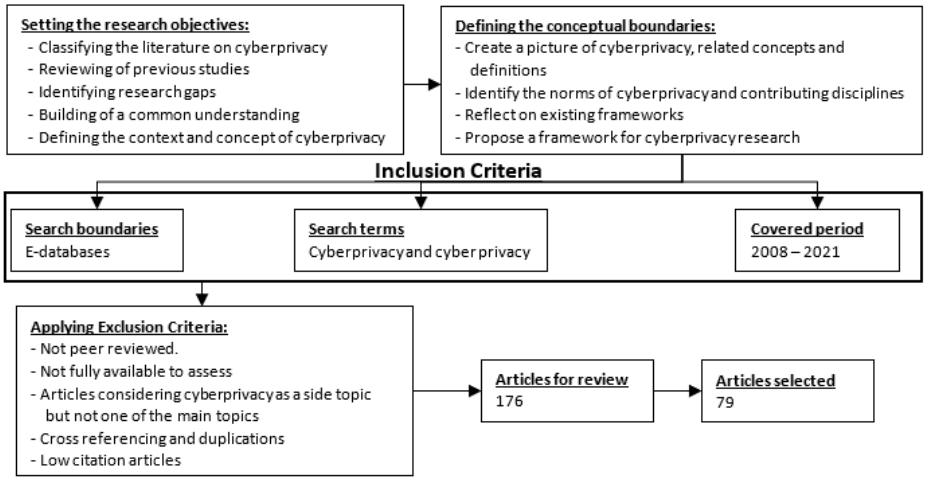


Figure 1: Scanning, inclusion, and exclusion criteria

From selected papers, the following preliminary data was extracted: Number of papers per year (Figure 2a); and Cyberprivacy-related topics and concepts (Figure 2b). The latter was done by counting keyword frequencies. Topics and concepts are then used for our synthesis, which is discussed in Sections 4 and 5.

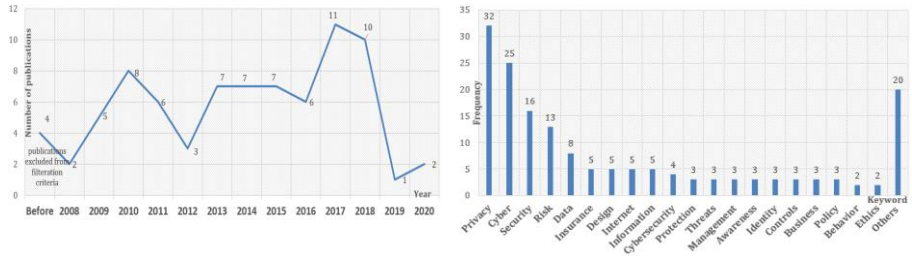


Figure 2: (a) Number of reviewed contents per year; (b) Frequency of keywords extracted from the reviewed literature

4 Findings

4.1 Cyberprivacy Context

Articles were classified into contexts based on the topic and area of concern, so that interpretation and relationship discovery could be conducted. Here we used the qualitative content research methodology practices specified in [38, 39] to help with this task. As a result, eight contexts were found, as shown in Table 1.

Table 1. Common context categories for analysis

Context	Topics and areas of concern
Technology	Applications, developments, and advances in applied knowledge (e.g., technologies and their challenges)
Legislation and rights	Law matters, Acts, constitutions, rights, and regulations
Ethics and morality	Values, beliefs, principles, and the general sense
Business and economy	Profitability and revenue making
Risk and insurance	Threats, danger, assets' loss, impacts and their probability
Behavior and psychology	Perception, acceptance, interpretation, thinking, and actions
Societal	Impact on the society, social matters, and the public
Medical	Health, and well-being

Figure 3 shows the number of articles in each context, noting that an article can fit into more than one context.

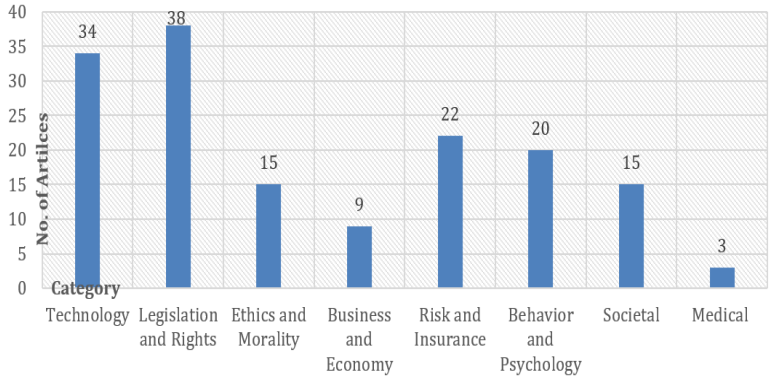


Figure 3: Number of articles concerning cyberprivacy context categories

Cyberprivacy in Technology Context. Services pose privacy risks through the data they collect and process [11], to create clusters and user profiles [11, 40], and in many cases PII [41] can be identified even after implementing some level of data obfuscation. Technologies allow revealing sensitive information, such as identities, physical features, biometric information [42], time, location, and used applications [43, 44]. Cyberprivacy in technology context thus aims to protect the digital persona while taking different forms, i.e. physical, virtual [9], or anonymous [45], since profiling and disclosing information about activities can lead to bigger problems [11, 40]. Table 2 summarizes technologies often discussed in selected papers.

Table 2. Technologies and their challenges for cyberprivacy

Technology	Challenges for cyberprivacy
Cookies [11]	Keep users' data and identifiers that contain personal attributes and thus can be used for tracking

Technology	Challenges for cyberprivacy
RFID and NFC [46, 47]	Allow monitoring and tracking and thus can be used to reveal personal activities
Data science and knowledge discovery [48]	BD, DM, DL, and AI, have great capabilities to learn users' activities and create users' profiles and their behavior [40]
IoT [49, 50]	Monitor, track, and control data, such as in Smart Grid [51, 52, 53], and Smart Cities [54, 55]
VR and AR [9]	Not only track the user, but others around VR/AR

Several papers addressed solutions to deal with those challenges in cyberprivacy [48, 56]. For example, law must address the use of emerging technologies, and similarly new technologies must take the law and regulations at their core. Moreover, solutions such as encryption and anonymity are no longer the key [42, 45, 49, 53, 57], since tracking can be done without decryption. Literature also discussed using technologies as a means to deal with those challenges. For example, blockchain can solve some of the mentioned issues as blockchain underpins encryption, anonymity, and traceability simultaneously, and thus can be used as a trusted third party [57]. Also, advanced encryption (e.g., asymmetric encryption or public key cryptography) should be included from the design [58] phase. Finally, subgroups and protected zones where privacy is measured differently [59], control and opting mechanisms [43, 60, 61], and systems' compatibility [59], should be considered.

Cyberprivacy in Legislation and Rights Context. Cyber governance is considered a complex task to regulations [12]. Many dilemmas and aspects have been discussed in selected papers. For example, the distinction between information that could be public or should be kept private [12]; self-regulation [43]; free speech against knowledge dissemination [62] and security; personal information [11] and useful utilizations [45]; public's safety [63, 64] versus privacy; the rights of liberty [12, 65] and democracy [46, 66, 67]; cyber terrorism and other cyber-backed illicit activities as bullying, stalking, misinformation, etc. [68]; political and governmental rights [1, 69, 70]; law consideration [7] and the way actions in cyberspace are perceived and evaluated; regional and global differences in viewing privacy rights [3, 71].

Cyberprivacy measures therefore are the key to resolving these dilemmas and aspects. Many articles (e.g., [3, 42, 43, 45, 62, 66, 71, 72]) specify that consent and control mechanisms are the key to achieving cyberprivacy. With consent mandated, individuals can accept or deny data collection and/or sharing prior to further processing. Moreover, consent itself requires transparency [1, 7, 59, 62, 64, 66, 73] and sharing of usage information, thus promoting awareness [67, 74, 75]. Control mechanisms play a vital role here as they regulate activities, allowing users to interact, control, and amend data in the event of changes. Acts as the General Data Protection Regulation (GDPR), the Fair Information Practice Principles (FIPPs) [59], and California Consumer Privacy Act (CCPA) [76], addressed this inquiry by mandating data collectors to provide users with safeguards and controls to modify preferences according to their needs. Besides

this, they also mandated the right to seek their own data erasure, which is known as the right to be forgotten [71, 77].

Law enforcement and accountability are a key to protecting cyberprivacy and ensuring systems that operate as expected. However, there is no common agreed legal framework for cyber activities [66]. As a result, awareness of legal consequences and liabilities should be informed and enforced. Moreover, some laws and regulations have shortcomings [45, 78] regarding data disclosure and prohibition of data collection. To overcome these obstacles, an independent legal privacy authority is needed to assess, mediate, and enact rules and policies that address these issues [45, 73, 78, 79, 80].

Cyberprivacy in Ethics and Morality Context. Ethics and morality are considered as one of the important topics in selected papers [68, 81]. For example, literature have discussed about anonymity; sharing information on cyberspace; sharing of personal records [82]; communication ethics; piracy [83] and using copyrighted or outdated materials; demographic data collection transparency; and ethics of new cutting-edge technologies (e.g., VR [9], DM [8], tracking technologies [47], and autonomous vehicles [3]).

Cyberprivacy can be viewed from two perspectives. First, cyberprivacy concerns the morals and ethics of personal rights [8, 84], and thus protects against technological harm and misuse of personal information [68]. Second, too much privacy is against morality [3], as it can be misused for illicit activities or to hide information that can prevent other sorts of harm. To balance these contradictions, cyberprivacy needs to be considered in context rather than in abstract [8], and people can be objectified to understand their needs in concrete rather than in abstract [81]. As a result, the concept of moral mediators was introduced [81] to help understanding the morality of relationships between objects and humans. Furthermore, the concept of privacy and belonging to the persona needs revising [46] since objectifying privacy brings up the concept of ownership [3] and intellectual property rights mentioned earlier. Such application is thus seen beneficial in many ways, since it can resolve many of the contentious issues between technology and the right to privacy, e.g. censorship of individuals and services [67], violations by some governments or service providers [85, 86].

Cyberprivacy in Business and Economy Context. Many businesses rely on data to optimize services and reach consumers [87]; however, their practices may lead to privacy violations, and the spread of misinformation [41] and spam. PII is beneficial to the business; yet, data collection methods have the capacity to address a person more precisely than needed. Accordingly, literature has raised significant concerns, such as incidents [87] as database theft or data tampering [60].

Also, questions about the relationship and importance of cyberprivacy and trust to business have been discussed in literature [48, 87], as well as the need for privacy measures in technology and business for economic growth [85, 86]. For example, it has been shown that in developing economies [88] cyberlaw played a vital role in recovery and building business trust [85, 86]. The same was also seen [48] when well-known

business brands suffered value loss due to opaque practices and lack of privacy safeguards [60]. Other issues that have been discussed in selected papers are open supply chain and information access since they are associated with data ownership rights' risks [48], and practices of businesses asking for more information than required, as in social accounts and credit card approval [41].

Cyberprivacy in Risk and Insurance Context. Cyber risks are mostly intangible [54, 55] and have broad impacts on many levels. For example, cyber risks can lead to the loss of some rights in favor of other interests [9], they also can trigger interference and influence decision-making [89]. From selected papers, cyber risks can be grouped into two categories: risks that affect security and integrity of systems, and risks that affect users and their rights (e.g., privacy, possession, and control). Regarding privacy, the use of data for operations has brought several challenges, such as data ownership rights, lack of a standardized model to develop security and privacy techniques [90], the tradeoff between protection and utility [59], and misleading regulations [9, 48, 91, 92, 93, 94, 95]. As a result, many risks have been discussed, including social networking data manipulation and privacy issues [96]; marketing and service tracking technologies [10]; VR and AR [9]; and risks of lack of awareness [97].

Literature has discussed risk management as a tool to help reduce the impact of these risks by identifying and quantifying privacy risks according to significance and impact, and ensuring compliance with standards and established agreements [59]. Risk management can also help delegate and transform risks into monetary value [98]. However, most cyber risks do not have such an option as policies require physical proof of loss or damage [79, 80]. Still, it is possible to overcome these limitations by framing privacy as an intellectual property [99] and considering cyber risks as operational and technical incidents. Literature also discussed the cautiousness of insurers in offering cyber liability solutions due to the increase in the attack surface [90] and changes in cyberlaw [91, 92, 93, 94, 95]. In fact, less than 10% of insurers cover cyber risks [99].

Cyberprivacy in Behavior and Psychology Context. Literature has discussed in this context, for example, that the identity [84], self-expression, and behavior [7, 67, 84] have changed in cyberspace. This is because of the state of the cyborg [68, 100], interaction on social media [84, 96], and acting differently while wearing different identities [3]. As a result, the meaning of harm itself changed as it shifted more towards emotional and social [7, 84] harm, through discrimination and shame [46].

Cyberprivacy has much to do with these changes, such as being known to many circles [7, 46], being monitored while exercising rights [46], bullying, stalking, intimidation, harassment, and spreading misinformation [68, 96]. This was evidenced in [7, 101, 102, 103] where violence erupted through technology and increased visibility. Moreover, many prefer reasonably priced services with privacy safeguards than free services without any [96, 98]. Accordingly, privacy-centric solutions [46] should be always the first option to consider. Attention should be paid to creating awareness and disseminating information as users tend to be the weakest link [97]. Yet, for effectiveness, awareness should come from a high trustworthy authority [104] to be

accepted and fully adopted by end-users. Finally, psychological mediators [81] should be considered as they help form reasoning about actions and behavior.

Cyberprivacy in Society Context. From a societal perspective, two views are discussed: the right to be left alone and the need for societal interaction [11]. To balance these views, it is necessary to preserve privacy norms while engaging in social and societal activities by taking measures regarding sharing and sensitivity of information, and defining attributes to preserve privacy [59, 88, 105]. Accordingly, it is important to specify private and public attributes, deploy means for controlling own data, and balance the societal benefits of sharing information with privacy needs [59, 106].

One of the solutions is to create different spheres (e.g., private, public) to exercise rights within [66]. Another solution is defining privacy depending on the group-level since the meaning of privacy varies according to the group [64]. Nevertheless, it is necessary to update privacy for the society [78] and review technologies, regulations, and policies, to ensure compliance and consistency with privacy norms.

Cyberprivacy in the Healthcare Sector Context. The healthcare sector [106] has been always driven by personal data, thus [45] has considered ensuring data integrity and availability, as well as an adequate level of privacy. One issue is the significant privacy risks considering current technologies capabilities for identification of individuals. Trust in the healthcare sector is vital, as records can be used for inappropriate purposes. Still, information and data should be available to authorized parties upon request, to provide services and assistance as needed. Recently, health and fitness Apps and services have been a concern as they can pose privacy infringements. Accordingly, this issue requires careful consideration.

4.2 Cyberprivacy Definitions

As discussed previously, different views exist on cyberprivacy. E.g., the technical side views data as belonging to systems, and thus can be used for services and optimization. The legislative side views privacy and information as a protected right of owners. The commercial side sees data as an enabler to provide insights about consumers, etc. In Table 3, we developed and summarized the definitions related to cyberprivacy.

Table 3. Common context categories for analysis

Concept	Definition
1. Cyberprivacy (Technical view)	An extension of the domain of physical privacy in cyberspace, thus following the reasoning of what is permitted and what is not in physical domains
2. Cyberprivacy (Sociotechnical view)	The collective set of norms and measures necessary to protect and control the activities and characteristics of cyber-identity in cyberspace and related domains

Concept	Definition
3. Cyberprivacy (Rights view)	A concept that aims to maintain the rights to privacy, freedom, self-expression, self-determination, and reasonable behavior across cyberspace, and thus it is the intellectual ownership and accountability for storing, processing, and sharing information in cyberspace
4. Cyberprivacy (Legislation view)	A protection layer that aims to raise awareness against misuse of personal data, enforce control, and seek to amend data and attributes of pre-established relationships when needed

4.3 Issues of Cyberprivacy

The issue of cyberprivacy comes from the definition of identity and the prevalence of similar characteristics, the morals and ethics behind processes, and the transformation of humans into cyborg-like entities [3, 7, 8, 81, 84]. Although these are psychological and sociological changes, they only have resulted from advances in the ICT sector [107], as shown in Table 4.

Table 4. Advances in the ICT Sectors

Issue	Advances
Storage	High-density; New architectures; Cloud management; Remote management; & Data resiliency and Recovery protection
Processing and Recognition	Distributed Computing; Cloud; Natural Language Processing; Image and Voice Recognition; & Enabling new technologies: ML, AI, VR, and AI.
Communication	Enabling new technologies: SG, IoT, and SCs; Network and Telecom technologies; Connectively clouds and Quantum networking; Content sharing; real-time streaming; & Social media integration with e-services accounts
Data	BD, DM, Data visualization, and advances in data science; Automated data categorization; Precise analytics, statistics, and forecasting; & Profiling

5 Discussion

Cyberprivacy is a set of concepts and solutions that collectively provide protection against leakage of personal information and data. This makes it clear how cyberprivacy differs from cybersecurity and data privacy as cyberprivacy is a holistic concept that incorporates technical and non-technical issues within. Regarding implementation, the main approach to achieving cyberprivacy is to define core and conceptual protection measures and then proceed with the technical ones, bearing in mind that conceptual and technical measures are required simultaneously. Based on contexts and issues of cyberprivacy, we define the layers required to achieve cyberprivacy as in Figure 4.

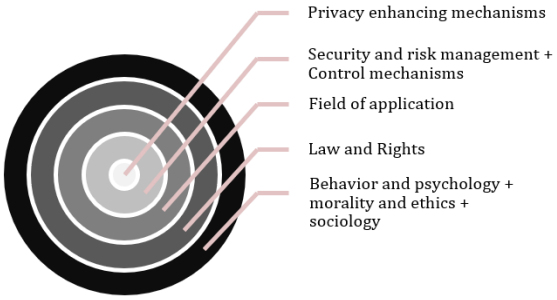


Figure 4: Layers of Cyberprivacy

Cyberprivacy is arranged in five layers that cover needs. First, norms and standards should be defined based on interaction and communication needs, then measured against moral and ethical standards to monitor their behavioral and psychological outcomes, and thus regulate and modify them as required. For this step, general frameworks of ethics and morality must be referred to, in addition to allowing a certain degree of flexibility, to suit different societies. Second, laws and regulations should define rights and obligations, what is permitted and what is not, and ensure enforcement through continuous monitoring of operations and processes. Here, laws and regulations should consider the scope and area of application, and therefore it is recommended to develop and use regulations that can be widely applied, e.g. GDPR. Third, the field of application brings specific and customized rules and policies of the sector or domain concerned, since these rules differ from one field to another.

The fourth- and fifth-layers deal with the application of the criteria, concepts, and approaches defined from the previous conceptual layers. Risk management is considered, thus to assess general risks of norms of the first two layers and specific risks associated with the field of application layer. Based on the results, measures are selected and adjusted. In particular, measures are based on cybersecurity and information security practices; however, control and monitoring mechanisms need to be integrated, to allow different parties to access, control, and monitor data based on permissions, privileges, and sensitivity. Finally, the fifth layer includes mechanisms to enhance and promote privacy; accordingly, this layer must consider anonymity and traceability. Anonymity can protect individuals and maintain the privacy of their data even in the event of data tampering, since data will not be linked to a specific entity. Traceability is required for communication, and to prove accountability for actions and information sharing. To enhance privacy, both criteria should be considered equally, thus permitting privacy without compromising or misusing the right. For this, identities should be separated from communication by means of using pseudonyms, and implementing separate identity domain management systems to provide linking and disengaging functions as required. Still, mechanisms for data removal after processing, opting out, changes tracking, and private data erasure, should be included.

Regarding the practical part, although out of the scope of this study, we have come across several solutions that can be used to provide a certain level of data privacy at the application layers, e.g. obfuscation [2, 53, 55], anonymizers [11, 41, 85], end-to-end

encryption [45, 53, 57], Public Key Infrastructure [46, 53, 57, 60, 66, 77, 85], differential privacy [2, 19, 51, 53, 55, 59, 77], k-anonymity [19, 53, 55, 59, 77, 82, 96, 104, 108], data minimization [40, 53, 59], Blockchain [56, 109], and others. However, as mentioned, these are methods of data privacy, but to achieve the level of protection targeted by cyberprivacy, protection should be considered across all layers simultaneously.

6 Conclusion, Future Research, and Limitations

We have addressed the topic of cyberprivacy in this study in the aim of understanding the context, concept, and cyberprivacy-related issues. We conducted a literature review on cyberprivacy and selected 79 papers for the study. We contribute to literature by providing eight contexts of cyberprivacy and their characteristics, i.e., technology, legislation, ethics, business, risk, psychology, society, and healthcare. These contexts indicate that cyberprivacy is not a single discipline, but it is an interdisciplinary approach that involves drawing appropriately from several disciplines to redefine problems outside of normal boundaries and reach solutions based on a new understanding of complex phenomena. We also contribute by providing the concepts of cyberprivacy in different views, i.e., technical view, sociotechnical view, rights view, and legislation view.

This study opens several opportunities for future research. First, future research should pay more attention to the four issues of cyberprivacy that emerged from this study, that is storage, communication, data, and processing and recognition. We argue that it is crucial to address these issues before they develop further in a negative way. Second, rapid digitalization, and technological change have been disrupting traditional norms in recent years [110, 111]. This indicates the importance of cyberprivacy in the new normal. As a result, an in-depth study on cyberprivacy in different contexts in digital transformation would strengthen our understanding on the subject, and it thus would help protect privacy in cyberspace. Third, there is an increasing ratio of renewable and decentral energy generation around the world [112]. This leads to growing trends in integration of ICT into electrical power systems, such as smart meters in households are connected to IoT devices over the Internet. This trend also brings cyberprivacy and cybersecurity threats to energy systems [113]. A study on cyberprivacy issues on the energy system is thus valuable for different parties as it could help to prevent physical consequences and very costly damages of data breaches in the energy system. Moreover, given that there is limited information regarding the educational perspective of cyberprivacy in selected papers, a study on cyberprivacy in higher education study programs would enhance cyberprivacy awareness and it also would help educate professionals in the field of cyberprivacy.

This study itself has its limitations. First, we focused on three databases: IEEEXplore, Finna, and Google scholar. Although Google scholar can cover all papers, some papers might not yet appear and thus were excluded from the study. Second, the time period of searching is 2008 to June, 2021. Articles accepted and published at the beginning of 2021 may not have been indexed by that point, and were thus excluded.

References

1. Demchak, C. C., and Fenstermacher, K. D. “Institutionalizing Behavior Based Privacy”. Admin. & Society, 41.7, 2009, pp 783-814.
2. Cranor, L. et al. “Towards a privacy research roadmap for the computing community”. arXiv preprint arXiv:1604.03160, 2016.
3. Magnani, L. “Chapter Seven Knowledge as a Duty: the ethical significance of the interest in information and knowledge”. Computing and Philosophy in Asia, 108, 2009.
4. Russell, D. et al. “Computer security basics”. O’Reilly, 1991.
5. Biselli, Tom, and Christian Reuter. "On the relationship between it privacy and security behavior: A survey among german private users." (2021).
6. J. Ma et al., “Perspectives on cyber science and technology for cyberization and cyber-enabled worlds”. Proc. CyberSciTech, New Zealand, 2016, pp 1-9.
7. Magnani, L. “Structural and technology-mediated violence: Profiling and the urgent need of new tutelary technoknowledge”. Intl. J. of Technoethics (IJT), 2.4, 2011, pp 1-19.
8. Magnani, L. “Abducing personal data, destroying privacy: diagnosing profiles through artefactual mediators”. Privacy, Due Process and the Computational Turn, Routledge, 2013, pp 81-104.
9. Yadin, G. “Virtual Reality Surveillance”. Cardozo Arts & Ent. L. J., 35, 2016, pp 707
10. Kimrey, B., and Clark, B. “Cyberprivacy and Digital Privacy Risks”. Comm. L., 29, 2012, pp 10.
11. Berghel, H. “Cyberprivacy in the new millennium”. Comp., 34.1, 2001, pp 132-134.
12. Post, D. “Cyberprivacy, or What I (Still) Don't Get”. Temp. Pol. & Civ. Rts. L. Rev., 20, 2010, pp 249.
13. Warren, S. D., and Brandeis, L. D. “The right to privacy”. Harvard L. Rev., 1890, pp 193-220.
14. Agre, P. E., and Rotenberg, M. “Technology and privacy: The new landscape”. MIT Press, 1998.
15. Loch, K. D., Conger, S., and Oz, E. “Ownership, privacy and monitoring in the workplace: a debate on technology and ethics”. J. of Bus. Ethics, 17.6, 1998, pp 653-663.
16. Foxman, E. R., and Kilcoyne, P. “Information technology, marketing practice, and consumer privacy: Ethical issues”. J. Public Policy & Marketing, 12.1, 1993, pp 106-119.
17. Hitachi Systems Security Inc. “Is Cybersecurity the Same as Data Privacy?” 2019, https://www.hitachi-systems-security.com/blog/is-cybersecurity-the-same-as-data-privacy/
18. Bashir, M. et al. “Information Privacy: Current and future research directions”. iConference, 2016.
19. “National Privacy Research Strategy”. Nat. Sci. Tech Council. 2016
20. Sponsler, C. “Cyberpunk and the Dilemmas of Postmodern Narrative: The Example of William Gibson”. Cont. Lit., 33.4, 1992, pp 625-644.
21. Mohamed, S. “Consensual hallucination & William Gibson”. 2010.
22. Singer, P. W., and Friedman, A. “Cybersecurity: What everyone needs to know”. Oup, USA, 2014.
23. Dukes, C. W. “Committee on national security systems (CNSS) glossary”. CNSSI, Fort Meade, MD, USA, Tech. Rep, 4009, 2015.
24. Craigen, D., Diakun-Thibault, N., and Purse, R. “Defining cybersecurity”. Tech. Innov. Mgmt Rev, 4.10, 2014.
25. “Framework for improving critical infrastructure cybersecurity”. Nat. Inst. Std. Tech. NIST, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf/

26. Thuraisingham, B. “Data mining, national security, privacy and civil liberties”. ACM SIGKDD Explorations Newsletter, 4.2, 2002, pp 1-5.
27. Taipale, K. A. “Data mining and domestic security: Connecting the dots to make sense of data”. Columbia Sci. Tech. L. Rev., 5.2, 2003.
28. Hayes, B. “Connecting the dots”. American Sci., 94.5, 2006, pp 400-404.
29. Seifert, J. W. “Data mining and the search for security: Challenges for connecting the dots and databases”. Govt. info. Qtly., 21.4,2004, pp 461-480.
30. Okoli, C., and Schabram, K. “A guide to conducting a systematic literature review of information systems research”. 2010.
31. Schryen, G. “Writing qualitative IS literature reviews—guidelines for synthesis, interpretation, and guidance of research”. Comm. Assoc. Info. Sys., 37.1, 2015, pp 12.
32. Rowe, F. “What literature review is not: diversity, boundaries and recommendations”. 2014.
33. Capurro, R., Eldred, M., and Nagel, D. “Digital whoness: identity, privacy and freedom in the cyberworld”. Walter de Gruyter, 2013.
34. Manovich, L. “Cultural analytics: visualising cultural patterns in the era of “more media”. Domus March, 2009.
35. Kelly, K. “The new socialism: Global collectivist society is coming online”. Wired Mag., 17.6., 2009, pp 17-06.
36. Godwin-Jones, R. “Emerging Technologies–Mobile-computing trends: lighter, faster, smarter”. Lang. Lrn. Tech., 12.3, 2008, pp 3-9.
37. Eagle, N., and Pentland, A. S. “Reality mining: sensing complex social systems”. Pers. ubiquitous Comp., 10.4, 2006, pp 255-268.
38. Hsieh, H. F., and Shannon, S. E. “Three approaches to qualitative content analysis”. Qual. H. Res., 15.9, 2005, pp 1277-1288.
39. White, M. D., and Marsh, E. E. “Content analysis: A flexible methodology”. Lib. trends, 55.1, 2006, pp 22-45.
40. Berghel, H. “PII, the FTC, Car Dealers, and You”. Comp., 47.5, 2014, pp 102-106.
41. Levit, N. “Family privacy bibliography”. J. American Acad. Matrimonial Lawyers, 17, 2009, pp183-255.
42. Bellaby, R. W. “Going dark: anonymising technology in cyberspace”. Ethics Info. Tech., 20.3, 2018, pp 189-204.
43. Sessler, J. B. “Computer cookie control: Transaction generated information and privacy regulation on the Internet”. J. L. Plcy., 5, 1996, pp 627.
44. Dodig-Crnkovic, G., and Horniak, V. “Togetherness and respect: ethical concerns of privacy in Global Web Societies”. AI Soc., 20.3, 2006, pp 372-383.
45. Kumar, S. R. et al. “Data-mining a mechanism against cyber threats: A review”. Intl. C. Innov. Cyb. Sec, IEEE, 2016, pp 45-48.
46. Peslak, A. R. “An ethical exploration of privacy and radio frequency identification”. J. Bus. Ethics, 59.4, 2005, pp 327-345.
47. Cooper, T., Faseruk, A., and Johnson, L. D. “Impact of Privacy and Confidentiality on Valuation: An International Perspective”. J. Fin. Mgmt. Anlys., 23.2, 2010.
48. Sadeeq, M. A. et al. “Internet of Things security: a survey”. Intl. C. Adv. Sci. Eng. ICOASE, IEEE, 2018, pp 162-166.
49. Lu, Y., Papagiannidis, S., and Alamanos, E. “Internet of Things: A systematic review of the business literature from the user and organisational perspectives”. Tech. Forecasting Soc. Change, 2018, pp 136, 285-297.
50. Liu, E., and Cheng, P. “Mitigating cyber privacy leakage for distributed dc optimal power flow in smart grid with radial topology”. IEEE Access, 6, 2018, pp 7911-7920.

51. Knapp, E. D., and Samani, R. "Chapter 4 Privacy Concerns with the Smart Grid". Appl. Cyb. Sec. Smart Grid, 2013, pp 2087-99.
52. Fhom, H. S., and Bayarou, K. M. "Towards a holistic privacy engineering approach for smart grid systems". Intl. C. Trust Sec. Priv. Comp. Comm., IEEE, 2011, pp 234-241.
53. Elmaghraby, A. S., and Losavio, M. M. "Cyber security challenges in Smart Cities: Safety, security and privacy". J. Adv. Res., 5.4, 2014, pp 491-497.
54. Braun, T. et al. "Security and privacy challenges in smart cities". Sustain. Cities Soc., 39, 2018, pp. 499-507.
55. Froomkin, A. M. "The death of privacy". Stan. L. Rev., 52, 1999, pp 1461.
56. Monti, M. et al. "An alternative information plan (Working paper)". Santa Fe Institute, 2017.
57. Adee, S. "Internet architecture". New Sci., 228.3051, 2015, pp 38-39.
58. Thuraisingham, B. et al. "Towards a Framework for Developing Cyber Privacy Metrics: A Vision Paper". Intl. Congress Big Data, IEEE, 2017, pp 256-265.
59. Palmer, C. C. "Preface: cybersecurity for a smarter planet". IBM J. Res. Dev., 58.1, 2014, pp 0–1.
60. Sovern, J. "Opting in, opting out, or no options at all: The fight for control of personal information". Wash. L. Rev., 74, 1999, pp 1033.
61. Bautista, A. "2010 Annual Survey: Recent Developments in Sports Law". Marq. Sports L. Rev., 21, 2010, pp 667.
62. Hansen, L., and Nissenbaum, H. "Digital disaster, cyber security, and the Copenhagen School". Intl. studies Qtly., 53.4, 2009, pp 1155-1175.
63. Simpson, B., and Murphy, M. "Cyber privacy or cyber surveillance? Legal responses to fear in cyberspace". 2014
64. Etzioni, A., and Rice, C. J. "Privacy in a cyber age: Policy and practice". Springer, 2015.
65. Schwartz, P. M. "Privacy and Democracy in Cyberspace." 2017.
66. Jin, C. H. "Self-concepts in cyber censorship awareness and privacy risk perceptions: What do cyber asylum-seekers have?" Comp. Hmn. Behav., 80, 2018, pp 379-389.
67. Isfandyari-Moghaddam, A. "Rocci Luppicini: Ethical impact of technological advancements and applications in society". 2013.
68. Bartholomew, M. "Intellectual Property's Lessons for Information Privacy". Neb. L. Rev., 92, 2013, pp 746.
69. Chatterjee, D. K. "Encyclopedia of Global Justice: A-I". Springer Sci. Bus. Media, 2011.
70. Saxby, S. "The 2012 CLSR-LSPI seminar on privacy, data protection & cyber-security". Intl. C. Lgl. Sec. Priv. Issues IT L. LSPI. Comp. L. Sec. Rev., 29.1, Athens, 2013, pp 4-12.
71. Black Jr, J. E. "Privacy Liability and Insurance Developments in 2012". J. Inet. L. 16, 2013, pp 3-12.
72. Reddick, C. G. "Citizens and e-government: Evaluating policy and management". Info. Sci. Ref., 2010.
73. Nolan, D. R. "Privacy and profitability in the technological workplace". Info. Tech. World Work, Routledge, 2017, pp 203-227.
74. Levinson, A. R. "Toward a cohesive interpretation of the electronic communications privacy act for the electronic monitoring of employees". W. Va. L. Rev., 114, 2011, pp 461.
75. Yu, S. "Big privacy: Challenges and opportunities of privacy study in the age of big data". IEEE access, 4, 2016, pp 2751-2763.
76. Huddleston, J. "Preserving Permissionless Innovation in Federal Data Privacy Policy". J. Inet. L., 22, 2019, pp.17-18.
77. Rosenzweig, P. "Cyber warfare: how conflicts in cyberspace are challenging America and changing the world". ABC-CLIO, 2013.

78. Breaux, R. W., Black, E. W., and Newman, T. “A Guide to Data Protection and Breach Response-Part 1”. Intellect. Property Tech. L. J., 26.7, 2014, pp 3.
79. Breaux, R. W., Black, E. W., and Newman, T. “A guide to data protection and breach response-part 2”. Intellect. Property Tech. L. J. 26.8, 2014, pp 23.
80. Magnani, L. “Material Cultures and Moral Mediators in Human Hybridization”. Intl. J. Technoethics IJT, 1.1, 2010, pp 1-19.
81. Hildebrandt, M. “Profile transparency by design? Re-enabling double contingency. Privacy, due process and the computational turn: The philosophy of law meets the philosophy of technology”. 2013, pp 221-46.
82. De George, R. T. “The ethics of information technology and business”. John Wiley & Sons, 2008.
83. Wiafe, I., Yaokumah, W. and Kissi, F.A. “Students' Intentions on Cyber Ethics Issues”. Mod. Theor. Prac. Cyber Ethics Sec. Compl, IGI Global, 2020, pp 105-121.
84. Warwick, K. “Cyborg morals, cyborg values, cyborg ethics”. Ethics Info. Tech., 5.3, 2003, pp 131-137.
85. Cross, F. B., and Miller, R. L. “The Legal Environment of Business: Text and Cases: Ethical, Regulatory, Global, and Corporate Issues”. Cengage Learning, 2011.
86. Quaddus, M., and Achjari, D. “A model for electronic commerce success”. Telecom. Plcy., 29.2-3, 2005, pp 127-152.
87. Karake-Shalhoub, Z., and Al Qasimi, L. “Cyber law and cyber security in developing and emerging economies”. Edward Elgar Publishing, 2010.
88. Thiele, R. D. “The new colour of war–Hybrid warfare and partnerships”. World Politics Sec., Rio de Janeiro: Konrad Adenauer Foundation, 2015, pp 47-59.
89. Barrett-Maitland, N., Barclay, C., and Osei-Bryson, K. M. “Security in social networking services: a value-focused thinking exploration in understanding users’ privacy and security concerns”. Info. Tech. Dev., 22.3, 2016, pp 464-486.
90. Biener, C., Eling, M., and Wirfs, J. H. “Insurability of cyber risk: An empirical analysis”. Geneva Papers Risk Ins. Issues Practice, 40.1, 2015, pp 131-158.
91. Eling, M., and Schnell, W. “What do we know about cyber risk and cyber risk insurance?” J. Risk Fin., 2016, pp 474-491.
92. Marotta, A. et al. “Cyber-insurance survey”. Comp. Sci. Rev., 24, 2017, pp 35-61.
93. Romanosky, S. et al. “Content analysis of cyber insurance policies: How do carriers write policies and price cyber risk?”. 2017.
94. Woods, D. et al. “Mapping the coverage of security controls in cyber insurance proposal forms”. J. Inet. Servs. Apps., 8.1, 2017, pp 8.
95. Thakur, K., and Kumar, H. “Challenges in protecting personated information in cyber space”. Intl. C. Emerging. Trends Nets. Comp. Comms. ETNCC, IEEE, 2015, pp 167-171.
96. Yan, Z. et al. “Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?”. Comp. Hmn. Behav., 84, 2018, pp 375-382.
97. Bughin, J. “Digital user segmentation and privacy concerns”. J. Direct Data Dig. Mktg. Practice, 13.2, 2011, pp 156-165.
98. Wright, M. F. “Cyber aggression within adolescents’ romantic relationships: Linkages to parental and partner attachment”. J. Youth Adolescence, 44.1, 2015, pp 37-47.
99. Murray, A. “Looking back at the law of the horse: Why cyberlaw and the rule of law are important”. SCRIPTed, 10, 2013, pp 310.
100. Magnani, L. “Distributed Morality in a Technological World, Knowledge as Duty”. Keynote speaker: 18, 2007.
101. Wright, M. F. “Intimate partner aggression and adult attachment insecurity: The mediation of jealousy and anger”. Evol. Behav. Sci., 11.2, 2017, pp 187.

102. Crane, C. A. et al. “Problematic alcohol use as a risk factor for cyber aggression within romantic relationships”. Amer. J. Add., 27.5, 2018, pp 400-406.
103. Carpenter, S. et al. “Expert sources in warnings may reduce the extent of identity disclosure in cyber contexts”. Intl. J. Hmn. Comp. Interact., 33.3, 2017, pp 215-228.
104. Lynch, K. “The global drivers of change”. OPTIONS POLITIQUES 2010, 2009.
105. Tschider, C. A. “Enhancing cybersecurity for the digital health marketplace”. Annals H. L., 26, 2017, p 1.
106. “Information and Communication Technologies: A World Bank Group Strategy”. World Bank Pub., 2002
107. Do, C. T. et al. “Game theory for cyber security and privacy”. ACM Comp. Surv. CSUR, 50.2, 2017, pp 1-37.
108. Awan, J. H. et al. “Cyber Threats/Attacks and a Defensive Model to Mitigate Cyber Activities”. Mehran Uni. Res J. Eng. Tech., 37.2, 2018, pp 359-366.
109. Xu, Hao, et al. “BeepTrace: blockchain-enabled privacy-preserving contact tracing for COVID-19 pandemic and beyond”. IEEE Inet. Things J., 2020.
110. Dang, D., and Vartiainen, T. “Digital strategy patterns in information systems research”, PACIS 2019 Proceedings, (2019).
111. Dang, D., and Vartiainen, T. “Changing patterns in the process of digital transformation initiative in established firms: the case of an energy sector company”, PACIS 2020 Proceedings, (2020).
112. Varela, I.: Energy Is Essential, but Utilities? Digitalization: What Does It Mean for the Energy Sector? In: Linnhoff-Popien, C., Schneider, R., and Zaddach, M. (eds.) Digital Marketplaces Unleashed. pp. 829–838. Springer, Berlin, Heidelberg (2018)
113. Dang, D., Vartiainen, T., and Mekkanen, M., “Towards Establishing Principles for Designing Cybersecurity Simulations of Cyber-Physical Artefacts in Real-Time Simulation,” Intl. C. Info. Sys. Dev. (ISD), (2021).

State of the Art in Cybersecurity and Smart Grid Education

Invited Paper

Andrejs Romanovs
Department of Modelling and Simulation
Riga Technical University
Riga, Latvia
andrejs.romanovs@rtu.lv

Jana Bikovska
Department of Modelling and Simulation
Riga Technical University
Riga, Latvia
jana.bikovska@rtu.lv

Janis Peksa
Department of Management Information Technology
Riga Technical University
Riga, Latvia
janis.peksa@rtu.lv

Tero Vartiainen
Computing Sciences Department
University of Vaasa
Vaasa, Finland
tero.vartiainen@uwasa.fi

Panos Kotsampopoulos
School of Electrical and Computer Engineering
National Technical University of Athens
Zografou 15780, Greece
kotsa@power.ece.ntua.gr

Bahaa Eltahawy
Computing Sciences Department
University of Vaasa
Vaasa, Finland
bahaa.eltahawy@uwasa.fi

Sebastian Lehnhoff
Carl von Ossietzky University
Oldenburg, Germany
sebastian.lehnhoff@uol.de

Michael Brand
OFFIS – Institute for Information Technology
Oldenburg, Germany
michael.brand@offis.de

Julija Strebko
Department of Modelling and Simulation
Riga Technical University
Riga, Latvia
julija.strebko@rtu.lv

***Abstract*—This paper was developed within the draft "Cybersecurity Curricula Recommendations for Smart Grids" framework. The paper deals with modern education in the field of cybersecurity of intellectual networks, using a systematic reading and analysis of literature from universities and private schools. Based on the research, basic conclusions were carried out, and essential requirements and recommendations were put forward for cybersecurity research programs on smart grids.**

***Keywords*—Education, Cybersecurity, Smart Grid**

I. Introduction

The European Union defines cybersecurity as one of the strategic digital capabilities [1] because IT's environmental security has a huge role to play [2]. The biggest problem in today's cybersecurity world is the lack of EU cybersecurity capabilities. The development of the EU strategy needs to increase collective resilience to cyber threats and all trusted services and digital tools [3].

EU received recommendations from the IEEE Committee on European Public Policy [4]:

- strengthen cyber resilience and response to cyber-attacks;
- rationalise the European cybersecurity regime into a common framework;
- support the development of effective cybersecurity certification schemes;
- facilitate regulatory compliance by stakeholders;
- promote cybersecurity education, awareness, and 'hygiene' habits;
- support research and innovation in cybersecurity.

The latest technologies are developing markets with new services and products. Nevertheless, that development leads to new cybersecurity threats. In the example of the energy sector, technological developments in this area can be seen by integrating digital calculations, communications, systems, and industrial management technologies. As Europe aims to move to a fully integrated internal energy market, all stakeholders must be informed about computer networks, software, integrated systems, and security management. The use of new technologies and large amounts of data in real-time leads to significant and new cyber threats, demonstrates the importance of education and training for cybersecurity threats on smart grids.

The paper consists of 4 sections. The introduction is followed by the second chapter that is devoted to the study method used for analysis. The third chapter provides the results of studies on strategic directions and the EU initiative. Furthermore, the fourth chapter provides the results of this study and a brief presentation of existing cybersecurity education programs.

II. Research Methods

The work used the following research methods:

- systematic literature review;
- universities and private education institutions study offering analysis.

The following primary sources have been studied carry out a systematic review of the literature:

- EU level political planning documents, regulations, and methodical materials (as ENISA recommendations, etc.) – published in institutions portals and web-pages;
- industry associations requirements and recommendations – published in industry portals and web pages;
- scientific papers regarding education in cybersecurity – published in scientific papers databases (IEEE digital library etc.).

The following keywords were used to search the selected sources:

- cybersecurity education;

978-1-6654-3299-3/21/$31.00 ©2021 IEEE

- smart grids cybersecurity education;
- smart grids security.

The main issues were raised for research:

- Q1 – What are EU strategic directions, requirements, and learning needs towards cybersecurity education?
- Q2 – What is the current cybersecurity education offering (with a focus on smart grids cybersecurity)?
- Q3 – What have identified gaps in cybersecurity education and improvement areas?

The results of the studies are detailed in the following paragraphs.

III. EU Policies, Industry Requirements, and Related Research

A. EU Policies and Strategic Directions

The European Commission has conducted research on the EU's digital capabilities, which identified the enhancement of knowledge, skills, and competencies in the field of cybersecurity as one of the EU's strategic instruments for digital transformation.

As already has been said, the energy sector must be developed at the highest level since it is currently part of essential services. Energy technologies must work at a higher level to ensure continuity in delivering essential services and strategic controls. The EU Cybersecurity Strategy [3][3] calls for a cyber-skilled workforce to respond to various cyber-attacks in a timely manner. In the meantime, unfortunately, cyber-readiness and awareness in companies and individuals are very low, and staff does not have sufficient cybersecurity skills. Therefore, the EU Cybersecurity Strategy argues that different kinds and forms of education should be directed towards cybersecurity themes and the integration of cybersecurity in this area.

The EU Digital Education Action Plan is based on two priorities [5]:

- fostering a high-performing digital education ecosystem;
- enhancing digital skills and competencies for the digital transformation.

This plan [5] focuses on awareness of cybersecurity among children and young people and small and medium-sized businesses. The plan states a need for adult accessible education, which involves raising qualifications and re-skilling convenient conditions for the learner.

Digital Europe program [1] focuses on promoting the EU's strategic digital potential and the deployment of digital technologies. The program continues to work on advanced skills and capacity strengthening in the EU Member States to ensure a consistent level of security for networks and information systems. Within the framework of the program, key actions have been taken to strengthen digital skills in the field of cybersecurity:

- develop new master programs (co-created together with EU cybersecurity excellence centers);
- introduce short-term specialized training courses for job seekers and employed people, especially SMEs and job placements.

Following academic offers and demand for Artificial Intelligence, High-Performance Computing, and Cybersecurity [5] research, the European Commission concluded that it was possible to extend master programs to the EU in the field of cybersecurity. It is necessary to identify problems, gaps and analyse them in other forms of learning.

European Parliamentary Research Service [7] said in a briefing that the energy system contains features that require a specialised industry approach to cybersecurity, in addition to cybersecurity standards and measures:

- real-time requirements;
- a mix of advanced and legacy technologies;
- cascading effects of disruption.

Experts from the Security and Resilience of Communication Networks and Information Systems for Smart Grids [8] argue that security awareness is of great importance to all stakeholders. The conclusions of the authors of the review show [8]: "cybersecurity in European Smart Grids requires well-trained proactive decision-taking operators of collaborating Smart Grid stakeholders to operate the next-generation Smart Grid infrastructure. Relevant stakeholders should generate the necessary expertise to design, build and maintain secure smart grid systems. To meet the increasing demand for ICT experts and ICT security experts with operational knowledge in electricity has become challenging and might require updating engineering and ICT education curricula". A training program consisting of four products (Fig. 1) is proposed, as training is offered throughout the life cycle of the new safety solutions for the intellectual networks. This type of training helps to be informed about all developments in the field of cybersecurity. Rapid development of ICT-based products generates high market demand on engineers with a multi-disciplinary background in cybersecurity, mathematics, IT and computer science, thus, the development of balanced study programs on one hand and motivation of students on another hand, allows bridging the gap between industry needs and educational output [8], [9].

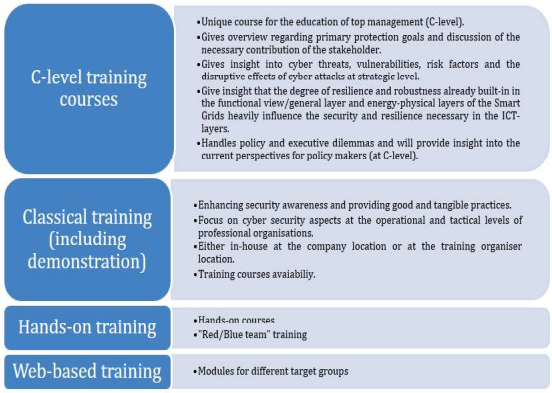


Fig. 1. European Commission Expert Group on the Security and Resilience of Communication Networks and Information Systems for Smart Grids curriculum recommendations

B. Industry Studies and Recommendations

Cybersecurity is essential not only in the energy sector but also in the ICT sector. Joint Task Force on Cybersecurity Education prepared the guiding principles of the Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity [11]. In the face of an increasing number of skilled cybersecurity professionals, The Joint Task Force has developed recommendations indicating that cybersecurity is an interdisciplinary training course. On the other hand, the thinking model consists of eight knowledge areas and eight cross-cutting concepts (Fig. 2).

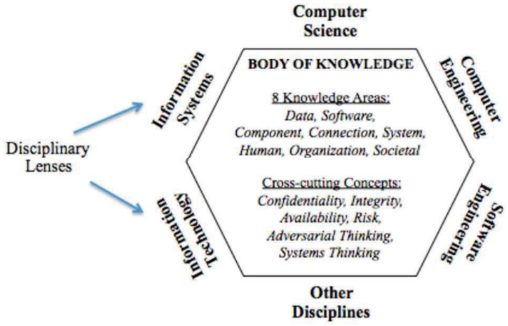


Fig. 2. Cybersecurity education curriculum thought model [11]

The Computing Engineering Association Committee for Computer Education in Public Colleges has prepared Cybersecurity Curricular Guidance for Associate-Degree Programs [12]. This manual used basic principles from the Curriculum Guidelines for Post-Secondary Degree Programs [11] but adapted to two-year programs. The training results are aligned with the NIST National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [13] and Centers of Academic Excellence – Cyber Defense (CAE-CD) Two-Year Knowledge Units [14].

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [15], which is assigned from the National Institute of Standards and Technology, is a benchmark model for the description of cybersecurity.

C. Scientific Research

Research on cybersecurity education is limited and focused on the development of online education platforms.

There is a module, practical and open education platform Smart Grid and supporting materials - TCIPG: Cyber Infrastructure for the Power Grid [16] from Yardley et al. Following the results of the study, this model does not meet the requirements of Smart Power Security Professional (SPSP) and is monolithic, leading to inadequate training. The study authors offer an educational platform that includes the following training topics [17]:

1. Cyberinfrastructure in the electric power grid;
2. Monitoring and situational awareness;
3. Advanced metering infrastructure;
4. Smart grid guidance documents;
5. Electric sector capability maturity model;
6. Privacy in the smart grid;
7. Critical infrastructure security examples and impact;
8. A perspective on security;
9. Security challenges in distribution automation;
10. Embedded assessment;
11. SCADA fundamentals;
12. Robust control systems.

Source [18] identified cybersecurity as an engineering tool and aimed to attract bachelor's students for cybersecurity purposes. Students could enter Smart Grid security studies with simulated cyberattacks and modeling.

IV. State of the Art in Education in Smart Grids and Cybersecurity

Higher education programs, continuous education programs, and massive open online courses (MOOC) can explore modern intellectual networks and cybersecurity.

A. Higher education study programs

Eighty-four universities offering training programs in information technology, starting with a bachelor's, were studied. All exploration programs are based on one concept, like an introductory course that gives cybersecurity. There are also practical courses for a bachelor who can learn skills and acquire knowledge in theory and practice. Of the 84 universities, 14 do not meet the overall cybersecurity criteria because the Information Technology, Computer Science, or Computer Systems programs are insufficient to investigate cybersecurity.

Master-level programs focus more on cybersecurity, considering knowledge before studies are launched. Such a level of program benefits that graduated already have experience in cybersecurity.

Doctoral programs have an even higher level of training in the field of cybersecurity. Of all 70 universities directed to Cybersecurity, only one offers a specific direction in cybersecurity: Cybersecurity and Software Technology Doctoral Program. This university is proud because it is the world leader in cybersecurity and software technologies. The developed doctoral program involves scientists from around the world in various disciplines, providing skilled and known researchers to graduate courses [19].

B. Continuing education programs

The development of intellectual networks, including Smart Grid, does not stand on the ground and continues to grow with billions of investments. Thanks to the development of Smart Grid, there is a need to address many cybersecurity challenges that are crucial to success. Source [16] authors point to the educational frameworks required: Active Learning, Project-based Learning, Piaget's learn-by-doing posture, and constructivism.

Smart Grid cybersecurity research can be assisted by various professional training courses [16], including the recently launched Global Information Assurance Certification (GIAC) certification program. This program is known as the Global Industrial CyberSecurity Professional Certification (GICSP) [20], which evaluates the expertise needed for this sector's security course. Other approaches are also used to train Smart Grid:

- Samurai SCADA security course [21];

- Cybati's Critical Infrastructure and Control System Cybersecurity course [22];
- SCADAhacker's Industrial Control System Cyber Security Training course [23];
- SANS ICS410 ICS/SCADA Security Essentials [24];
- Cimation's ICS/SCADA Security courses [25].

K12 pupils in the EU and US will soon learn the basics of cybersecurity. Due to the establishment of the CS and the basis for cybersecurity in the K12 Florida system [26].

As EU research shows, there is a clear division of knowledge, competencies, and precise national divisions. Each knowledge unit is covered in most large countries, e.g., in Spain, France, Germany, and Italy, 75% of knowledge units (KUs) are covered. Nevertheless, the size of the country is not an indicator that there will be a high percentage of knowledge (Fig. 3, Fig. 4) [27].

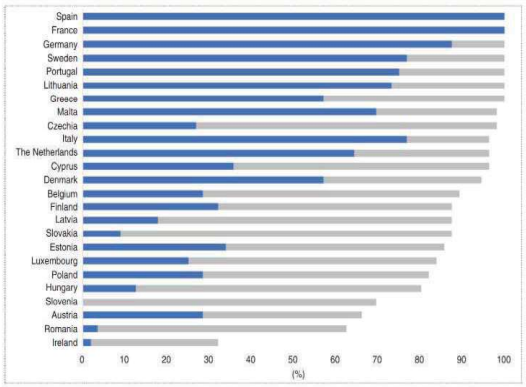


Fig. 3. The percentage of the KUs that each country covers with mandatory courses (blue) and other courses (gray) [27]

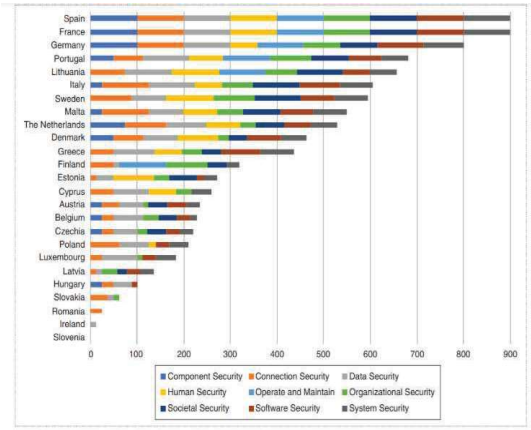


Fig. 4. The percentage of each knowledge areas and knowledge units covered with mandatory courses for each country [27]

C. *Massive open online courses (MOOC)*

Online courses are becoming more popular, and one of the reasons is that many will want to acquire knowledge and certificates. Source [28] authors report 35 online courses on cybersecurity that fit the NICE structure. Online course studies based on edX MOOC analysis in cybersecurity can result in gaps between what is provided and what employers are requiring. Based on the results of these studies, a series of recommendations were put forward for course preparation, and a platform with an open-source code for further analysis of student outcomes on the edX platform was established.

Machine learning [29] requires cybersecurity expertise and artificial intelligence; of the 72 points initially found, only 15 research, where cyber-security online courses were reviewed. Of those, three studies involved some cybersecurity MOOCs, while 12 dedicated to individual courses. The results of the study analysis showed that there is no information available in the academic literature on the online delivery of artificial intelligence cybersecurity [29].

In conclusion, MOOC does not provide 100% of the result because all online courses are different. It should also be noted that the MOOC has a place to develop in cybersecurity and intellectual networks, providing practical examples with the possibility of working in real-time.

V. Conclusion and Recommendations

Unambiguously, the development and improvement of cybersecurity and smart grids skills are significant, supported by EU political documents, sectoral studies, and recommendations. The sources studied also talk about the need for available training in the field of cybersecurity.

At the end of the work, the following conclusions have been drawn based on an overview of the literature:

1. In the EU, there is a significant and persistent digital skills gap. The current education offer of specialized education programs does not address all needs (especially for adults who want to re-skill or up-skill and new specialists).
2. Cybersecurity education has been identified as one of the strategic digital skills in the EU that needs to be straightened by providing formal and informal education (including VET, continuing education) and topics practical application (practicing) in organizations' R&D projects.
3. Cybersecurity is represented in different education forms, as Higher education, Continuing education, MOOC. However, smart grid security topics are addressed relatively rarely.
4. Cybersecurity programs include various topics; organizational security (security operations and personal security) and the knowledge unit system retirement are the least covered [30].
5. The main findings coming from the literature review and university Cybersecurity offer in both the EU and the USA are pretty similar, and yet, the technical reporting coming from the universities is more theoretical. At the same time, the MOOC and continuing learning provide specific knowledge with a greater emphasis on the practical side.
6. Slim divisions from the literature on EU countries indicate that study courses are intense, but students are not prepared at lower levels.

7. Explicit Smart Grids study courses are not currently available in university study programs, but in MOOC, they are available and are also available in continuing education programs with certificate supporting documents.

On the other hand, when developing cybersecurity training programs for smart grids, EU policy and industry research make the following recommendations and requirements:

1. Education must be accessible for different EU citizens groups (including enterprises, C-level managers, adults who want to up-skill and re-skill, and new specialists).
2. It is recommended to provide cybersecurity distance, online and blended learning opportunities to make up-skilling and re-skilling more accessible to adults.
3. The education must address general cybersecurity grounds and industry-specific topics (energy supply chain cybersecurity and tools/methods and measures on monitoring and controlling it).
4. It must provide theoretical lectures and practical training, as the use of cybersecurity management tools (as SIEM, etc.) and virtual laboratories, perform simulations and experiments using digital twins and similar environments. In smart grids cybersecurity education, specific smart-grid-related cybersecurity tools, like energetics domain controllers monitoring tools, are essential.
5. Education and training programs must be developed in collaboration with relevant partners (like universities and industry representatives).
6. In cybersecurity of smart grids programs, attention should be paid to all these domains [8]: Confidentiality, Integrity, and Availability (including performance and timeliness) as well as data privacy (the combination of organization, integrity, and confidentiality) and non-repudiation (e.g., electronic contracts). So, the scope is broader than only data security since data security is only one of the security aspects (though important) while implementing the smart grids in Europe [8].
7. Cybersecurity topics should be integrated as a mandatory part of energy studies programs.
8. It is recommended to integrate gamification elements to students, like, threat games, cyber ranges, and cybersecurity escape rooms, to make cybersecurity education more interactive and attractive.
9. In the context of relevant higher cybersecurity education, student mobility should be considered as part of programs.

As part of the project, two questionnaires were developed for sectoral companies and educational institutions, which will help to analyze the current situation in the field of cybersecurity in grid.

ACKNOWLEDGMENT

Cybersecurity Curricula Recommendations for Smart Grids (CC-RSG) project is funded by the Erasmus+ Strategic Partnership program. The European Commission is not responsible for the content of this publication.

REFERENCES

[1] European Commission (2020). *Europe investing in digital: the Digital Europe Programme*. [Online] Available: Europe investing in digital: the Digital Europe Programme | Shaping Europe's digital future (europa.eu)

[2] European Union agency for cybersecurity (2020). A trusted and cyber secure Europe. ENISA Strategy. [Online] Available: a-trusted-and-cyber-secure-europe-enisa-strategy (europa.eu)

[3] European Commission (2020). The EU Cybersecurity Strategy for Digital decade. [Online] Available: The EU's Cybersecurity Strategy for the Digital Decade | Shaping Europe's digital future (europa.eu)

[4] Cybersecurity for a stronger and more resilient digital Europe. An IEEE European Public Policy Committee Position Statement (2020). [Online] Available: An IEEE European Policy Committee Position Statement

[5] European Commission (2020). The Revised Digital Education Action Plan. [Online] Available: Digital education action plan (update) (europa.eu)

[6] European Commission Joint Research center (2019). Academic offer and demand for advanced profiles in the EU: Artificial Intelligence, High Performance Computing and Cybersecurity. [Online] Available: Academic offer and demand for advanced profiles in the EU | EU Science Hub (europa.eu)

[7] Cybersecurity of critical energy infrastructure. Briefing of European Parliamentary Research Service (2019). [Online] Available: Cybersecurity of critical energy infrastructure

[8] Kunicina, N., Zabasta, A., Nikiforova, O., Romanovs, A., Patlins, A. Modern Tools of Career Development and Motivation of Students in Electrical Engineering Education. From: 2018 IEEE 59th International Scientific Conference on Power and Electrical Engineering of Riga Technical University (RTUCON 2018): Conference Proceedings, Latvija, Riga, November 12-14, 2018. Piscataway: IEEE, 2018, 1.-6.lpp. ISBN 978-1-5386-6904-4.

[9] Romanovs A., Soshko O., Merkuryev Y. Information Technology Focused Training in Logistics. In: 2010 9th International Conference on Information Technology Based Higher Education and Training, ITHET 2010. Turkey, Cappadocia, 29 April - 1 May, 2010. - pp 27-34. ISBN 978-142445792-2

[10] European Commission Expert Group on the Security and Resilience of Communication Networks and Information Systems for Smart Grids (2020). Cyber Security of the Smart Grids. Summary Report.

[11] Joint Task Force on Cybersecurity Education (2017). Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. [Online] Available: csec2017_web.pdf (acm.org)

[12] Association for Computing Machinery (ACM) Committee for Computing Education in Community Colleges (CCECC) (2020). Cybersecurity Curricular Guidance for Associate-Degree Programs. [Online] Available: ccecc.acm.org/files/publications/Cyber2yr2020.pdf

[13] Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2020). [Online] Available - NICE Cybersecurity Workforce Framework | National Initiative for Cybersecurity Careers and Studies (cisa.gov)

[14] Centers of Academic Excellence – Cyber Defense (CAE-CD) Two-Year Knowledge Units (2020). [Online] Available - Cyber Defense CAE Overview.pdf (nsa.gov)

[15] National Initiative for Cybersecurity Education (NICE) (2017). NICE Cybersecurity Workforce Framework. NIST Special Publication 800-181.

[16] T. Yardley, S. Uludag, K. Nahrstedt and P. Sauer, "Developing a Smart Grid cybersecurity education platform and a preliminary assessment of its first application," 2014 IEEE Frontiers in Education Conference (FIE) Proceedings, Madrid, 2014, pp. 1-9, doi: 10.1109/FIE.2014.7044273.

[17] TCIPG web page [Online], Available - TCIPG: Trustworthy Cyber Infrastructure for the Power Grid

[18] D. Navarro, J. C. Méndez, K. Berríos, E. Ortiz-Rivera and E. Arzuaga, "Using cybersecurity as an engineering education approach on computer engineering to learn about Smart Grid technologies and the next generation of electric power systems," *2014 IEEE Frontiers in Education Conference (FIE) Proceedings*, Madrid, 2014, pp. 1-8, doi: 10.1109/FIE.2014.7044336.

[19] De Montfort University Leicester, Cyber Security and Software Technology Doctoral Programme [Online]. Available: https://www.dmu.ac.uk/study/technology/doctoral-training-programme/cyber-security-doctoral-programme.aspx

[20] Global Information Assurance Certification (GIAC). (2014) Global Industrial Cyber Security Professional Certification (GICSP). [Online]. Available: http://www.giac.org/certification/global-industrial-cyber-securityprofessional-gicsp

[21] Utilisec. (2014) Assessing and Exploiting Control Systems with SamuraiSTFU. [Online]. Available: http://www.samuraistfu.org/training-syllabus

[22] Cybati. (2014) Critical Infrastructure and Control System Cybersecurity. [Online]. Available: https://cybati.org/education

[23] SCADAhacker. (2014) Industrial Control System Cyber Security Training. [Online]. Available: http://www.scadahacker.com/training.html

[24] SANS. (2014) ICS410 ICS/SCADA Security Essentials. [Online]. Available: http://www.sans.org/course/ics-scadacyber-security-essentials

[25] Cimation. (2014) ICS/SCADA Security Courses. [Online]. Available: http://www.cimation.com/training/

[26] G. Javidi, E. Sheybani, "K-12 Cybersecurity Education, Research, and Outreach" 2018 [Online]. Available: https://ieeexplore-ieee-org.resursi.rtu.lv/stamp/stamp.jsp?tp=&arnumber=8659021

[27] N. Dragoni, A. L. Lafuente, F. Massacci, A. Schlichtkrull, "Are We Preparing Students to Build Security In? A Survey of European Cybersecurity in Higher Education Programs", 2021 [Online]. Available: https://ieeexplore-ieee-org.resursi.rtu.lv/stamp/stamp.jsp?tp=&arnumber=9336077

[28] González-Manzano, L. and de Fuentes, J.M., 2019. Design recommendations for online cybersecurity courses. Computers & Security, 80, pp.238-256.

[29] Laato, S., Farooq, A., Tenhunen, H., Pitkamaki, T., Hakkala, A. and Airola, A., 2020, July. AI in Cybersecurity Education-A Systematic Literature Review of Studies on Cybersecurity MOOCs. In 2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT) (pp. 6-10). IEEE.

[30] Cybersecurity for Europe project deliverables (2020). D6.2 Education and Training Review [Online]. Available: Deliverables | CyberSec4Europe | Cyber Security for Europe

Towards A Massive Open Online Course for Cybersecurity in Smart Grids – A Roadmap Strategy

Bahaa Eltahawy
Computing Sciences Department
University of Vaasa
Vaasa, Finland
bahaa.eltahawy@uwasa.fi

Andrejs Romanovs
Department of Modelling and Simulation
Riga Technical University
Riga, Latvia
andrejs.romanovs@rtu.lv

Maria Valliou
School of Electrical and computer Engineering
National Technical University of Athens
Athens, Greece
mariavalliou@mail.nuta.gr

Tero Vartiainen
Computing Sciences Department
University of Vaasa
Vaasa, Finland
tero.vartiainen@uwasa.fi

Jirapa Kamsamrong
OFFIS e.V.
Oldenburg, Germany
jirapa.kamsamrong@offis.de

Mike Mekkanen
Computing Sciences Department
University of Vaasa
Vaasa, Finland
mike.mekkanen@uwasa.fi

***Abstract*— The major trends and transformations in energy systems have brought many challenges, and cybersecurity and operational security are among the most important issues to consider. First, due to the criticality of the energy sector. Second, due to the lack of smart girds' cybersecurity professionals. Previous research has highlighted skill gaps and shortage in cybersecurity training and education in this sector. Accordingly, we proceeded by crafting a roadmap strategy to foster cybersecurity education in smart grids. This paper outlines the methodology of teaching cybersecurity in smart grids to a large group of students in selected European universities via implementing a Massive Open Online Course. Unlike other solutions, this one focuses on hands-on practical skills without trading-off theoretical knowledge. Thus, flipped learning methodology and gamification practices were used to maximize retention rate. Also, a remote lab that includes a real-time simulator was established for training. Here, the process, outcome, and obstacles to overcome in future deployments, are presented.**

Keywords—MOOC, Cybersecurity, Curricula, Training, Smart Grids, Real-time Simulator

I. INTRODUCTION

The energy sector has recently witnessed major changes that resulted in the concept of smart grids. As defined, "a smart grid is an electricity network that can intelligently integrate the behavior and actions of all users connected to it such as generators, consumers, and those that do both, to efficiently deliver sustainable, economic and secure electricity supplies" [1] [2]. Accordingly, cybersecurity of the smart grid has become one of the most important issues to address, due to the increase in the attack surface, and the criticality of assets connected. Cybersecurity has long been identified as one of the European Union digital capabilities to achieve [3]. "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets" [4]. Many tools and software packages from different vendors, e.g. [5] [6], already exist to cover security needs and to ensure grid robustness, however, the issue with cybersecurity is still prominent.

In Cybersecurity Curricula Recommendations for Smart Grid (CC-RSG)[1] project, this issue was investigated more closely using surveys, reviews and workshops, and results indicated the following:

1. Cybersecurity topics are not well addressed [7].
2. The lack of cybersecurity professionals in the smart grid field due to scarcity of education that covers this specific field [8] practically.
3. Existing educational offers do not meet the Smart power Security Professional (SPSP) requirements [7]
4. Lack of real-life scenarios [8] and connection with industry [9]

It is clear the critical need for educational offers that can strengthen skills and fill the above-mentioned gaps, especially in light of previous reports that indicate that 50% of cybersecruity incidents at least are merely human error [10]. In our project, the aim is to help post-secondary insitutions include learning outcomes about cybersecury in smart grids in their curricula. In this paper, we present our work in designing a course that is able to cover the required skills without compromising the theoretical knowledge. The remainder of this paper is organized as follows: Section II presents the research methods adopted. Section III introduces educational methodologies and the different learning approaches. Section IV is dedicated to the Massive Open Online Course (MOOC). In Section V, we present our approach and steps considered for the course design. Section VI is for discussion and faced challenges. Finally, Section VII concludes with summary and future work.

II. RESEARCH METHODS

This work adopts the practices of the Design Science Research (DSR) methodology specified in [11]. Processes are shown in Fig. 1. below.

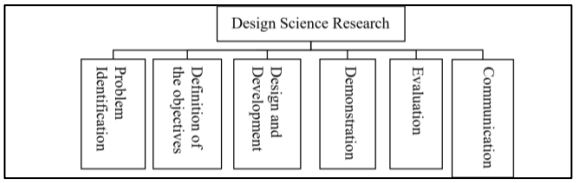


Figure 1: Design Science Research processes [11]

[1] CC-RSG is an Erasmus+ funded project focusing on cybersecurity from an educational perspective. The project has partners from Finland, Germany, Latvia and Greece. More information: https://www.uwasa.fi/en/research/projects/cybersecurity-curricula-recommendations-smart-grids-cc-rsg

The primary resources that have been used are:

1. CC-RSG project reports [8] and [12]
2. Scientific papers in the field of education, from scientific paper databases (IEEE, AIS, etc.)
3. Technical papers and manuals from manufactures websites.

The main issue covered by this research is "How to design an effective MOOC course to raise knowledge and awareness of cybersecurity in smart grid systems?" Next, we take the steps to answer this question considering educational and technical perspectives and needs.

III. Educational methodologies & Learning Approaches

As highlighted above, there is a lack of educational offers and educators that can cover theoretical and technical aspects of cybersecurity in smart grids. The educational methodology plays a vital role here as it specifies how learning objectives are met and validated. Depending on the level of retention targeted, different educational methodologies and approaches exist [8] [13] [14], e.g., lecture-based, experiential, active learning, cooperative learning, flipped learning, inquiry-based, problem and project-based learning, and gamification.

In brief, lecture-based learning [15] is the traditional model in which the instructor delivers the material, carries assessments, and is fully responsible on the educational experience. This approach is mostly passive and depends on memorization; however, as practiced in [16], by adding activities including, e.g. cold calling, discussions, learning cards, and so, this model can turn active and more effective. Experiential learning [17] is an active learning approach in which students engage in the learning process and learn by gaining and developing experience. Active learning [18], despite what the name implies, is not just about including activities and participating in the learning process, but is rather the participation of all learners and processing of their responses before new information is presented. Cooperative learning [19] refers to an approach in which participants work in teams on a certain task or a project to meet certain criteria and take full responsibility for completing the task. Flipped learning [20] is a modern approach that enables participants to take full ownership on learning by distributing educational material beforehand, thus allowing more room for a dynamic interactive guided environment to take place in the classroom. Inquiry-based learning [21] is an approach in which students follow the same practices of professional scientists in order to build similar knowledge and experience. Problem and project-based learning [22] are approaches that actively engage participants in the learning process by exploring a specific problem/question with the aim of finding answers or developing a solution. Finally, gamification [23] is the use of featurs commonly found in games (e.g., storytelling, level-beating, badges) with the aim to encourage participation. About effectiveness and learning retention, as the given approaches promote different activities, they vary in their retention rates. Fig. 2 [24] shows these differences.

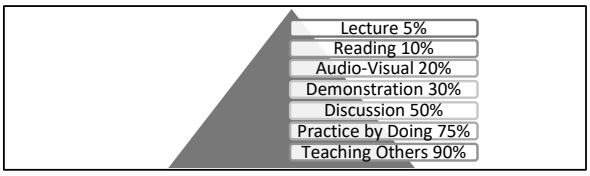


Figure 2: Retention rate of different learning activities [24]

From Figure 2, it is clear that the greater the number of activities, the shift towards the learners' space and the engagement an approach promotes, the higher the retention rate, and thus more knowledge and skills acquired.

Finally, the method of delivery itself has a great impact on the educational process. Previous research [25] has revealed that although distant online courses feature higher flexibility, they have lower rates – 50 to 80% – to retain students compared to 80 to 90% with face-to-face courses. On the other hand, online learning and blended learning [26] [27] [28], which combines face-to-face learning with computer-mediated instruction, showed better effectiveness in achieving the learning goals as well as higher performance since they allow for a semi-guided interactive environment between participants and instructors. To remove any ambiguity, it is worth mentioning that an online course can still be considered face-to-face if it has a synchronous live interaction [29].

Based on the explained methodologies and the different factors that affect the educational process, and to meet with CC-RSG project main goals of promoting knowledge of cybersecurity in smart grid and covering existing gaps, a MOOC has been designed. In the next section, a justification of this method is given, in addition to more details about MOOCs design models.

IV. Massive Open Online Course Approach

A. Introduction

According to [30], a MOOC is an "online course designed for large numbers of participants, that can be accessed by anyone anywhere as long as they have an internet connection, is open to everyone without entry qualifications, and offers a full/complete course experience online for free". By this definition, the main pillars and benefits of a MOOC are accessibility, flexibility, being affordable and not requiring much knowledge beforehand. While these are great benefits, MOOCs face two main concerns. First [31], the lack of guidance, structure and support that traditional courses offer. Second [32] [33], issues related to less reliability, pedagogical structure, homogeneity and depersonalization of course offerings. Fortunately, with academic institutions entering the MOOCs market [34], e.g. Stanford university with Coursera Platform and MIT with edX, some of these issues – especially the second set – were fixed, after adopting academic guidelines.

In terms of coverage, MOOCs mostly cover diverse topics with less emphasis on specialization and advanced courses [34]. Accordingly, different types and formats of MOOCs exist to cater to different needs and goals of different topics. In Table I, the main types of MOOCs are briefly highlighted.

TABLE I. Main MOOC Types Explained [34] [35]

Type	Definition	Focus
Extended, xMOOC	"Traditional e-learning courses organized by universities".	Knowledge duplication
Connective, cMOOC	Courses that "emphasize creation, creativity, autonomy, and social networking learning".	Knowledge creation
Social, sMOOC	"Social courses characterized by interactivity using social networks"	Active participation and engagement
Transfer, tMOOC	Courses "generating interest towards action and professional interaction	Transfer of learning and Pedagogical transformation

From Table I, although there is a clear distinction between the different types of MOOCs, in practice a MOOC offering may combine more than one format to effectively cover its curriculum. Chapter IV explains and exemplifies this clearly.

B. MOOC Instructional Design Models

As mentioned, MOOCs combine eLearning approaches and tools with pedagogical learning methodologies. Thus, to successfully design a MOOC, general Instructional Design (ID) models should be referred to. In brief, ID [36] is the "principles and procedures by which instructional materials, lessons, and whole systems can be developed in consistent and reliable fashion", or as described in [37], it is "the planning, creation, refinement, selection sequencing, managing and evaluating activities and resources in support of targeted goals and objectives". ID is thus the application of learning theories [37] [38], e.g., behaviorism (gradual attempt and error, reinforcement, and stimulus-response sequence), cognitivism (formation of cognitive structure), constructivism (learner-centered, collaboration and communication, appropriate resources), and connectivism (creating networks – the role of social and cultural context). Various ID models exist to provide guidance and direction on developing course content, the most famous of which are [38] [39]:

1) Bloom's Taxonomy: A model for measuring learning progress, in which levels of learning and related activities are represented in a hierarchical order that includes remembering at the bottom, then understanding, applying, analyzing, evaluating, and finally creating at the top. Depending on the expected outcome, the activities can be designed accordingly.

2) Gagne's Nine Events Model: A description of instructional events required for effective learning, i.e. gain attention, inform objectives, recall prior knowledge, present the content, provide guidance, practice, provide feedback, assess performance, and finally enhance retention/transfer.

3) ADDIE Model: A framework of the processes required for course design/development, which include: Analyze, Design, Develop, Implement, and Evaluate. The framework supports continuity by including revision instances between different processes.

4) Merrill's Principles: Identified principles common to effective ID models, which are: task/problem-centered, activation of prior knowledge, demonstration of new knowledge, application, and encouraging integration.

5) Dick and Carey Model (Systems Approach Model): A model for planning lessons through: defining instructional goals, conducting instructional analysis, defining entry requirements, specifying performance objectives as well as test items, developing instructional strategy and material, and finally conducing a formative and summative evaluation.

The processes and practices of these or other ID models should be adopted and modified to meet the desired outcomes of a MOOC, especially since MOOCs need a specific ID curriculum [40]. Next, we present our approach on designing a MOOC for cybersecurity in smart grid.

V. MOOC For Cybersecurity in Smart Grid

A. Course Elements

First, MOOCs that cover general topics of cybersecurity already exist. However, as our previous research [7] [12] revealed, specific topics as cybersecurity in smart grids are rarely if not at all covered. This was the motivation for initiating this course. Second, by performing the reviews presented in Chapters II and III, and by following guidelines of [41], the elements and approach needed to design an effective course, were identified, adopted, and adjusted. In Table II, the proposed approach is presented.

TABLE II. Course Design Approach

#	Element	Description
1	Learning Objectives	To cover the gap of cybersecurity knowledge related to smart grids
2	Prerequisites to join this course?	The course is **ONLY** open to students and professionals with pre-knowledge in the fields of cybersecurity and smart grids
3	Retention level projected by this course	60% to 75%, aiming at active discussions and simple practice by doing tasks
4	Type of MOOC adopted	xMOOC, with practices of tMOOC
5	Instructional Design methodologies adopted	ADDIE and Dick and Carey models for design, and targeting the third level – applying – of Bloom's Taxonomy for retention.
6	Approaches used	Flipped learning and gamification mainly, with tasks that promote cooperative learning
7	Method of delivery	Supervised recorded sessions (lectures and tutorials) with online face-to-face mediation by instructors
8	Criteria to increase attention and engagement	Bonus points, the use of games, and discussion forums
9	Assessment and Measurement	Regular quizzes and a final exam
10	Credits	5 credit points (ECTS = 125-140 hours of lectures, exercises, and self study material)

Regarding the selection of specific criteria, justifications are:

1. Point 2: the course covers a very specific topic, which is the reason why pre-knowledge is mandatory.
2. Point 3: as the main aim is active participation, discussions and simple practice by doing tasks can fulfill such criterion.
3. Point 5: with MOOC offers and large number of participants, resources cannot match the needs to analyze, evaluate or create levels. These levels require higher engagement and fewer participants.
4. Points 9 and 10: according to general academic standards, 1 credit point is 25 to 28 study hours.

B. Real-Time Simulation for Education

Real-time simulation [42] [43] is a technique in which a computer model simulates a physical system in approximately the same amount of time it takes in real time. Unlike other simulation techniques, real-time simulators are powerful computer platforms that allow a code to execute near the real-time it would take in reality with minimum delay. These systems can solve highly complex equations and consider many attributes simultaneously that typical simulation systems cannot provide. Accordingly, real-time simulation systems are used for applications [43] that include large scale systems, control of actual operating conditions, automotive simulation, automation, robotics, and power systems.

Here, to cover the practical part of the course, real-time simulator is used to create a cyber-physical testbed to simulate power systems and events that may emerge. Such a testbed can be used for [44], e.g., vulnerability analysis, disturbance scenarios, assessment metrics, impact analysis, and training. In Fig. 3, a typical testbed consisting of Intelligent Electronic Devices (IEDs) controller connected to a Real-Time simulator (OPAL-RT) and a communication and network simulator (EXATA Server), is shown. Such a testbed can be connected with other systems, e.g., SCADA, to run one of the mentioned tests, or used individually to develop attack and mitigation scenarios.

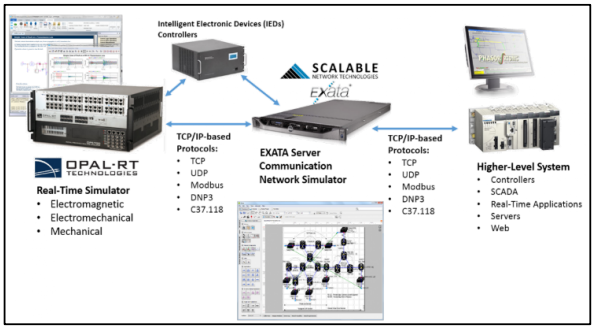


Figure 3: Cyber-physical testbed (adopted from [45])

The shown testbed is used to show students the actual work using the Real-Time simulator and its capabilities to simulate power systems and attack scenarios, and to train students to use the general components and settings of the system. As mentioned in the next section, pre-designed models will be used to perform this task efficiently.

C. Course Syllabus

Teaching and supporting material were selected to reflect on the goals of the course and to cover the gaps found previously. In Table III, the course structure in the form of modules that cover the different topics, is presented. Noting that one module is typically covered in two lectures.

TABLE III. COURSE STRUCTURE

Module and Goals	Material
Module #1 Fundamentals of Smart Grids To learn about: 1. Smart Grid Infrastructure 2. Cyber-physical Systems	• **Pre-reading material** 1. "Ready or not, here comes the smart grid!" 2. "Smart grids: A cyber–physical systems perspective" 3. "Smart grid for a sustainable future" • **Main Material and handouts** "Smart Grids Infrastructure Technology and Solutions"
Module #2 Cybersecurity and Operational Security in Smart Grids To learn about: 1. Cybersecurity fundamentals 2. Operational security 3. Smart Grid Security	• **Pre-reading material** 1. "Cyber-security in smart grid: Survey and challenges" 2. "Cyber-security on smart grid: Threats and potential solutions" 3. "Cyber-physical systems security: Limitations, issues and future trends" • **Main Material and handouts** "Applied Cyber Security and The Smart Grid"
Module #3 IEC 61850 and IEC 62351 To learn about: 1. IEC 61850 grid communication standard 2. IEC 62351 security standard for IEC 61850	• **Pre-reading material** 1. "Overview of IEC 61850 and Benefits" 2. "IEC 61850 for power system communication" 3. "Iec tc57 wg15: Iec 62351 security standards for the power system information infrastructure" • **Main Material and handouts** "IEC 61850 Communication Protocol Manual"
Module #4 Fundamentals of Real-Time simulation systems To learn about: 1. Real-Time simulation systems	• **Pre-reading material** 1. "Review of real-time simulator and the steps involved for implementation of a model from MATLAB/SIMULINK to real-time." 2. "Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed" 3. "Cyber security of a power grid: State-of-the-art" • **Main Material and handouts** "Real-time simulation technologies: Principles, methodologies, and applications"
Exercises and Lab #1 Opal RT Simulator To learn about: 1. Real-Time simulation systems	• **Main Material and handouts** "Opal RT user manual"
Exercises and Lab #2 Exercises and case scenarios To learn about: 1. Implementation and simulation	• **Main Material and handouts** Pre-designed models to run and test

D. Delivery Strategy

About the actual and detailed strategy of delivering the course, it goes as follows:

1. Course objectives and schedule are announced and communicated to participants.
2. A MOOC course page is created and hosted by one of the course hosting platforms (Moodle platform [46] is selected for this purpose following its rich features).
3. Guest access is enabled to allow enrollment of participants from other institutions, and also continuing education professionals. Access will be approved by instructors after assessing pre-knowledge.
4. A repository of the course content is created and divided into modules that cover the different topics.
5. For each module, there a section for a pre-reading material list that contains 2 to 3 general articles about the topic to be covered. This should be available and announced one week at least before the scheduled lecture.
6. Lectures' materials, e.g., presentations, handouts and other supporting materials, are also designed and uploaded to the lecture's section one week beforehand.
7. A set of 3 to 4 short videos – 15 to 20 minutes each – covering the main topic of the lecture, is recorded and published on the scheduled day of the lecture.
8. Simple pre-lecture quizzes consisting of 3 to 4 multiple choice, match, and true and false questions that cover the pre-reading material list, are designed.
9. Pre-lecture quizzes open on the scheduled lecture's time and last for 10 to 15 minutes.
10. To avoid any sort of plagiarism, it is advised to create a questions bank, thus questions would differ from a participant to another.

11. Quizzes results should be considered as bonus points or count only for up to 5% of the course's grade.
12. On the scheduled time of the lecture, recorded videos are played and facilitated/supervised by course instructors who are present online. After each video, 10 to 15 minutes are given to questions and any discussions.
13. A game, simple competition, or a similar activity that is related to the lecture's topic, could be created on one of the gaming platforms, e.g., Kahoot [47] or similar ones, and played in the middle of the lecture. Points received are considered bonus points as well.
14. A forum that hosts different topics open for discussion is created. Topics can be defined beforehand or emerge as needed.
15. For assessment, similar to points 8, 9 and 10, a questions bank is created to cover the main material of the lecture. Questions should be of auto-graded type, i.e., multiple-choice, multiple selection, true and false, fill in the blank and so on.
16. 15 to 20 questions are randomly selected from the questions bank for the weekly quizzes.
17. Weekly quizzes are available one day after the lecture and for a period of a week. Once a quiz is open, it can be completed within a certain timeframe, e.g. 30 minutes. After that, the quiz cannot be taken or open again.
18. Weekly quizzes should count for 60 to 70% of the course's final grade.
19. Regarding exercises and practical skills, 2 to 3 exercise sessions based on study cases and also to conduct a supervised remote connection with the lab, are given at the second part of the course once theoretical background is established and covered.
20. Students are encouraged to try given pre-designed models, to learn the general concepts and criteria regarding the system in place.
21. Finally, after the course completion, questions already existing in the questions bank can be reused to design an exam covering the whole content of the course, e.g. 50 to 60 questions that can be answered in 2 to 3 hours. The final exam contributes 30 to 40% of the course's final grade.

VI. Discussion and Challenges

Knowledge and awareness of cybersecurity operations are essential for the energy sector to mitigate incidents and disruption scenarios. Although many courses exist on different fields of cybersecurity, such specific domains are not well covered. The main issues that current courses face are, either they are more academic or more practical, however, offers that combine both are rarely found. To fix this gap by designing a MOOC course that covers this topic, it was found that the topic has more perspectives than the technical one. First, MOOC types were investigated carefully to find out which type is more suitable to deliver the content and how to adjust it to meet the objectives of the course. Second, back to basics, instructional design models provide the foundation for designing an effective course, therefore, before embarking on course design – whether traditional, online, or a MOOC – the ID model should be selected carefully. After defining the MOOC type and the ID type, designing a course is rather a straight forward process following the available guidelines.

Regarding implementation, we have encountered the following challenges:

1. Resources: MOOCs by default are open to large number of students, therefore all side tasks of the course, e.g. evaluation, should be automated, to optimize resources and provide time for the more important tasks, e.g., mediation, discussion, and so.
2. Retention rate: Depending on the assigned resources, the targeted rate of retention should be adjusted. However, typically for courses with no contact teaching, it is difficult to achieve higher retention rates that match with analyzing and creating criteria.
3. Retaining students: One of the main issues online courses face is the low completion rate which is due to lack of interest, interaction, and assistance. This was solved by opting for supervised sessions, discussion forums, and the use of simple gamification practices to encourage engagement.
4. Technical challenges regarding exercises and tutorials: Real-Time simulators are not available in every organization as they are very costly. Moreover, they have limited user licenses so they cannot be used remotely by several users. Therefore, a Virtual Priavate Network (VPN) connection is being established, and time slots are being distributed upon needs to participants who want to connect remotely to the cyber-physical lab for practicing. To make the process more efficient and to allow more students to practice, pre-designed models are provided, thus participants can move forward to running models and trying the different configurations.

As the time of this writing, the course is yet to be completed and deployed. After that, results of the last two phases of the DSR– evaluation and communication – methodology will be available, and accordingly any measures needed to improve the course will be considered.

VII. Conclusion and Future Work

This paper presents the roadmap for desgining an effective MOOC that is able to fill the cyberspecutiy knowledge gap in the field of smart grids. It was found that:

1. MOOC are resource intensive if they try to imitate traditoinal contact courses, especially in very specifc topics, as the one of this paper. Therefore, measures were taken to automate the educational process and to optimize resoucres, thus to give more time for interaction and engagment.
2. Techniques as flipped learning and gamification if well adjusted, they can provide such optimization and engagament required.
3. Retention rate cannot be the same as contact teaching.
4. By using techuiqes as remote access and VPN, partcipants could practice and gain practical knowledge, and thus create a richer MOOC experience.

In continuation of this work and as a part of CC-RSG project, this course is generalized and a framework for cybersecurity educaiton in smart grids will be developed.

Acknowledgment

CC-RSG project is funded by the Erasmus+ Strategic Partnership program. The European Commission is not responsible for the content of this publication.

REFERENCES NEW

[1] European Technology Platform, European Commission, “Strategic deployment document for Europe electricity networks of the future”, April 2010.

[2] Elzinga, David. "Electricity system development: A focus on smart grids. overview of activities and players in smart grids." UNECE. www. unece. org/fileadmin/DAM/energy/se/pdfs/eneff/eneff_h. news/Smart. Grids. Overview. pdf, (2015).

[3] European Commission (2020). Europe investing in digital: the Digital Europe Programme.

https://digital-strategy.ec.europa.eu/en/activities/digital-programme

[4] ITU. 2009. Overview of Cybersecurity. Recommendation ITU-T X.1205. Geneva: International Telecommunication Union (ITU). https://www.itu.int/rec/T-REC-X.1205-200804-I/en

[5] Young, Susan, and Dave Aitel. The hacker's handbook: the strategy behind breaking into and defending networks. Auerbach publications, 2003.

[6] Vacca, John R., ed. Managing information security. Elsevier, 2013.

[7] Romanovs, Andrejs, et al. "State of the Art in Cybersecurity and Smart Grid Education." IEEE EUROCON 2021-19th International Conference on Smart Technologies. IEEE, 2021.

[8] Valliou, Maria, et al. "Strategy for Cybersecurity Education in Smart Grids." (2022).

[9] González-Manzano, Lorena, and Jose M. de Fuentes. "Design recommendations for online cybersecurity courses." Computers & Security 80 (2019): 238-256.

[10] Arora, Bela. "Teaching cyber security to non-tech students." Politics 39.2 (2019): 252-265.

[11] Peffers, Ken, et al. "A design science research methodology for information systems research." Journal of management information systems 24.3 (2007): 45-77.

[12] Kamsamrong, Jirapa, et al. "State of the Art, Trends and Skill-gaps in Cybersecurity in Smart Grids." (2022).

[13] Merriam, Sharan B., and Lisa M. Baumgartner. Learning in adulthood: A comprehensive guide. John Wiley & Sons, 2020.

[14] Becker, S. Adams, et al. NMC horizon report: 2017 higher education edition. The New Media Consortium, 2017.

[15] Shi, Yinghui, et al. "Examining interactive whiteboard-based instruction on the academic self-efficacy, academic press and achievement of college students." Open Learning: The Journal of Open, Distance and e-Learning 33.2 (2018): 115-130.

[16] Hall, Steven R., et al. "Adoption of active learning in a lecture-based engineering class." 32nd Annual frontiers in education. Vol. 1. IEEE, 2002.

[17] Kolb, David A. Experiential learning: Experience as the source of learning and development. FT press, 2014.

[18] Felder, Richard M., and Rebecca Brent. "Active learning: An introduction." ASQ higher education brief 2.4 (2009): 1-5.

[19] Felder, Richard M., and Rebecca Brent. "Cooperative learning." Active learning: Models from the analytical sciences 970 (2007): 34-53.

[20] Bergmann, Jonathan, and Aaron Sams. Flipped learning: Gateway to student engagement. International Society for Technology in Education, 2014.

[21] Keselman, Alla. "Supporting inquiry learning by promoting normative understanding of multivariable causality." Journal of Research in Science Teaching 40.9 (2003): 898-921.

[22] English, Mary C., and Anastasia Kitsantas. "Supporting student self-regulated learning in problem-and project-based learning." Interdisciplinary journal of problem-based learning 7.2 (2013): 6.

[23] Deterding, Sebastian, et al. "From game design elements to gamefulness: defining" gamification"." Proceedings of the 15th international academic MindTrek conference: Envisioning future media environments. 2011.

[24] Lalley, J., and R. Miller. "The learning pyramid: Does it point teachers in the right direction." Education 128.1 (2007): 16.

[25] Carr, Sarah. "As distance education comes of age, the challenge is keeping the students." Chronicle of higher education 46.23 (2000).

[26] Means, Barbara, et al. "The effectiveness of online and blended learning: A meta-analysis of the empirical literature." Teachers college record 115.3 (2013): 1-47.

[27] Ward, Barbara. "The best of both worlds: A hybrid statistics course." Journal of Statistics Education 12.3 (2004).

[28] Ryan, Sarah, et al. "The effectiveness of blended online learning courses at the community college level." Community College Journal of Research and Practice 40.4 (2016): 285-298.

[29] Boelens, Ruth, et al. "Blended learning in adult education: towards a definition of blended learning." (2015).

[30] Jansen, Darco, and Robert Schuwer. "Institutional MOOC strategies in Europe." Status Report Based on a Mapping Survey Conducted in October-December 2014 (2015).

[31] L17 Kim, Sung-Wan. "MOOCs in higher education." Virtual learning (2016): 121-135.

[32] Fischer, Gerhard. "Beyond hype and underestimation: identifying research challenges for the future of MOOCs." Distance education 35.2 (2014): 149-158.

[33] Vardi, Moshe Y. "Will MOOCs destroy academia?." Communications of the ACM 55.11 (2012): 5-5.

[34] Palacios Hidalgo, Francisco Javier, Cristina A. Huertas Abril, and M. Gómez Parra. "MOOCs: Origins, concept and didactic applications: A systematic review of the literature (2012–2019)." Technology, Knowledge and Learning 25.4 (2020): 853-879.

[35] Osuna-Acedo, Sara, Carmen Marta-Lazo, and Divina Frau-Meigs. "From sMOOC to tMOOC, learning towards professional transference: ECO European Project [De sMOOC a tMOOC, el aprendizaje hacia la transferencia profesional: El proyecto europeo ECO]." Comunicar ART-2018-105258 (2018).

[36] Reigeluth, Charles M. "Instructional design: What is it and why is it." Instructional-design theories and models: An overview of their current status 1 (1983): 3-36.

[37] Spector, J. Michael. Foundations of educational technology: Integrative approaches and interdisciplinary perspectives. Routledge, 2015.

[38] Huang, Ronghuai, J. Michael Spector, and Junfeng Yang. Educational technology a primer for the 21st century. Springer, 2019.

[39] Brown, Abbie H., and Timothy D. Green. The essentials of instructional design: Connecting fundamental principles with process and practice. Routledge, 2015.

[40] Kopp, Michael, and Elke Lackner. "Do MOOCs need a special instructional design." EDULEARN14 Proceedings 71387147 (2014).

[41] Dietz-Uhler, Beth, Amy Fisher, and Andrea Han. "Designing online courses to promote student retention." Journal of Educational Technology Systems 36.1 (2007): 105-112.

[42] Faruque, MD Omar, et al. "Real-time simulation technologies for power systems design, testing, and analysis." IEEE Power and Energy Technology Systems Journal 2.2 (2015): 63-73.

[43] Popovici, Katalin, and Pieter J. Mosterman, eds. Real-time simulation technologies: Principles, methodologies, and applications. CRC Press, 2017.

[44] Poudel, Shiva, Zhen Ni, and Naresh Malla. "Real-time cyber physical system testbed for power system security and control." International Journal of Electrical Power & Energy Systems 90 (2017): 124-133.

[45] “SCALABLE and OPAL-RT Innovate Cyber-Physical Solution.” *Scalable Network Technologies,* 5 July 2017, www.scalable-networks.com/news/scalable-and-opal-rt-innovate-cyber-physical-solution.

[46] Rice, William, and H. William. Moodle. Birmingham: Packt publishing, 2006.

[47] Dellos, Ryan. "Kahoot! A digital game resource for learning." International Journal of Instructional technology and distance learning 12.4 (2015): 49-52.

Towards a Model for Assessing the Effects of Social-Cyber-Physical Threats on the Future Power Grid – Review and Workshop Results

Petra Berg
School of Marketing and Communication and VEBIC
University of Vaasa
Vaasa, Finland
petra.berg@uwasa.fi

Sonja Monica Berlijn
Electrical Power Engineering
KTH Royal Institute of Technology
Stockholm, Sweden
berlijn@kth.se

Bahaa Eltahawy
Digital Economy Research Platform
University of Vaasa
Vaasa, Finland
bahaa.eltahawy@uwasa.fi

Patrik Hilber
Electromagnetic engineering and fusion science
KTH Royal Institute of Technology
Stockholm, Sweden
hilber@kth.se

Mazaher Karimi
School of Technology and Innovations
University of Vaasa
Vaasa, Finland
mazaher.karimi@uwasa.fi

Karina Barnholt Klepper
The Norwegian Defence Research Establishment (FFI)
Kjeller, Norway
karina-barnholt.klepper@ffi.no

Linda Turtola
Industrial management
University of Vaasa
Vaasa, Finland
linda.turtola@uwasa.fi

Andrea Ulshagen
The Norwegian Defence Research Establishment (FFI)
Kjeller, Norway
Andrea.ulshagen@ffi.no

Qianwen Xu
Electrical Power Engineering
KTH Royal Institute of Technology
Stockholm, Sweden
qianwenx@kth.se

***Abstract*— The energy system, including the electrical power system, is currently undergoing major changes to meet increased demands and climate target plans, and to stand against potential malicious activities and all sorts of disruptions. Specifically, the electrical power system is drastically changing with regards to consumption, production, transmission, control, monitoring, markets, and digitalization. Such a change, however, makes the power system an attractive and vulnerable target to all kinds of disruptive events and social-cyber-physical attacks since the system is crucial for the functioning of the society and economy. In this work, to act against such events and to study the future power system's susceptibility and resilience towards social-cyber-physical attacks, the Resilient Digital Sustainable Energy Transition (REDISET) project has shown the need for a new model that is able to describe the future electrical power system in a way that reflects the future reality. In this paper, existing power systems models, the changing landscape of power systems, the drivers for a new model, the suggested model that comprises 7 building blocks instead of today's 3, and finally a direction of future related work are presented.**

Keywords—Power Grid, Resilience, Social-cyber-physical Threats.

I. Introduction and Background

With the current unprecedented global changes, the energy system, including its subdomains, such as the electrical system, is undergoing a substantial transition into a fully digitalized, cyber-physical system. These changes are driven by the increased demands and shifts in the market, the need to meet climate target plans, achieve sustainable development goals, and enhance resilience against potential malicious activities and other disruptive events. Specifically, due to digitalization, the electrical system is currently witnessing changes in monitoring, protection, and control systems across generation, transmission, and distribution plants. While these changes bring about new opportunities, products, added services, expanded markets, and an improved user experience, they also increase the complexity and vulnerability of the power system. This accordingly renders the power system susceptible to various disruptive events, ranging from minor malfunctions to large-scale cyber-physical attacks, resulting in significant social and economic impacts. Existing smart energy models, e.g., NIST [1] and SGAM [2], could provide guidance on the structure of the power system's components and interaction in a hierarchical manner. However, they lack a thorough consideration of the "human risk" factor, as in organizational cybersecurity-culture [3] and policy implications [4]. Recent attempts, e.g., [5] and [6], have partially addressed this gap by introducing integrated and interdisciplinary gird models, considering different domains, levels, and interactions, holistically, rather than separately, as previously done. This work acknowledges these efforts, and as a part of the Resilient Digital Sustainable Energy Transition (REDISET) project – which is a research project combining academic institutions and energy providers in Finland, Sweden, and Norway – it continues in the same direction.

In this work, we thoroughly examine the power grid system from the threats angle to answer the following question: *"How to assess the effects of social-cyber-physical threats on the future power grid?"* The aim of this multidisciplinary research is to counter social-cyber-physical threats affecting the grid, and to assess the future power system's susceptibility and resilience against such vulnerabilities.

The remainder of this paper is organized as follows: Section II describes the research approach. Section III highlights existing models of power systems, workshop results, and the changing landscape. Section IV follows with our proposed model for assessing the effects of social-cyber-physical threats on the future power grid, are presented. Section V concludes and suggests future work directions.

II. Research Methods

To comprehensively address our research question from both the conceptual and practical sides, two research approaches were employed in this research. First, a rapid

review method [7] was used to gather information on existing energy models. Second, qualitative research in the form of workshops [8] was conducted, to discuss these models, the challenges they face, and gain insights and suggestions on filling the identified gaps. For the latter, two workshops were held, involving multidisciplinary experts from academia and industry, focusing on exploring power models and their social aspects. Figure 1 shows a schematic diagram of the research methodology employed. Table 1 presents a description of workshops and participants.

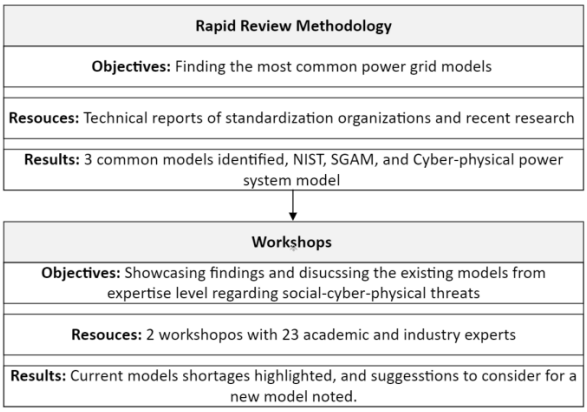


Figure 1. Research method

TABLE I. WORKSHOPS DESCRIPTIONS

Attribute	Description
Dates	October 27th, 2022, and February 17th, 2023
Location	KTH, Royal Institute of Technology, Stockholm, Sweden
Countries involved	Sweden, Finland, and Norway
Research institutions involved	4: KTH from Sweden, University of Vaasa from Finland, and FFI and NTNU from Norway
Companies involved	7: Ellevio, Svenska Kraftnät, Vattenfall, Statnett, Fingried, Hitachi Energy, and Sintef
Total number of participants, present or online	23
Academic participants	14
Industrial participants	9

In the following section, the most common energy models from selected articles as well as workshop results on these models and the evolving landscape, are presented.

III. REVIEW AND WORKSHOPS RESULTS

A. Review summary on existing power system models

First, though the existence of various power systems models that describe power systems from different perspectives, the review has identified three common models, namely, ISO/IEC Smart Grid Architecture Model (SGAM), NIST's framework, and the Cyber-physical power system model, as follows:

1) SGAM Model

The ISO/IEC Smart Grid Architecture Model (SGAM) [2], as shown in Figure 2, is a hierarchical layered representation of smart grids, consisting of five interactive layers that represent different domains and their associated objectives. The model encompasses the business, function, information, communication, and component layers, in which the latest encompasses the domains of the energy sector, i.e., generation, transmission, distribution, Distributed Energy Resources (DER), and customer premises. Furthermore, the component layer is also divided into different zones, i.e., process, field, station, operation, enterprise, and market, depending on the function to be performed. With such a structure and flexibility, the SGAM model is well-suited to showcase, simulate, and implement various use cases and scenarios covering different aspects of smart grids [9].

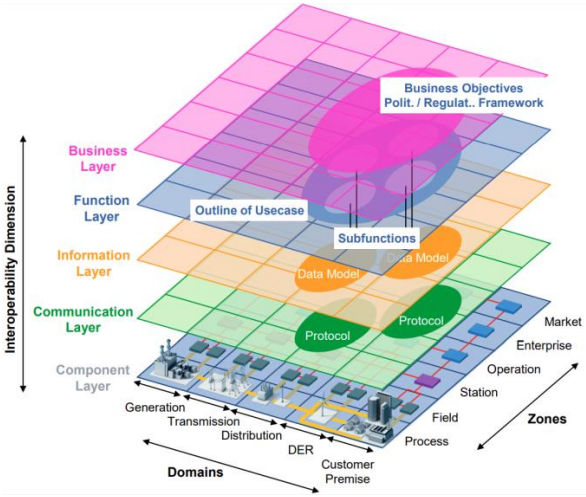


Figure 2. SGAM model (adopted from [2])

2) Smart Grid Conceptual Model

NIST's framework, the Smart Grid Conceptual Model (SGCM) [1], is a high-level framework that illustrates the roles and responsibilities, as well as the interactions between the different domains within the power grid. The model, as shown in Figure 3, encompasses the operations, service provider, customer, generation, transmission, markets, and distribution planes, delineating the lines needed for information exchange from the direct energy exchange ones, forming the actual grid. With its distinct detailed roles, SGCM acts as a guideline for understanding the grid by different stakeholders and is used for developing standards that ensure interoperability and seamless communication among the grid's components, thus enhancing the efficiency, reliability, sustainability, and resilience of the power system.

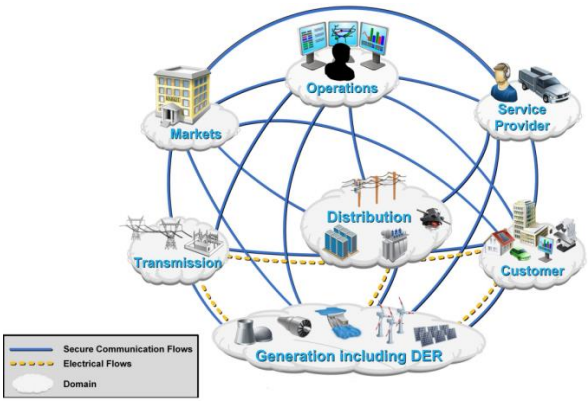


Figure 3. NIST's SGCM model (adopted from [1])

3) Cyber-Physcial Power Model

In the Cyber-Physical Power Model [10], power systems are modelled as cyber-physical systems, combining a physical power system, a control center (cyber layer), and communication between the two. As shown in Figure 4, the model's physical power system comprises a generation system including various DER, a transmission and distribution system, and customers. The cyber system, i.e. the control center, performs monitoring, operation, optimization, and control functions. Finally, the communication network handles sensors' measurements and control commands between the two systems. With its structure, the model effectively separates the actual grid and explicitly adds a cyber layer, where all information flow and control functions are executed.

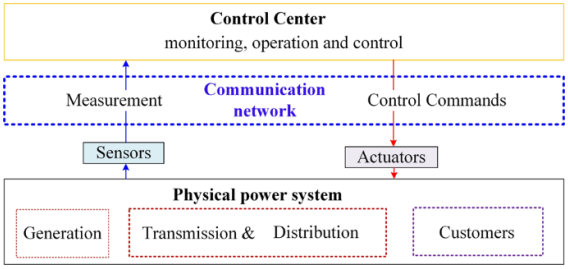


Figure 4. Cyber-physical power model (adopted from [10])

B. Applicability and deficiencies of the existing models – Workshop results

Although the given models provide comprehensive views on modeling the grid, they also exhibit several deficiencies. First, SGAM model suffers from complexity and lacks flexibility due to its segmented layered approach. Furthermore, issues [2] highlighted in the literature include formal functional description, the need for a well-defined interfacing tool for the architectural structure, and difficulties with automatic testing and configurations. Second, SGCM model faces similar complexity, flexibility, and interoperability limitations. In addition [11], the model faces concerns related to confidentiality, privacy, and compliance with anti-trust laws; hindrance in deployment due to being voluntary in the private sector; and human error, including user awareness in the customer domain and user errors in the operations domain. Finally, the cyber-physical power model's control center is oversimplified, considering that many Transmission System Operators (TSOs), Distribution System Operators (DSOs), producers, and larger consumers, have multiple control and monitoring centers, infrastructure monitoring centers, dispatch centers, and cyber surveillance centers, alongside switch centers. Moreover, the model lacks clarity addressing the market system.

Other notes that were emphasized during the workshops include: 1) The existing models are highly technical and lack on addressing the human factor adequately; 2) Building on the preceding point, the models neglect behavioral aspects such as social-cultural matters and their impact on the energy sector; 3) There is a lack of emphasis on privacy and cybersecurity issues; 4) Additionally, they fail to incorporate emerging technologies, e.g., Artificial Intelligence (AI) and blockchain.

C. Changing landscape

The abovementioned concerns, along with ongoing changes in the energy system, make it vulnerable and more susceptible to cyber and physical attacks. As modern society is more reliant on electricity, hostile actors can exploit weaknesses such as outages and instabilities to pose threats to our communities. Grid operators, i.e. TSOs and DSOs, have already witnessed a significant increase in cyberattacks. Additionally, the interdependencies within the current energy system can be exploited in international conflicts and hybrid warfare, as seen in Russian cyberattacks in 2015 [12], [13] and attacks on Ukrainian power infrastructure since February 2022 [14], to cause major disruptions and blackouts. These conflicts have led to what is called the "energy war", where energy resources are manipulated for political purposes. Alongside cyber threats, issues like the maintenance of nuclear reactors in France and the decommissioning of German nuclear power plants, shed light on the interdependencies within the European energy system, highlighting the risk of energy shortages and poverty. Given the vital role of energy supply and delivery in modern society, they have become a target for adversaries. Thus, ensuring the security and resilience of the energy infrastructure is crucial for the functioning of our society.

IV. Proposed Model for Future Power System

A. Social-Cyber-Physical grid model

Based on the reviews conducted and the workshop results, a system-of-systems energy model that explicitly emphasizes social-cultural aspects and disruptions, is proposed. The model, as shown in Figure 5, encompasses seven system domains, as follows: 1) supply system; 2) demand system; 3) transmission/distribution infrastructure system; 4) market system; 5) control system; 6) disruption system; 7) and, the social-cultural system. As the name indicates, every system of the proposed model encompasses its own sub-systems, which might vary depending on many factors and the types of DERs used, for example. Here and for simplicity, we present the proposed model from an abstract high-level view.

1) Supply System

The main purpose of the supply system is to generate and supply electricity and create revenue for investors and producers of electricity. Key functions of the supply system are:

- Generating electricity from different resources through energy conversion processes.
- Providing inertia, frequency reserves, and ancillary services to support grid stability.
- Connecting different electricity resources to the grid
- Generating financial returns for investors and stakeholders.
- Securing energy demands.
- Monitoring and controlling voltage and frequency conditions to maintain grid reliability.

2) Demand System

The main task of the demand system is to use electricity, compensate for services delivered, and to transmit data to the system for further analysis. Key functions of the demand system are:

- Utilizing the supplied energy for purposes, such as generating motion or alternative types of energy.

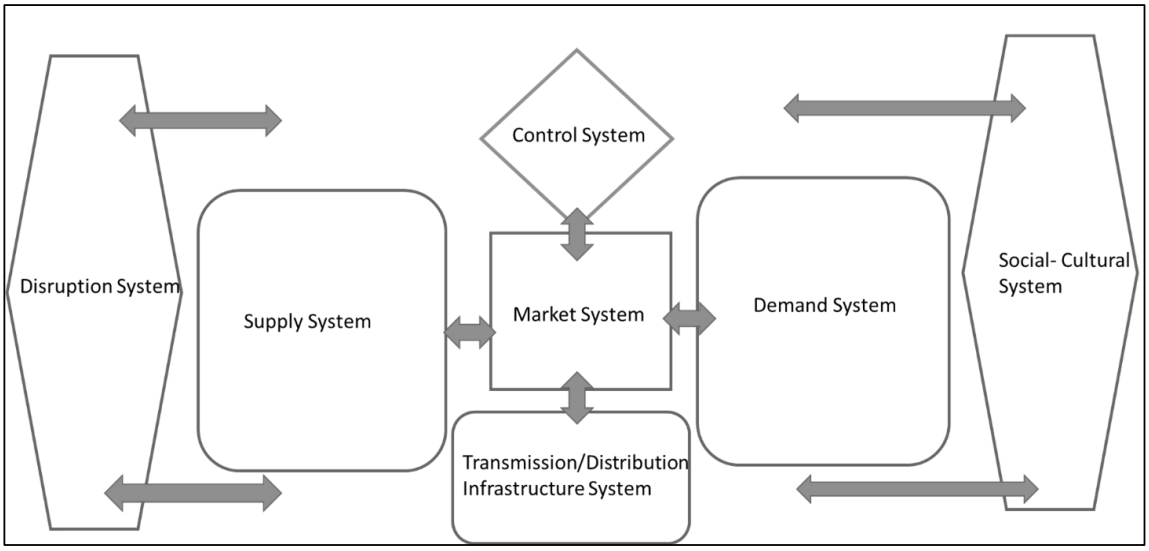


Figure 5. Proposed Social-Cyber-Physical Grid Mode, Version 1.0

- Implementing own monitoring and control.
- Generating value or fulfilling functions for the consumer.
  - Heating
  - Industrial processes
  - Data storage
  - Transportation
- Responding to price signals through demand-response mechanisms.

3) Transmission / Distribution Infrastructure System

The primary objective of the grid system is to facilitate the transportation of electricity and information, while measuring parameters necessary for optimizing grid capacity utilization. Key functions of the transmission/distribution infrastructure system are:

- Transmitting electricity across various points of the grid.
- Facilitating the transmission of data necessary for grid operations.
- Incorporating demand and supply domains, thus forming the operational grid network.
- Performing data measurement tasks to monitor grid performance.
- Implementing control and protection measures to safeguard infrastructure equipment.

4) Market System

The primary objective of a well-functioning market system is to promote a secure supply of energy produced sustainably and at affordable prices. Key functions of the market system are:

- Integration of markets.
- Supporting decarbonization initiatives.
- Continuous intraday trading (market).
- Performing balancing actions (balancing market, end-user market).
- Enabling flexibility through aggregators.
- Collecting data on grid capacity.
- Gathering market data (demand, supply, capacity).
- Providing market data services as needed.
- Maintaining trading platforms for both intraday and day-ahead markets.
- Facilitating price settlements.
- Achieving balance between supply and demand.

5) Control System

The primary function of the control system is to maintain a balance between electricity demand and supply in accordance with market dynamics, ensuring the quality of supply, and communicating signals to the market regarding grid capacity. Key functions of the control system are:

- Maintaining a stable 50 Hz frequency.
- Regulating voltage levels.
- Controlling power generation for stable operation
- Ensuring grid stability and security
- Monitoring key parameters, such as frequency, voltage, power, and overall system stability.
- Responding to disruptions and anomalies.
- Collecting data for investigation and analysis purposes.

6) Disruption System

The main task of the disruption system is to create disturbances that disrupt the smooth functioning of the energy system. In response, the energy system needs to demonstrate resilience to withstand such disruptions, employing strategies like n-1 redundancy, manual operation, island operation, etc. Key functions of the disruption system are:

- Weather events and climate change impacts
- Cyberattacks targeting the system or its components.
- Equipment malfunctioning.
- Social disruptions affecting operations.
- Natural disasters causing system disturbances.
- Political conflicts or wars affecting energy infrastructure.
- Market interruptions affecting energy supply.
- Frequency fluctuations impacting system stability.
- Disrupting the balance between functionality, security, and economic considerations.

7) Social-Cultural System

The main purpose of the social-cultural system is to establish a stable framework for the energy system, integrating

social, economic, and environmental aspects. It recognizes individual's integration into broader social structures shaped by collective beliefs and agreements [15]. This system interacts closely with socio-technical institutions, reflecting the culture of a society [16]. It examines drivers of energy behavior [17] and vulnerabilities, including cyber ones. Key functions of the social-cultural system are:

- Governance, including policy and legal frameworks.
- Influencing security interests and decisions.
- Shaping the business climate and culture.
- Driving economic and financial considerations.
- Influencing energy consumption behaviors.
- Influencing production behaviors, including prosumer activities.
- Providing relevant services.
- Adapting and shaping the global landscape in response to international structures and dynamics.

B. Feedback on the model

As part of REDISET project Work-Package 3 development, the proposed model was presented during two project workshops held in Vaasa, Finland, in June and September 2023. The model generated positive feedback from both industrial and academic experts, although some points were raised. Below are the main concerns and responses to them.

- Issue 1: Control system is positioned solely above the market system.
  Response: In this model, which represents a system-of-systems, each system possesses its own control mechanism. Therefore, in this proposed model, the control system serves as the most centralized control system.
- Issue 2: Arrows only connect certain domains.
  Response: Since every domain is interconnected with other domains, the connections can occur directly or indirectly. The current model shows only direct connections for simplicity, with future iterations emphasizing interconnectedness.
- Issue 3: Arrows from the social-cultural and disruption systems are directed solely towards the control and transmission - distribution infrastructure systems.
  Response: The arrows of the social-cultural and disruption systems are inclusive, indicating their influence extends these systems.

V. CONCLUSIONS AND FURTHER WORK

This paper critically evaluates the most prominent existing power systems in light of the changing landscape, emphasizing the need for developing a model capable of meeting future grid demands. It is clear that existing models lack consideration of the human and social-cultural factors, which are critical for the future grid. Moreover, they also fail to address some of the most recent critical issues, such as security and privacy. Accordingly, the paper presents a model that provides a comprehensive framework for mapping the interdependencies among various infrastructure environments within the Nordic power system. By considering the disruption system, supply system, market system, control system, transmission/distribution infrastructure system, demand system, and social-cultural system, the proposed model enables a holistic understanding of the system-of-systems perspective.

Moving forward, our future research will delve deeper into exploring both intra- and inter-dependencies within and between these infrastructure environments. This analysis will provide valuable insights into the vulnerabilities present in the power system. We will specifically focus on simulating and studying the potential cascading consequences of failures in critical components at both the component and the executive levels. By conducting such analysis, we aim to enhance our understanding of the system's overall resilience. To facilitate further development, we recognize the importance of providing more detailed descriptions and discussions of the individual sub-systems within the power system. This additional level of refinement and development will allow for a more comprehensive exploration of the system's intricacies. The model approach outlined in this paper provides a solid foundation for investigating the dependencies and vulnerabilities within the Nordic power system. Through future research, we aspire to advance our understanding of the system's behavior and contribute to the development of strategies for ensuring its robustness and reliability.

ACKNOWLEDGMENT

The authors would like to acknowledge the following financers: Nordic Energy Research, Business Finland, The Swedish Energy Agency, The Norwegian SmartGrid Centre, Statnett, Svenska Kraftnät, Fingrid. The authors would like to acknowledge the following project participants and technical and scientific reference group: Elevio, Hitachi, Vattenfall, Statkraft, F-secure, Wärtsila, Traficom, ABB and Recorded Future.

REFERENCES

[1] Gopstein, Avi, et al. NIST framework and roadmap for smart grid interoperability standards, release 4.0. Gaithersburg, MD, USA: Department of Commerce. National Institute of Standards and Technology, 2021.

[2] Uslar, Mathias, et al. "Applying the smart grid architecture model for designing and validating system-of-systems in the power and energy domain: A European perspective." Energies 12.2 (2019): 258.

[3] Georgiadou, A., Michalitsi-Psarrou, A., & Askounis, D. (2023). A security awareness and competency evaluation in the energy sector. Computers & Security, 129, 103199.

[4] Krkoleva Mateska A, Krstevski P, Borozan S. (2021) Overview and Improvement of Procedures and Practices of Electricity Transmission System Operators in South East Europe to Mitigate Cybersecurity Threats. Systems. 9(2):39. https://doi.org/10.3390/systems9020039

[5] Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. Computer networks, 169, 107094.

[6] Sun C., Hahn A., Liu, C. (2018) Cyber security of a power grid: State-of-the-art. International Journal of Electrical Power & Energy Systems. Vol. 99. p.45-56, ISSN 0142-0615. https://doi.org/10.1016/j.ijepes.2017.12.020.

[7] Hamel, Candyce, et al. "Defining rapid reviews: a systematic scoping review and thematic analysis of definitions and defining characteristics of rapid reviews." Journal of Clinical Epidemiology 129 (2021): 74-85.

[8] Thoring, Katja, Roland Mueller, and Petra Badke-Schaub. "Workshops as a research method: Guidelines for designing and evaluating artifacts through workshops." (2020).

[9] Hooshyar, Hossein, and Luigi Vanfretti. "A SGAM-based architecture for synchrophasor applications facilitating TSO/DSO interactions." 2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). IEEE, 2017.

[10] Aravinthan, Visvakumar, et al. "Reliability modeling considerations for emerging cyber-physical power systems." 2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS). IEEE, 2018.

[11] Kotut, Lindah, and Luay A. Wahsheh. "Survey of cyber security challenges and solutions in smart grids." 2016 cybersecurity symposium (CYBERSEC). IEEE, 2016.

[12] Jim Finkle, "U.S. firm blames Russian 'Sandworm' hackers for Ukraine outage", Reuters, published January 8, 2016. Retrieved 22 May 2023

[13] N. Kostyuk and Y. M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?", J. Conflict Resolution, 63(2), pp. 317-347, 2019. Available: https://doi.org/10.1177/0022002717737138

[14] Human Rights Watch, "Ukraine: Russian Attacks on Energy Grid Threaten Civilians", published December 6, 2022. Retrieved 22 May 2023.

[15] A. Stirling, "Transforming power: Social science and the politics of energy choices," Energy Research & Social Science, vol. 1, pp. 83-95, 2014.

[16] M. Sarrica, S. Brondi, P. Cottone and B.M. Mazzara, "One, no one, one hundred thousand energy transitions in Europe: The quest for cultural approach," Energy Research & Social Science, vol. 13, pp. 1-14, 2016.

[17] L. Steg, R. Shwom, and T. Dietz, "Engaging People in a Sustainable Energy Transition," IEEE Power & Energy Magazine, vol. 16(1), pp. 20-28, 2018.

Industrial Systems and Industrial Data Privacy – A Comprehensive Review

Bahaa Eltahawy*

Computer Science, School of Technology and Innovations, University of Vaasa
Wolffintie 32, 65200 Vaasa, Finland
bahaa.eltahawy@uwasa.fi

*Corresponding author

Abstract. The rise of industrial systems, driven by recent advances in engineering and data science, has significantly reshaped manufacturing and production. Equipped with modern tools and capabilities, industrial systems can streamline processes, enhance production, analyze complex scenarios, and support decision-making. Central to these systems is industrial data, which provides the insights and means necessary to drive operations and achieve production objectives. Given its critical value, protecting industrial data from potential risks is essential for ensuring consistency, utility, and competitiveness. While various studies focus on security, the literature addressing industrial data privacy remains limited. Acknowledging this gap, this work thoroughly explores these topics. First, industrial systems are examined, highlighting their prevalent types and establishing a foundation for understanding their distinctive features. The study identifies 10 common types of industrial systems and their shared characteristics. It then presents 15 definitions and contexts before proposing an inclusive definition that aligns with modern industrial systems. Next, 34 selected studies on industrial data privacy are reviewed, discussing its significance, current challenges, and potential solutions. The study defines industrial data and identifies eight contexts associated with industrial data privacy, then provides a comprehensive review of each. Finally, it highlights a range of operational and technical solutions for protecting industrial data. Taken together, the findings underscore the pressing need to prioritize industrial data privacy and address it more closely in both research and practice.

Keywords: Industrial Systems, Industrial Data, Privacy, Data Protection, Industrialization, Emerging technologies

1 Introduction

1.1 Overview

In the past two decades, manufacturing and production have undergone a remarkable transformation, driven by the convergence of advanced technologies and shifting demands that have reshaped industries globally [1]. Thanks to rapid technological innovations and the strategic utilization of industrial data, the dynamic interaction between systems, customization, and process optimization have revolutionized the landscape of manufacturing and production. Specifically, advances in engineering, Information Technology (IT), and Operational Technology (OT) have converged to drive a new shift in industrial systems, encompassing comprehensive frameworks, specialized tools, and capabilities designed to meet the challenges of modern manufacturing [2-3]. With the introduction of Industry 4.0 (I4.0) in 2011 and the integration of the Internet of Things (IoT), data analytics, and automation technologies, industrial systems became more interconnected and intelligent [4-5]. This resulted in higher precision, customization, adaptability, speed, and efficiency, as seen in smart factories where manufacturing is fully digitalized and systems continuously collect, process, and share data for real-time monitoring, predictive maintenance, and adaptive manufacturing [3]. The result is a very dynamic and responsive industrial ecosystem capable of meeting complex demands and adapting to abrupt changes while minimizing interruptions, controlling costs, and ensuring product quality.

Industrial data plays a fundamental role in this context, serving as the key enabler for the intelligence in industrial systems [6]. Only through the utilization of industrial data generated by sensors, machinery, interconnected devices, as well as market and supply chain signals and processes, has value been created and manufacturing transformed [7]. Within the I4.0 paradigm, data is no longer merely a byproduct of industrial systems, but is rather a strategic asset [8-9]. It carries real-time metrics, measures, indicators, parameters, and control commands that are analyzed and used to provide operational and production insights [3]. As the role of industrial data has grown in significance, associated risks have also increased, including potential cyberattacks, data breaches, and the exploitation of sensitive information [10-12]. These can lead to several potential consequences, such as operational malfunctions, production disruptions, compromised systems, Intellectual Property (IP) theft, and even impacts on personal data rights [13]. Several trials have been conducted to address these issues, e.g., [14-17], as well as the studies reviewed in Section 4. However, these efforts either addressed industrial data topics separately or focused on aspects and measures of cybersecurity and governance frameworks without giving sufficient attention to the actual value of data and its privacy while being processed and shared. Accordingly, more comprehensive approaches that integrate privacy practices into industrial data are needed, as protecting and maintaining the integrity of industrial data is essential for ensuring consistency, utility, and competitiveness.

1.2 Research Questions, Research Approach, Contributions, and Limitations

Motivated by the importance of industrial data and the growing concern over its privacy, this study investigates the existing literature to answer the central research question: *"What is the current status of industrial data privacy?"* The question is further refined using the Mutually Exclusive and Collectively Exhaustive (MECE) framework [18] into the following three sub-questions: 1) *"What are industrial systems?"* 2) *"What is industrial data?"* and 3) *"What challenges and solutions exist regarding industrial data privacy?"*

To answer these questions, the study employs a mixed-method research design, combining a narrative review to examine industrial systems with systematic review to investigate the topic of privacy within the context of industrial systems, then performs a synthesis to integrate the findings, identify patterns across the literature, and propose a structured understanding of industrial data privacy.

The main contributions of this study are threefold: 1) Proposing a definition of industrial systems that aligns with their current capabilities, features, and characteristics; 2) Offering one of the few dedicated endeavors to comprehensively cover the topic of industrial data privacy from all relevant perspectives in the existing literature; and 3) Providing eight themes related to industrial data privacy along with a set of recommended solutions.

Finally, this study is based on desk research, thus only reviewing available literature without producing any primary data or solutions of its own.

1.3 Research Organization

The remainder of this work is structured as follows: Section 2 defines industrial systems, outlines their common types and characteristics, and reviews industrial data attributes and classifications. Section 3 describes the literature review methodology used to address industrial data privacy. Section 4 presents a comprehensive review of the literature on industrial data privacy, highlighting identified risks and solutions. Section 5 synthesizes and discusses the findings. Finally, Section 6 concludes the work and offers directions for future research.

2 Background – Industrial Systems and Industrial Data

This sections provides a narrative review to establish the foundational understanding needed for examining industrial data privacy [19-20]. It introduces key concepts and common definitions related to industrial systems, outlines their types and characteristics, and defines industrial data within these systems. Together, these elements set the stage for the exploration of industrial data privacy issues in the following sections.

2.1 Industrial Systems – Definitions

First, finding a unanimous and precise definition of the term "industrial systems" was challenging, primarily due to the term's broad applicability and contextual nature across various sectors. In Table 1, the most common definitions of the term "industrial systems" identified in the literature are highlighted along with their contextual backgrounds.

Table 1. Industrial systems definitions and their contexts

Contexts	Definition
Manufacturing; Services; Value-creation	"An industrial system includes the context, resources, activities, processes, actors, and interdependencies that support the creation and delivery of products and services. A clearer understanding of industrial systems – a holistic view – can identify those 'levers' which are available to generate and, crucially, capture value" [21]
Energy; Operations	An "industrial system means the whole or any part of an electric system primarily intended to serve one or more industrial operations of which the system forms a part" [22]
Internet of Things; Networks; Machinery	"The industrial systems of the future are complex systems composed of vast numbers of devices interacting with each other and with enterprise systems." [23]
Management	"An industrial system is a collection of interrelated elements brought together to achieve a specific objective of meeting product or service goals" [24]
Data mining; Manufacturing	"The industrial system is a typical real-time control and real-time information processing system" [25]
Industry 4.0	"An industrial system is an ensemble of parts connected in a networked fashion, which show a peculiar behavior that is not observable when the parts are considered separately" [26]
Business	"The modern industrial system is a concatenation of processes which has much of the character of a single, comprehensive, balanced mechanical process" [27]
Environment management	"An industrial system is an ecological system" [28]
Industrial symbiosis	"The regional industrial system (RIS)" is "a more or less stable collection of firms located in proximity to one another, where firms in principle can develop social and material/energy connections as a result of that proximity" [29]
Marketing; Production	"The industrial system is a network of firms engaged in the production, distribution and use of goods and services through which lasting business relationships are established, developed and maintained" [30]
Behavioral	"The industrial system … is a very complex multi-loop and

management; Accounting	interconnected system … Decisions are made at multiple points throughout the system. Each resulting action generates information that can be used at several but not all decision points. This structure of cascaded and interconnected information-feedback loops, when taken together, describes the industrial system." [31]
Informatics; Data	"A large-scale industrial system is a networked information system, where the raw data sampled at the lowest device level flows up to upper-layers. Various data acquisition and processing tasks are carried out at different layers for different purposes." [32]
Private data; Internet of Things; Blockchain	"An industrial system is a loosely distributed organization" [33]
Simulation; Modeling	"Eco-industrial system is a typical complex adaptive system that generates intricate patterns with given constraints … An eco-industrial system always tries to find an optimal process to obtain maximized flux under given constraints." [34]
Manufacturing; Business	"An industrial system is a highly complex system … It consists of many interacting and interconnected autonomous entities that are continuously adapting, while new entities are added and old entities are removed. As a result of this complexity, it is difficult – if not impossible – to predict the development of the industrial system." [35]

As seen in Table 1, the term "industrial systems" varies significantly depending on the sectors considered and their specific characteristics. Additionally, common themes can be identified across the given definitions, including complexity, adaptability, purpose, information-driven operations, networked and interlinked architecture, as well as an ecological perspective.

2.2 Industrial Systems – Types and Characteristics

Second, industrial systems are not limited to a single form or structure; rather, they come in various types and sizes depending on the sector in which they are deployed and the purpose they are intended to fulfill, as highlighted in the definition proposed earlier. Below is a list of the most common industrial systems identified while conducting this research. It is worth noting that this list is not exhaustive, as industrial systems continuously evolve and extend beyond it.

1. **Industrial control systems** (ICS) are integrated infrastructures to control industrial systems distributed over large geographical areas and locations. These include networks, sensor devices, and controllers to automate and operate industrial tasks and processes effectively. ICS are either Supervisory Control and

Data Acquisition (SCADA), Distributed Control Systems (DCS), or hybrid systems that combine the best features of both systems [36].

a. **Supervisory control and data acquisition (SCADA)** refers to the centralized systems that control production infrastructures. SCADA is frequently used interchangeably with process control and ICS; however, the distinction may lie in the observation that SCADA systems are considered to support the coordination of infrastructures rather than controlling the discrete elements of these infrastructures. ICS encompasses both coordination and control functions.
b. **Distributed control systems (DCS)** refer to systems in which the controller elements are distributed rather than centralized – as in SCADA – with each component and discrete subsystem managed by one or more controllers.
c. **Programmable Logic Controller (PLC)** is the control component of the ICS that provides process management. PLC provides supervisory, remote access, and control to devices such as actuators and sensors [37].
d. **Human Machine Interface (HMI)** provides a graphical user interface (GUI) application that facilitates the interaction between hardware, control system, and operators [37].
e. **Safety Instrumented Systems (SIS)** are hardened ICS elements designed for high reliability and safety in the event of system failure. SIS includes functional elements that contribute to operational safety and risk management, often sharing technical architectures and features with more general-purpose ICS [36].

2. **Industrial Automation and Robotics** is the control of machinery and processes used in various industries by autonomous systems through technologies like robotics and computer networks [3, 38].
   a. **Machine Vision (MV)** refers to the technology and methodologies used for imaging-based autonomous inspection and analysis in various applications. MV is used for material inspection, object recognition, pattern recognition, electronic component analysis, signature recognition, optical character recognition, and money recognition [39].
   b. **Additive Manufacturing (AM)**, a subset of Adaptive Manufacturing, is the process of joining materials to create parts from 3D model data, usually built in layers [40].
3. **Industrial communication networks** are the infrastructure that connects bottom field devices, such as sensors and actuators, with control devices like PLC, DCS, and SCADA to achieve industrial automation control, system interconnection and interoperability. These networks include fieldbus, Industrial Ethernet, industrial wireless networks, and other heterogenous networks [41].
   a. **Industrial Edge Computing (IEC)** is a system of micro data centers located at the edge of the network, close to or within factory premises. In edge computing, computing tasks are executed near the end users or devices in terms of geographical and network proximity. This enables levels of latency and throughput that are unattainable with cloud computing [42].
4. **Industrial analytics (Industry 4.0 analytics**, or **Industrial Intelligence**) is an interdisciplinary field that bridges data science and industrial engineering, and it lies at the core of Industry 4.0 and the Industrial Internet of Things (IIoT).

Industrial analytics aims at exploiting the business value of data by developing data-driven products, services, and processes [43].

a. **Artificial Intelligence (AI)** is "the science and the engineering of making intelligent software systems and machines" [44]. It is the "simulation system of collecting knowledge and information and processing intelligence … and disseminating it to the eligible in the form of actionable intelligence" [45].

5. **Industrial Internet of Things (IIoT)** is "the extension and use of the Internet of Things (IoT) in industrial sectors and applications. A powerful emphasis on big data, machine-to-machine communication, and machine learning, the IIoT enables industries and enterprises to have better efficiency and credibility in their operations" [46]. IIoT "is built for bigger 'things' than smartphones and wireless devices. It aims at connecting industrial assets, like engines, power grids and sensor to cloud over a network" [47].
6. **Cyber-Physical Systems (CPS)** are the integration of computing and physical processes. CPS are primarily characterized by the flow of information involving multiple heterogeneous physical systems [48].
7. **Manufacturing execution systems (MES)** are IT tools commonly deployed in organizations involved in traditional manufacturing. An MES enables information exchange between the organizational level, commonly supported by an Enterprise Resource Planning (ERP), and the control systems for the shop-floor, usually consisting of several, different, highly customized software applications [49].
8. **Energy Management Systems (EMS)** are complex hardware and software systems that assist in monitoring and controlling power systems to minimize operating expenses, ensure a continuous power supply, and maintain an adequate operating margin to accommodate potential power outages. EMSs also perform essential functions such as data collection and maintenance for customer billing [50].
9. **Quality Management Systems (QMS)** are management systems comprising interconnected and interacting processes that work together to control and achieve an organization's quality objectives [51-52].
10. **Industrial Cybersecurity** is "a set of practices, processes and technologies designed to manage cyber risks arising from the operation, processing, storage and transmission of information used in industrial organizations and infrastructures, using a people, process and technology perspective" [53]. Industrial Cybersecurity is a "dedicated portfolio of technologies and services designed to protect operational technology layers and elements of industrial enterprises – including SCADA servers, HMIs, engineering workstations, PLCs, network connections and even engineers – without impacting on operational continuity and consistency of industrial processes" [54].

As seen from the given examples, industrial systems share key characteristics and features that strongly distinguish them from consumer and commercial systems. Below is a brief list of the identified characteristics:

1. Integrated infrastructure and connectivity: as of being composed of multiple interconnected physical components and software applications that work together within processes to achieve specific objectives.
2. Complexity: as of being interconnected with multiple components that have a wide range of functionalities and intricate processes.
3. Automation: as of utilizing software tools, programmable logic, and similar technologies and methods to efficiently and accurately execute tasks and streamline operations while adapting to changing conditions.
4. Distributed control and coordination: as of being distributed across large areas yet still functioning as a unified system.
5. Data-driven: as of being equipped with sensors and data acquisition systems to optimize processes and enhance decision-making
6. Advanced technologies and specialized networks: as of utilizing cutting-edge technologies with enhanced capabilities, throughput, and latency to enable efficient and reliable operations.
7. Focus on efficiency, reliability, and scalability: as of emphasizing the achievement of higher efficiency and reliability levels while enhancing seamless integration and robust scalability to ensure longevity and meet future demands.
8. Risk management and resilience: as of being designed to withstand unexpected events and disruptions, mitigate risks, and ensure continuous operations.

By integrating the key characteristics and features identified above with the definitions and themes identified from Table 1, a ***comprehensive*** definition of *"modern"* industrial systems is suggested as follows:

Industrial systems are sophisticated, interconnected networks of components, subsystems, and processes that utilize information, control systems, automation, and adaptive mechanisms to achieve specific objectives related to the production and delivery of goods and services, while emphasizing efficiency, reliability, scalability, and resilience through data-driven approaches.

2.3 Industrial Data

Finally, "w*hat is industrial data?"* is a fundamental question of this research, as the answer is essential for understanding the nature of industrial data and how to preserve its privacy. Fortunately, Xu *et al.* [55] have clearly addressed this issue, providing a comprehensive classification of industrial data and its sources, as shown in Table 2.

Table 2. Industrial data classifications and their sources (Adopted from Xu *et al.* [55])

Data field	Classification	Sources
R&D	R&D design and Development data	Computer-Aided Design (CAD); Simulation and analysis Computer-Aided Engineering (CAE); Industrial software development system; Industrial system testing tools; etc.
Production	Control information;	MES; PLC; SCADA; DCS; QMS; Working

	Industrial control; Process parameters; and System log	condition database; etc.
Operation and maintenance	Logistics and After-sales maintenance data	EMS; Product logistics system; Product after-sales status tracking system; After-sales service management system; etc.
Management	System equipment asset information; Customer and product information; Product supply chain data, Business statistics, and Safety Systems	Product Lifecycle Management (PLM); Supply Chain Management (SCM); QMS; Enterprise Resource Planning (ERP); Customer Relationship Management (CRM); Warehouse Management System (WMS); SIS; etc.
External	Data shared with other subjects	Access to supply chain and collaborative R&D; etc.
Platform Operation	Data collection; Customer application data; Knowledge base repository; Analysis data; Configuration data; Application data; Technical and management data	Production data; Monitoring data; Sensors; Customer platform-independent data; Knowledge base and cloud data; Reports, results and data analysis techniques; Configurations, user accounts, application services, and equipment; Industrial applications; Source codes, tools, test cases; etc.
Enterprise management	Customer and solution data; Business cooperation; Personnel; and Financial data	Customer information; Behavior characteristics; Usage records; Customer service and maintenance records; Customization and deliverables; Agreements; Contracts; Employee information; Assets; Audit information; Financial statements; etc.

Having defined industrial systems and industrial data, we proceed to addressing the issue of industrial data privacy in the following sections.

3 Methodology

In this work, we followed the systematic literature review practices of Okoli and Schabram [56] along with the recommendations of Rowe [57] and Schryen [58] to identify and synthesize literature on industrial data privacy. First, three databases were considered: Google Scholar for its broad coverage, followed by Scopus and IEEEXplore for their specialized, focused content. The search strings used are: “Industrial data privacy”, “Privacy of industrial data”, and “Privacy of the industrial data”. Second, due to the limited number of results – less than 50 – all results were considered, regardless of the publication year. Table 3 shows search strings and their corresponding results.

Table 3. Search strings and the corresponding results.

#	Search String	Database	Returned Results and description
1	Industrial data privacy	Google Scholar	**22 – inclusive**
		Scopus	3 – duplicated in Google Scholar
		IEEEXplore	3 – duplicated in Google Scholar
2	Privacy of industrial data	Google Scholar	**20 – inclusive**
		Scopus	2 – duplicated in Google Scholar
		IEEEXplore	2 – duplicated in Google Scholar
2	Privacy of the industrial data	Google Scholar	**7**
		Scopus	0
		IEEEXplore	0

Finally, after removing duplicates, assessing quality and relevance, and considering peer-reviewed scientific content from conferences or journals (with three articles exempted from the peer-reviewed criterion due to their relevance) exclusively in English while excluding others from the scanning phase, 34 articles were considered for the final review stage. Figure 1 illustrates the adopted methodology.

Fig. 1. The adopted research methodology

4 Industrial Data Privacy – A Literature Review

4.1 Preliminary Insights

4.1.1 Timeline

Figure 2 shows the frequency of reviewed literature covering the topic of industrial data privacy. As shown in the figure, no explicit research addressing this topic with the given search strings was found before 2017. However, since 2017, the topic has received increased attention, reflecting a growing awareness of its potential and significance. This can be explained in light of the increasing capabilities of industrial systems, their potential impacts, increased security and privacy concerns, and the growing recognition of the importance of industrial data.

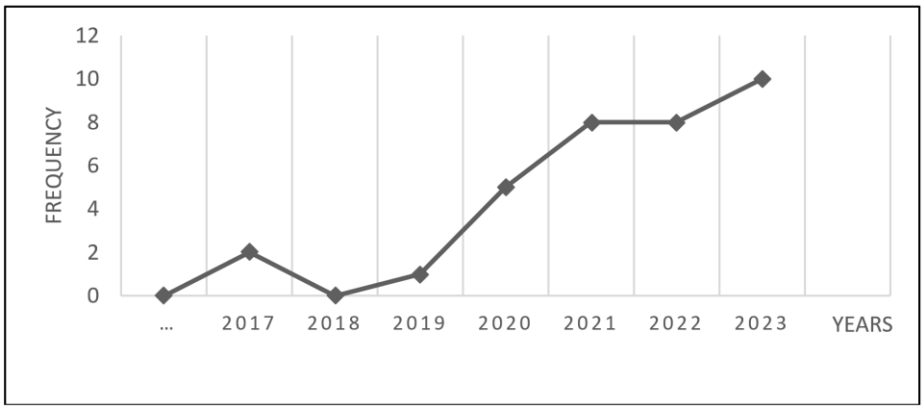


Fig. 2. Frequency of research covering the topic of industrial data privacy

4.1.2 Keywords

Figure 3 shows the frequency of keywords extracted from the reviewed literature. This serves as a preliminary tool to provide insight into the covered topics and their relevance. It is worth mentioning that the column Security Techniques differs from the more general column Security, as it includes keywords related to techniques, such as encryption, decryption, authentication, confidentiality, key generation, etc.

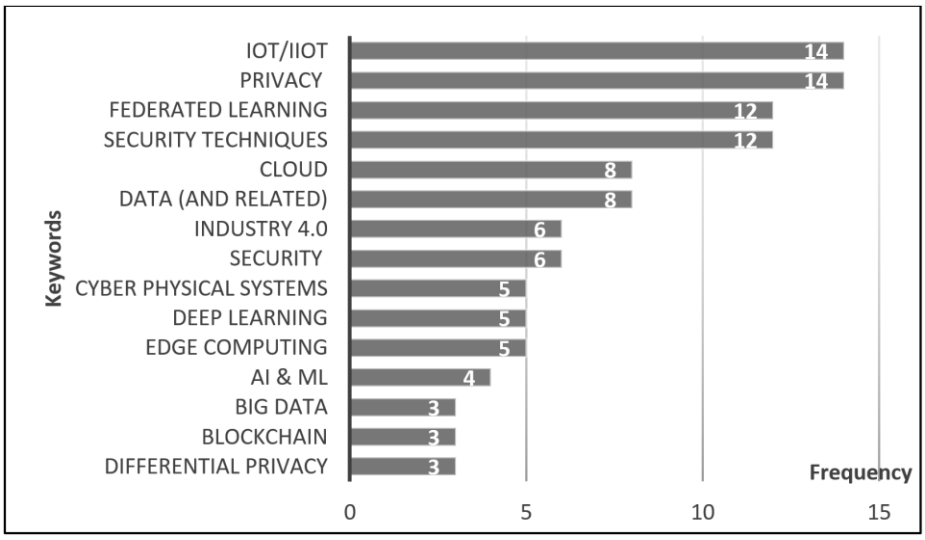


Fig. 3. Frequency of keywords extracted

4.1.3 Topics

Before proceeding with the literature survey and synthesis, the reviewed studies were categorized into relevant topics as shown in Table 4. In Table 5, the reviewed studies are mapped to the defined categories.

Table 4. Reviewed studies' categories and topics

Category	Topics
C1: Privacy	Data privacy, differential privacy, identity privacy, location privacy, IoT data privacy, privacy metrics, private federated learning, Multimedia security and privacy, cloud privacy, and forward privacy.
C2: Security	Data aggregation, rule engine, certificateless encryption, searchable encryption, authentication, multifactor authentication, data security, secure transmission, encryption, access control, confidentiality, integrity, decryption, and blockchain.
C3: Industry 4.0 and Cyber physical systems	Cyber Physical Systems, Industrial Cyber Physical Systems, Industry 4.0, and autonomous systems.
C4: Cloud computing	Cloud, edge, and fog computing.
C5: Internet of Things	Internet of Things, Industrial Internet of Things, and distributed Internet of Things.
C6: Data analysis cluster	Data analysis, data analytics, data mining, big data, diagnosis, monitoring, simulation, alarm systems, intrusion detection, anomaly detection, unsupervised clustering, scenarios, and

	Product Lifecycle Management (PLM).
C7: AI Cluster	Artificial Intelligence, machine learning, dictionary learning, deep learning, deep models, and reinforcement learning.
C8: Federated learning	Federated learning, data federation, transfer learning, federated dictionary learning, federated deep learning, and contrastive learning.

Table 5. Mapping the reviewed studies to the defined categories in Table 4

Studies (in order of review)	C1	C2	C3	C4	C5	C6	C7	C8
S1: [59]	✓						✓	
S2: [60]	✓			✓				✓
S3: [61]	✓			✓	✓			
S4: [62]	✓	✓			✓		✓	
S5: [63]	✓			✓	✓		✓	
S6: [64]	✓					✓	✓	✓
S7: [65]						✓	✓	✓
S8: [66]					✓			✓
S9: [67]			✓			✓		
S10: [68]	✓					✓		
S11: [69]						✓		
S12: [70]		✓						
S13: [71]			✓	✓		✓	✓	
S14: [55]	✓				✓			✓
S15: [72]	✓	✓			✓			✓
S16: [73]			✓	✓	✓			
S17: [74]			✓			✓		✓
S18: [75]		✓				✓		
S19: [76]		✓			✓			
S20: [77]		✓	✓		✓		✓	✓
S21: [78]		✓			✓			
S22: [79]						✓		✓
S23: [80]					✓		✓	✓
S24: [81]		✓		✓	✓			
S25: [82]							✓	✓
S26: [83]			✓			✓		
S27: [84]	✓	✓		✓				
S28: [85]		✓		✓			✓	

S29: [86]			✓					
S30: [87]	✓	✓		✓	✓			
S31: [88]	✓		✓				✓	✓
S32: [89]	✓	✓		✓	✓		✓	
S33: [90]		✓		✓				
S34: [91]			✓			✓	✓	

4.2 Literature Survey

4.2.1 Privacy

Data privacy is a growing concern for the industry. For instance, Faujdar and Kaur [63] highlight the threats to data privacy from both technological and management perspectives. Jiang *et al.* [62] discuss the risks of industrial data being used in warehouses and automation, including the potential for leakage during transmission through, e.g., Wi-Fi or other wireless media. Li *et al.* [64] emphasize the issue of commercial collaborations due to the risks of exposing users' private data, and that faulty data might still include sensitive records. Tajanpure and Muddana [68] emphasize the risks of unrestricted access to individuals' information records, while Xu *et al.* [55] discuss the potential of losing competitive advantages due to the use of users' data for optimization and training algorithms. Li *et al.* [88] examine the latter issue closely, as privacy regulations restrict the exchange of industrial data between entities, which itself results in issues related to less optimization and efficiency. Yang *et al.* [72] extend the discussion to include multimedia data privacy risks, since multimedia data is of high criticality to privacy and is used in deployments, such as in IoT. Additionally, they raise concerns about the level of privacy, feasibility, heterogeneity of systems, computational overhead, transparency, and governance. Finally, Ahmadi and Salehfar [84], Venkatesan *et al.* [87], and Li *et al.* [89] discuss the potential of cloud services that access sensitive personal and industrial data, e.g., personal, smart-home, energy, etc.

Solutions related to data privacy have been closely examined and given special consideration due to their impacts. For instance, Wu *et al.* [59] and Xu *et al.* [55] point out that differential privacy techniques – though still in their early stages – can provide better privacy protection than current solutions that rely mostly on encryption. This is because differential privacy is computationally efficient and depends on adding noise into datasets according to a predefined privacy budget. This technique is also suggested by Jiang *et al.* [60], Tajanpure and Muddana [68], Jiang *et al.* [62], and Yang *et al.* [72]. In [59], a Software-Defined Network (SDN) algorithm based on centralized differential privacy with a trusted third party is proposed and proven to provide strong industrial data privacy protection and high availability. Jiang *et al.* [60] emphasize attack types and how they change the requirements for industrial data, and propose the use of a hybrid differential privacy combined with adaptive gradient compression of data. Tajanpure and Muddana [68] suggest the use of differential privacy techniques with a convolution-based privacy-preserving algorithm that transforms data into lower dimensions, and thus preserves its privacy. Xu *et al.*

[55] highlight the importance of balancing protection and accuracy by controlling the privacy budget and propose the use of a privacy-preserviNg InCEntive (NICE) mechanism based on differential privacy. Similarly, Venkatesan *et al.* [87] raise concerns about increased computational complexity, costs, performance issues, recommending the use of forward privacy property due to its efficiency and cost-effectiveness.

On the other hand, Jiang *et al.* [62] state that industrial data differs from social data in aspects such as volume and required computational power, which could hinder the application of differential privacy techniques. They further highlight that network security, data value, and interconnection protocols are the main considerations for maintaining industrial data privacy. Sadique *et al.* [61] observe that no existing study has identified all the points where end-user and industrial data privacy risks exist. Then, they propose a privacy enhancing framework focusing on security, communication, and gateway security; a layered approach; role-based authentication and access rules; restricted data sharing; intelligent privacy enhancing services; raising awareness; and law enforcement. Faujdar and Kaur [63] propose a similar framework, and like Li *et al.* [64], suggest using decentralized identifiers to enhance privacy. Ahmadi and Salehfar [84] make similar suggestions, emphasizing encryption, anonymization, and the lifecycle of privacy-preserving systems, i.e., design, verification, implementation, and deployment.

4.2.2 Security

Security is a fundamental requirement for protecting data and maintaining industrial data privacy, which is why security and privacy are often discussed together. For instance, Paul and Roslin [70] discuss Wireless Sensor Networks (WSNs) and methods for protecting the security and privacy of aggregated data. Yang *et al.* [72] focus on IoT and the security and privacy of multimedia data. Shi *et al.* [75] look at industrial data flow scenarios, examining how rule engines and access control mechanisms can be used to improve security and privacy. Zhang *et al.* [76] and Venkatesan *et al.* [87] investigate searchable encryption techniques, targeting the security and privacy of stored data. Li *et al.* [89] similarly investigate homomorphic encryption, highlighting IIoT demands and focusing on improving the security and privacy of stored data. Das *et al.* [78] look at multifactor authentication and assess the security and privacy of shared data transmitted over open channels. Finally, Cao *et al.* [81] overview edge computing and examine security and privacy challenges and associated risks.

As noticed, the reviewed studies highlighted various security measures, e.g., confidentiality, integrity, availability, utility, authentication, non-repudiation, and access control, which when effectively implemented help protect data privacy. Moreover, some studies [76, 78, 87] referred to privacy as a key security measure, sometimes using the terms of privacy and confidentiality interchangeably. For example, Paul and Roslin [70] discuss a homomorphic encoding method that enables the aggregation of encoded data, thus reducing the communication cost and guaranteeing accuracy, integrity, and authentication. Additionally, they explore

certificateless signcryption for lightweight devices and RSA encryption to secure the order information of multifaceted data, thus enhancing the privacy of aggregated data. Yang *et al.* [72] identify cryptography, data hiding, chaos-based, and clustering-based schemes among the means employed to protect security and privacy. They also advise against the use of encryption techniques such as RSA, DES, and AES with multimedia data. Besides encryption, Shi *et al.* [75] emphasize access control, identity verification, authentication, authorization, and intrusion detection for establishing a control mechanism to limit data access and identify anonymization as a key method to protect sensitive data. Zhang *et al.* [76] stress the role of encryption in protecting industrial data privacy, proposing a Verifiable Certificateless Public Key Searchable Encryption (VCLPKSE) scheme capable of resisting two types of adversaries related to forging and replacing master encryption keys while authenticating the data owner's identity. Das *et al.* [78] emphasize lightweight security schemes to authenticate communicating devices, suggesting a multi-factor authentication scheme with low computation and communication costs, utilizing smart cards, passwords, Physical Unclonable Function (PUF), and fuzzy extractor. Cao *et al.* [81] consider searchable encryption and discuss an attribute-based authentication and authorization framework that uses attributes and distributed certificates to replace traditional P2P networks' public key certificates and access control authentication mechanisms to protect privacy. Furthermore, the study explores technologies for unified, cross-domain, and handover authentication, explicitly stating that access control is the key technology for ensuring system security and protecting user privacy. Ahmadi and Salehfar [84], among others, highlight cryptography, anonymization, and authentication. Venkatesan *et al.* [87] present a Lightweight Searchable Encryption and Delegation (LSED) Scheme for secure data storage and retrieval. Li *et al.* [89] propose a Robust Cramer Shoup Delay Optimized Fully Homomorphic (RCS-DOFH) encryption technique, surpassing conventional encryption methods and ensuring secure data transmission. Lastly, blockchain technology has emerged as an innovative and modern technique for securing data and protecting privacy [62, 72, 77, 85, 90], with its ability to overcome the tradeoff between productivity and privacy, thus can be used for storing information, establishing trust, and protecting transactions.

Finally, concerning risks, Paul and Roslin [70] mention that the two main security challenges are confidentiality and integrity, while Zhang *et al.* [76] stress these factors industrial data is handled externally. Yang *et al.* [72] emphasize the importance of determining the level of security and privacy and their associated computational overhead costs. In [75], stability, scalability, and real-time performance are among the issues highlighted. Cao *et al.* [81] emphasize that the need for lightweight data encryption, sharing mechanisms, and multi-source heterogeneous data propagation control is among the challenges facing security and privacy. The issue of lightweight encryption is also emphasized by Ahmadi and Salehfar [84]. Yang *et al.* [85] overview efficiency issues related to security. Lastly, Sharma *et al.* [90] highlight blockchain limitations, including insufficient computation resources and data breach risks, which may lead to information misuse and privacy threats.

4.2.3 Industry 4.0 and Cyber-Physical Systems

Industry 4.0 (I4.0) and the emergence of Cyber-Physical Systems (CPS) play a critical role in transforming the industrial landscape and changing the perception of industrial data. For instance, Hinojosa-Palafox *et al.* [67] highlight a previous architecture that collects and integrates industrial data and Manufacturing Information Systems (MIS). They then propose an analytics architecture for Industrial CPS (ICPS) and discuss industrial process challenges. O'Donovan *et al.* [71] compare I4.0 computing models and mention that ICPS are the primary enabler for I4.0, combining legacy industrial and control engineering with emerging technology paradigms. Similarly, Pivoto *et al.* [73] survey the architecture of CPS for IoT applications in I4.0, emphasizing their characteristics, objectives, advantages, and contributions to I4.0. Zainudin *et al.* [74] studies a federated learning Intrusion Detection (ID) and classification framework for SDN, highlighting the critical role of ICPS in storing actual network information, including personal data of manufacturing firms. Abdel-Basset *et al.* [77] address the same topic, discussing the convergence of I4.0 with other technologies, ICPS, and the tradeoff between accuracy and privacy, and propose a federated learning threat hunting model suitable for ICPS owners due to its efficiency, awareness of heterogeneity, and privacy-preserving characteristics. Bokrantz *et al.* [83] cover I4.0 from the angle of maintenance in digitalized manufacturing and highlight resistance to changing traditional systems, along with challenges of security, privacy, liability, and data ownership. Kumar *et al.* [86] highlight the barriers in endorsing I4.0, which affect mitigation strategies, and emphasize the sensitivity of industrial data privacy concerning confidential organizational details. They also emphasize the I4.0 resistance issue and discuss data management, training, skills, and legal policies. Lastly, Milicic *et al.* [91] address autonomous systems and Product Lifecyle Management (PLM) and present an ontology for protecting privacy of data.

Concerning industrial data privacy, several topics have been discussed in the literature. Hinojosa-Palafox *et al.* [67] highlight ICPS analytics privacy issue, concerns related to handling sensitive data without taking appropriate measures, and the potential for external servers to access confidential information. O'Donovan *et al.* [71] stress that I4.0 can ensure appropriate levels of industrial data privacy through strict governance and firewall policies on automation and control networks. Yet, the real-time nature of industrial data and the need to sometimes send it outside the premises still pose a significant challenge. Pivoto *et al.* [73] highlight the increased number of processing devices and systems, which can potentially pose privacy threats. They also emphasize the challenge of protecting user and industrial data privacy and examine the privacy of CPS. Zainudin *et al.* [74] focus on the issue of sharing original data and the use of public networks. Abdel-Basset *et al.* [77] concern the transmission of large volumes of data and associated privacy threats, emphasizing the criticality of maintaining industrial data privacy. In [83], the dilemma of sharing data throughout supply chain for collaboration and related privacy concerns are highlighted. Kumar *et al.* [86] discuss the importance of I4.0 data privacy and raise concerns that strict privacy could undermine the openness of various integrated digital infrastructures. They also mention that data privacy and theft issues are among the

cyberattacks that could disrupt vital infrastructures, emphasizing that legal regulations and technical measures, such as hardware encryption and secure transit data networks, are essential. Lastly, Li *et al.* [88] discuss the use of data aggregation to address industrial data security and privacy concerns.

Other concerns and challenges related to industrial data in I4.0 and CPS have also been identified. For instance, Hinojosa-Palafox *et al.* [67] highlight the criticality of real-time industrial data processing. O'Donovan *et al.* [71] emphasize performance, reliability, interoperability, and resilience. Bokrantz *et al.* [83] address the lack of understanding regarding specific issues faced by maintenance organizations and emphasize the need for developing long-term strategy scenarios for realizing digitalized manufacturing. Additionally, they discuss socio-ethical aspects such as competence, training, education, and knowledge sharing. Kumar *et al.* [86] highlight challenges facing the manufacturing industry, including high investments, unclear benefits, a lack of skilled workforce, resistance to change, inadequate infrastructure, data management, and legal policy constraints. Li *et al.* [88] further emphasize the challenges of fault prediction and decision-making. Lastly, Milicic *et al.* [91] point out that a fully automated system does not yet exist.

4.2.4 Cloud Computing

Cloud computing plays a major role in the realization and advancement of I4.0. As highlighted in the categorization section, cloud computing is a broad term encompassing three models, i.e., cloud, fog, and edge, which operate hierarchically [71, 81]. These models are used to deliver on-demand resources, such as computing power, storage, and service access to end users within various contexts, criteria, and limitations. That being said, cloud computing – characterized by its processing power – operates within the core and data centers. Fog computing is for data processing, management, and transmission, while edge computing with its low latency, high performance, and consistency focuses on distribution and executing tasks closer to end users.

Due to its significance for the modern industry, the literature has paid considerable attention to cloud computing and associated privacy issues. For instance, Jiang *et al.* [60] emphasize the need for industrial data privacy and raise concerns about emerging attack types and the requirements these impose on industrial edge computing to address the risks of industrial data leakage. Sadique *et al.* [61] and Faujdar and Kaur [63] overview IoT privacy risks, focusing on cloud devices and edge computing. O'Donovan *et al.* [71] compare fog and cloud computing cyber-physical interfaces in terms of latency and reliability, highlighting the privacy challenges associated with controlling data transmitted outside the network boundaries. They also mention that fog computing can help mitigate this issue. Pivoto *et al.* [73] focus more on CPS and industrial systems, highlighting the need to implement cloud computing broadly while addressing I4.0 requirements and the privacy challenges associated with large data flows. Cao *et al.* [81] overview edge computing comprehensively, stating that traditional cloud computing is no longer sufficient to meet current needs. They suggest that edge computing can address these limitations by processing data locally,

thereby mitigating security and privacy issues related to data leakage, data loss, and cyberattacks. Furthermore, they outline a list of security and privacy challenges facing edge computing, highlighting data outsourcing and trust issues, the need for lightweight data encryption and data-sharing control schemes, and the importance of combining traditional privacy protection methods with edge processing. Ahmadi and Salehfar [84] discuss the topic of privacy-preserving cloud computing along with its associated ecosystem (anonymization, authentication, access control, cryptography, and watermarking) and lifecycle (design, verification, implementation, and deployment). They emphasize the importance of privacy for cloud computing for ensuring the integrity, accuracy, and accessibility of the stored data. Furthermore, they identify privacy as the most critical security aspect of cloud computing and list the types of industrial data stored in the cloud. Yang *et al.* [85], while discussing edge computing and blockchain, highlight concerns about industrial enterprises uploading their production and related data to the cloud. Venkatesan *et al.* [87] focus on cloud privacy issues resulting from IIoT systems and along with Li *et al.* [89] emphasize the potential of untrusted cloud services and the need for additional data collection measures when data is outsourced. Finally, Sharma *et al.* [90] highlight privacy conflicts, efficiency, and computation complexities associated with cloud computing. They explicitly state that no single cloud solution can provide optimum privacy, therefore several solutions should be considered simultaneously.

On the other hand, many solutions have been proposed to address cloud privacy issues. For instance, Jiang *et al.* [60] propose a data privacy scheme for industrial edge computing utilizing federated learning, combining different privacy models along with differential privacy. Sadique *et al.* [61] propose a data privacy framework and advocate for cloud layer data privacy enforcement, cloud-limited data sharing, and the implementation of edge intelligence to enhance data privacy. Faujdar and Kaur [63] add enforcement of rules, policies, and laws as well as user awareness and legal education to the equation. Cao *et al.* [81] suggest that processing data nearby in edge computing provides better privacy protection, and that computing offloading, mobility management, traffic offloading, and network control technologies can help with edge privacy. Moreover, they along with Venkatesan *et al.* [87] emphasize the importance of searchable encryption as one of the key solutions for protecting privacy and data stored in the cloud without suffering from computational complexity and increased costs. Ahmadi and Salehfar [84] highlight the need for categorizing data according to sensitivity, thus preserving it while reducing costs. They also emphasize the need for integrity-by-design data sharing systems, lightweight layered privacy architecture, and data auditing. Then along with Li *et al.* [89], they mention the solution of encrypting data before uploading it to the cloud and performing operations on encrypted data rather than raw data. Yang *et al.* [85] suggest edge computing to improve the efficiency of parallel model training, thus ensuring the privacy of industrial data. Lastly, Sharma *et al.* [90] present a cloud-assisted, secured protocol based on Elliptical Curve Cryptography (ECC) to enhance privacy through optimized key generation, encryption, and decryptions times.

4.2.5 Internet of Things

Similarly, Internet of Things (IoT) technology plays a vital role in the industrialization and realization of I4.0 objectives. This technology, which includes paradigms such as the Industrial Internet of Things (IIoT), the Internet of Everything (IoE), etc., incorporates connected sensor devices and data transmission means, enabling real-time monitoring, smart operations, event sensing, data analysis, self-decision, and process optimization [62, 78]. However, with the proliferation of interconnected smart devices and the substantial amounts of data being collected, careful consideration of both security and privacy is required [62, 73, 77-78, 80-81]. Sadique *et al.* [61] – for instance – highlight the issue of IoT data privacy and identify the areas where end-user and industry risks exist. Specifically, end devices, gateways, mobile devices, and communication channels are among the places where IoT risks are present. Jiang *et al.* [62] suggest that IIoT is an extension of cloud and edge computing; hence, the issue of industrial data privacy is very important, especially considering the increase in data volumes. Faujdar and Kaur [63] address the issue of IoT sharing private users' data. This is also raised by Xu *et al.* [55], where clients' data carried by IIoT applications are revealed during machine learning model training. Yang *et al.* [72] discuss multimedia data and the importance of security and privacy in IoT systems, examining how these factors can impact trustworthiness. Additionally, they classify multimedia into five categories and security and privacy into three levels, thus allowing for the implementation of effective measures. Zhang *et al.* [76] and Venkatesan *et al.* [87] explore the storage of IIoT data in the cloud, highlighting the importance of security and privacy research. On a different topic, Abdel-Basset *et al.* [77] note that IoT and I4.0 have increased the vulnerability of ICPSs, while Das *et al.* [78] highlight that IIoT has introduced new risks, making devices more susceptible to various attacks, such as cloning, impersonation, man-in-the-middle, and physical attacks. Then, Cao *et al.* [81] discuss the risks of IoT data leakage during transfer and the need for new data sharing and governance requirements for interconnected IoT devices to ensure effective privacy.

On the other hand, several approaches have been suggested to address the points outlined above. In [61], a framework for data privacy enhancement is suggested, emphasizing protection at IoT gateways. Jiang *et al.* [62] distinguish between social and industrial data and provide differential privacy applications for IIoT. Xu *et al.* [55] suggest several solutions, including encryption, secure multiparty computation, and differential privacy as a lightweight tool for data privacy. Yang *et al.* [72] identify several security and privacy requirements for IoT that can be addressed through schemes like cryptography, data hiding, chaos-based methods, and blockchain. Zhang *et al.* [76] focus on encryption solutions, highlighting VCLPKSE as a lightweight encryption scheme for protecting IIoT data before uploading ciphertext to cloud servers. This approach addresses trustworthiness issues in the IIoT environment by authenticating the data owner's identity and resisting two types of adversaries, thereby enhancing security and privacy measures. Abdel-Basset *et al.* [77] address privacy, eavesdropping, and data leakage issues by proposing a federated learning approach to add intelligence to the edge layers of IoT networks [80]. In [78], a

Physical Unclonable Function (PUF) with a Fuzzy Extractor (FE) is proposed as a two-factor authentication scheme for protecting IoT devices. Cao *et al.* [81] suggest the previously mentioned searchable encryption solution, focusing on identity authentication and access control to ensure systems' security and data privacy. Venkatesan *et al.* [87] emphasize the same solution and propose a Lightweight Searchable Encryption and Delegation (LSED) methodology with forward privacy to enable secure data storage and retrieval in IIoT-cloud systems. Finally, Li *et al.* [89] provide a secure data transmission mechanism for IIoT with a privacy-preserving hash-based deep learning method in separate encryption and decryption to protect privacy and address latency and increased computational costs.

4.2.6 Data Analysis Cluster

Data analysis plays a pivotal role in modern industrialization, serving as a key enabler for advancements through providing insights and directions for improvements, optimization, and efficiency. The literature has accordingly paid considerable attention to this and related topics. For instance, Li *et al.* [64] emphasize the benefits of training models collaboratively between industries; however, privacy, permissions, and data sharing emerge as significant risks and critical issues. Similarly, Huang *et al.* [65] address the same topic, highlighting the challenges facing centralized monitoring due to not sharing raw data externally, though privacy and leakage threats persist. Hinojosa-Palafox *et al.* [67] discuss the architecture design of industrial data analytics concerning big data and ICPS, emphasizing privacy concerns and the handling of sensitive data. Tajanpure and Muddana [68] address data mining applications and associated personal information risks; while they focus on statistically useful patterns, these applications still pose a threat of unrestricted access to records. Additionally, the authors emphasize the importance of sharing analytics privacy in I4.0 and the need for privacy-preserving techniques for real-time mining. Yang *et al.* [68] highlight the conflict between privacy policies and sharing data analysis and new results, emphasizing the need for a large-scale simulated alarm system to create event data for testing new methods. Zainudin *et al.* [74] discuss the privacy issues associated with centralized deep learning-based Intrusion Detection System (IDS) as well as the communication overhead. On a different note, Shi *et al.* [75] address the topic by highlighting the gap and the need for a trusted and controllable data management platform and ecosystem to handle industrial data issues. Additionally, they discuss challenges in data flow based on user behavior analysis results, such as security, privacy, and performance. Shrestha *et al.* [79] discuss knowledge extraction techniques and their potential for data misuse, manipulation, or privacy leakage. Moreover, they state that privacy is not well-considered in the design of smart grid systems due to the assumption that systems could be isolated. Finally, Milicic *et al.* [91] suggest that independent data mining systems cannot be fully automated.

On the solutions side, Li *et al.* [64] stress that traditional centralized data aggregation approaches should be avoided completely to protect privacy, opting for federated learning and federated data for collaboration when needed. In [65], distributed K-Singular Value Decomposition (K-SVD) method is suggested for

centralized data collection, as it can perform monitoring tasks without sharing local data between nodes, thus preserving privacy. Hinojosa-Palafox *et al.* [67] propose an architecture for collecting and integrating industrial data from IIoT and MIS, enabling subsequent industrial analytics. In [68], a convolution-based privacy-preserving algorithm that transforms data into lower dimensions, thus preserving its privacy while mining, is proposed. Such an algorithm benefits from better accuracy, data utility, and performance. In [74], the issue with deep learning-based IDS systems is addressed through a low-complexity federated learning-based IDS combined with a classification framework for SDN-based ICPS. This solution is becoming popular for industrial applications due to its effectiveness, privacy features, and low communication overhead. In [75], customizing and configuring strict, refined rule engines, assessing user access behavior before, during, and after data circulation, and establishing data access control and identity authentication mechanisms, are proposed. Bokrantz *et al.* [83] suggest adjusting the legal framework to manage ongoing issues, including the privacy of industrial data, thus making data systems more efficient and socially sustainable. Finally, Milicic *et al.* [91] present an ontology combined with PLM to protect industrial data privacy.

4.2.7 Artificial Intelligence Cluster

Artificial Intelligence (AI) technologies are currently driving the industry forward through their advanced human-like intelligence and capability for effective and efficient analysis and decision-making. As a result, significant focus has been placed on this field and related areas, particularly due to the privacy concerns they may raise. For instance, Wu *et al.* [59] examine Deep Learning, proposing an algorithm that provides strong industrial data privacy protection and high availability. Likewise, Li *et al.* [64] explore deep learning and emphasize collaboration for training powerful models, noting that centralized data aggregation model training is not preferred in real scenarios. Huang *et al.* [65] discuss dictionary learning methods and the privacy risks associated with industrial raw data, along with the increased risks from centralized data collection methods. O'Donovan *et al.* [71] highlight the role of AI in enabling I4.0. In [77], topics such as threat hunting and ICPS are covered, along with data federation and deep learning, highlighting the issues of training deep learning models centrally and the threats posed by transmitting data to other nodes. The study also underscores the challenges of developing distributed deep learning due to resources constraints and privacy matters, including eavesdropping and data leakage. Zhang *et al.* [80] and Huang *et al.* [82] also examine deep learning training models, emphasizing the privacy concerns associated with traditional centralized training methods. In [85], reinforcement learning is discussed in the context of edge computing, along with the role of parallel reinforcement learning for collaborative resource scheduling. Li *et al.* [88] highlight the role of AI in fault prediction, traffic analysis, and decision-making, discussing the regulatory challenges of transferring and exchanging industrial data between entities, which can limit the accuracy of AI models. Li *et al.* [89] focus on encryption methods in IIoT and cloud computing in

relation to AI. Lastly, Milicic *et al.* [91] focus on autonomous systems for PLM and discuss the use of data mining and AI in manufacturing systems.

Several solutions have been proposed in the literature to address some of the identified concerns. For example, Wu *et al.* [59] suggest privacy protection through the use of synthetic data semantics and centralized differential privacy models. Similarly, Jiang *et al.* [62] propose generating noisy data to protect privacy. Faujdar and Kaur [63] focus on conceptual aspects of privacy protection, such as enhancing security and awareness, as well as enforcing rules and policies. Li *et al.* [64] explicitly state that local data should not be shared for centralized AI model training to avoid privacy concerns. Huang *et al.* [65] suggest K-SVD dictionary learning method for monitoring without sharing local data between nodes, noting that a third party cannot infer the original data if it obtains the dictionary model, due to the over-completeness of the model, thus protecting industrial data privacy. O'Donovan *et al.* [71] opt for decentralized intelligence for its benefits, including near real-time performance, privacy, and the openness and interoperability of systems. Abdel-Basset *et al.* [77], Zhang *et al.* [80], and Huang *et al.* [82] highlight collaborative learning and training models, for their efficiency addressing privacy issues. Li *et al.* [88] suggest data aggregation for training models following the centralized learning, though this method might compromise the security and privacy of industrial data. Finally, Li *et al.* [89] recommend the use of AI in the form of convolutional neural networks to enhance privacy and present two deep learning schemes based on asynchronous patterns to preserve secrecy. They also note that combining deep learning with cryptographic methods offers several advantages, such as reducing computational costs and enhancing privacy preservation.

4.2.8 Federated Learning

Finally, although federated learning is a subset of data analysis and AI, it is highlighted separately in this section as it received special attention in the reviewed literature for its unique features, particularly decentralization and enhanced data privacy. For instance, Jiang *et al.* [60] suggest federated learning for industrial edge computing and highlight the need for emerging technologies to pay more attention to industrial data privacy. Li *et al.* [64] discuss federated transfer learning and emphasize the risks associated with centralized training. Huang *et al.* [65] examine federated dictionary learning in the field of monitoring, shedding light on economic and industrial risks of centralized data collection and emphasizing the risks associated with transmitting model parameters, hence the need for robust data privacy requirements in federated learning applications. Zainudin *et al.* [66] discuss Distributed Denial of Service (DDoS) attacks in SDN-enabled IIoT networks and the capabilities of federated learning in building resilience against such attacks. Yang *et al.* [72] address the challenges facing data security and privacy in IoT, highlighting federated learning among other protection schemes such as cryptography, data hiding, chaos-based methods, blockchain, and clustering. Zainudin *et al.* [74] discuss a federated learning IDS technique, highlighting privacy concerns and communication overhead associated with the use of centralized deep learning-based IDSs. Abdel-

Basset *et al.* [77] focus on federated threat hunting and discuss the limitations of distributed deep learning, emphasizing how federated learning addresses these issues. Additionally, they highlight the risks posed by central authorities, including their potential to provoke federated learning models if not fully trustworthy in managing model training. Shrestha *et al.* [79] address anomaly detection along with the security and privacy concerns arising from poorly shared local models. Zhang *et al.* [80] discuss federated learning techniques for distributed IIoT systems, emphasizing privacy concerns related to massive raw data from IIoT devices and highlighting the benefits of local data processing and model training. Huang *et al.* [82] discuss federated domain adaptation, highlighting the heterogeneity of local data, mutual information silos, and associated privacy risks. Finally, Li *et al.* [88] emphasize the use of federated learning to address the challenges of data silos and fragmented training data, pointing out the vulnerability of federated learning to interference and Byzantine attacks from aggregators and participants.

Regarding contributions and proposed solutions, several were identified. For instance, Jiang *et al.* [60] propose the use of federated edge learning based on differential privacy and adaptive compression for industrial data processing. Li *et al.* [64] suggest the inclusion of synthetic data to protect data sources. Zainudin *et al.* [66] emphasize decentralization through federated learning and the transmission of training parameters to an aggregation server, thus overcoming machine learning privacy concerns. Additionally, the authors mention the successful implementation of a federated learning-based IDS, also applied to DDoS attack classification. Xu *et al.* [55] propose the use of NICE privacy mechanism and Stackelberg games for federated learning, thus offering flexibility, control over one's own data, and preventing data and privacy leaks. Zainudin *et al.* [74] suggest combining federated learning with ICPS to transform IIoT applications into significant industrial domains where privacy concerns are effectively addressed. They also emphasize federated learning-based IDS systems for their low complexity, computational efficiency, and effectiveness in preserving privacy. In [77], a novel federated threat hunting approach is presented, providing threat intelligence solution suitable for all ICPS owners due to its efficiency, awareness of heterogeneity, and privacy-preserving characteristics against actors capturing network data. Shrestha *et al.* [79] propose using federated learning for anomaly detection in smart grid systems with artificial neural networks, such as Long Short-Term Memory (LSTM) autoencoders, along with homomorphic encryption to ensure privacy and security throughout the model training process. Zhang *et al.*[80] introduce a three-layer architecture of device-edge-cloud to support federated learning and optimize distributed IIoT networks by reducing backbone network traffic and parameter transmission. Huang *et al.* [82] propose an effective federated multi-source domain adaptation algorithm based on knowledge distillation and contrastive learning to train high accuracy models locally while protecting data privacy. Lastly, Li *et al.* [88] suggest a robust privacy-preserving Byzantine-based federated learning scheme (PBFL) that works for the majority or participants and aggregators, to protect privacy and leverage clustering.

5 Synthesis and Discussion

In this section we synthesize the findings and analyses by answering two key questions: “What are the implications?” and “What have we learnt and what should be done next?” [92-93].

First, current industrial systems encompass a broad spectrum of architectures and domains, from SCADA, DCS, and PLC-driven control commands to advanced MES, QMS, EMS, robotics, machine vision, additive manufacturing, communication networks, edge-computing platforms, and others. To understand these systems and their characteristics, they can be studied individually in context to reveal system-specific details and insights, or collectively in abstraction, which is the practical approach given the continuous growth of these systems [94]. Following the latter, the analysis reveals that industrial systems all share eight core characteristics: integration, connectivity, complexity, automation, distribution, coordination, specialization, and data-driven operation. These characteristics reflect a shared foundation focused on optimization, efficiency, reliability, scalability, and resilience, but the emphasis on each varies by domain. Such diversity suggests the need for tailored approaches to address system-specific challenges while leveraging shared foundations. Moreover, it indicates that frameworks aimed at protecting industrial data and its privacy must be layer-aware, recognizing that requirements differ sharply across systems.

Second, industrial data itself is multifaceted, spanning the fields of R&D, production, operation and maintenance, and management. Its value ranges from design and development data to real-time sensor streams and strategic business insights. The ability of industrial systems to optimize operations, manage resources, and maintain quality standards depends on how effectively this data is used. Given this diversity, industrial data carries varying levels of sensitivity and risks, which result in distinct threat profiles, such as:

- Data leakage threatens competitive advantage.
- Tampering with control commands affects operations and endangers safety.
- Unauthorized access to business records can result in regulatory fines.

Accordingly, data-sensitivity-driven protection strategies are essential, mapping privacy controls to the intrinsic value and vulnerability of each data type.

Third, the review of 34 studies revealed eight overlapping themes grouped into three areas:

1. Core privacy and security: differential privacy, anonymization, encryption, metrics, forward privacy.
2. Enabling technologies: Industry 4.0/CPS, IoT/IIoT, cloud/edge/fog.
3. Advanced analytics: big-data, data mining, AI/deep learning, federated and distributed learning.

These themes highlight not only different aspects of industrial systems, but also the interdisciplinary nature of this field, and the challenges of protecting data privacy across domains. Yet, these themes are largely treated in isolation, with solutions in

one domain often overlooking the constraints of another, e.g., homomorphic encryption and secure transit data networks secure "data in use" but impose computational overhead unsuitable for low-power edge devices, and federated learning preserves data locality but opens new threats and inference attacks at the analytics layer.

Fourth, to integrate these insights, we propose a layered guidance matrix that plots industrial data along two axes, Data Sensitivity (Low – routine operational and management records, to High – design and assets, as well as critical control parameters), and Latency Tolerance (Batch – datasets stored, collected, and processed in scheduled jobs, to Real-time – live streams of control and monitoring), assigning each quadrant specific privacy measures:

- **Real-time, high-sensitivity** (e.g., SIS data and critical SCADA control operations): lightweight homomorphic encryption + secure multiparty computation + strict identity and access control mechanisms
- **Real-time, low-sensitivity** (e.g., environmental and status sensors): data aggregation + anonymization at the edge.
- **Batch, high-sensitivity** (e.g., PLM datasets and CAD model archives): robust differential privacy + federated analytics + blockchain for trust and traceability
- **Batch, low-sensitivity** (e.g., historical logs and maintenance reports): encryption (in transit and at rest) + access control and authorization mechanisms.

This framework brings together system types, data categories, and identified threats into a practical tool for guiding privacy solutions across diverse industrial systems, shifting from broad classifications to concrete implementation approaches.

Fifth, despite the practical guidance offered by this framework and the existence of diverse solutions, several key gaps and critical challenges affect implementation, including:

1. The continuous evolution of industrial systems and the need for embedding privacy-by-design principles into core architecture of future systems.
2. Most existing approaches focus on specific technologies or components, lacking comprehensive, integrated methods that span the full industrial ecosystem.
3. Although many solutions exist in the literature, few studies explore how they can be combined in real environments without conflict or performance degradation.
4. Only a few works offer practical guidance on choosing and deploying Privacy Enhancing Technologies (PET).
5. Interoperability, coordination, and scalability remain underaddressed.
6. Promising solutions such as federated learning and blockchain still face practical implementation challenges and questions about adaptability to industrial contexts.
7. Addressing workforce skill gaps and change management issues, in addition to developing use cases that demonstrate the value of privacy-centric manufacturing, are essential for lasting adoption.

6 Conclusions and Future work

This study examines industrial systems, their roles, and their reliance on data to perform critical operations and advanced functionalities. It then focuses on industrial data, emphasizing its value and the importance of protecting its privacy amidst increasing risks in manufacturing. As an outcome, a comprehensive definition of modern industrial systems is proposed, along with identification of three key areas encompassing eight domains of conceptual measures and specific technologies related to industrial data privacy. The findings highlight the diversity of the topic and the multifaceted challenges it presents. This mandates the adoption of a multi-layered, holistic approach to develop comprehensive solutions that consider industrial data privacy from the outset, rather than relying on individual system-specific solutions requiring later adjustments. Additionally, a practical tool is proposed to guide industrial data privacy solutions based on data sensitivity and tolerance, combining system types and data categories; and identified threats and open challenges hindering implementation and adoption are also outlined. Future work should focus on fostering conceptual approaches, such as embedding privacy-by-design principles and addressing workforce skill gaps related to data privacy. Moreover, modern privacy-native technologies, including edge computing, differential privacy, and federated learning, should receive greater emphasis in industrial contexts and in relation to other solutions to overcome implementation constraints. Finally, PET, adaptive privacy frameworks, and operational conflicts, all require considerable attention.

References

1. Brennan, Louis, et al. "Manufacturing in the world: where next?." International Journal of Operations & Production Management 35.9 (2015): 1253-1274.
2. Agarwal, Nivedita, and Alexander Brem. "Strategic business transformation through technology convergence: implications from General Electric's industrial internet initiative." *International Journal of Technology Management* 67.2-4 (2015): 196-214.
3. ElMaraghy, Hoda, et al. "Evolution and future of manufacturing systems." *CIRP Annals* 70.2 (2021): 635-658.
4. Lu, Yang. "Industry 4.0: A survey on technologies, applications and open research issues." *Journal of industrial information integration* 6 (2017): 1-10.
5. Zhong, Ray Y., et al. "Intelligent manufacturing in the context of industry 4.0: a review." *Engineering* 3.5 (2017): 616-630.
6. Bordeleau, Fanny-Eve, Elaine Mosconi, and Luis Antonio Santa-Eulalia. "Business Intelligence in Industry 4.0: State of the art and research opportunities." (2018).
7. Wang, David. "Building value in a world of technological change: Data analytics and industry 4.0." *IEEE Engineering Management Review* 46.1 (2018): 32-33.
8. Martínez, Patricia López, et al. "A big data-centric architecture metamodel for Industry 4.0." *Future Generation Computer Systems* 125 (2021): 263-284

9. Kayabay, Kerem, et al. "Data science roadmapping: An architectural framework for facilitating transformation towards a data-driven organization." *Technological Forecasting and Social Change* 174 (2022): 121264.
10. Raptis, Theofanis P., Andrea Passarella, and Marco Conti. "Data management in industry 4.0: State of the art and open challenges." *IEEE Access* 7 (2019): 97052-97093.
11. Corallo, Angelo, et al. "Cybersecurity challenges for manufacturing systems 4.0: assessment of the business impact level." *IEEE Transactions on Engineering Management* 70.11 (2021): 3745-3765.
12. Haleem, Abid, et al. "Perspectives of cybersecurity for ameliorative Industry 4.0 era: A review-based framework." *Industrial Robot: the international journal of robotics research and application* 49.3 (2022): 582-597.
13. Onik, Md Mehedi Hassan, K. I. M. Chul-Soo, and Y. A. N. G. Jinhong. "Personal data privacy challenges of the fourth industrial revolution." *2019 21st International Conference on Advanced Communication Technology (ICACT)*. IEEE, 2019.
14. Waidner, Michael, and Michael Kasper. "Security in industrie 4.0-challenges and solutions for the fourth industrial revolution." *2016 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2016.
15. Timan, Tjerk, and Zoltan Mann. "Data protection in the era of artificial intelligence: trends, existing solutions and recommendations for privacy-preserving technologies." *The elements of big data value: Foundations of the research and innovation ecosystem*. Cham: Springer International Publishing, 2021. 153-175.
16. Sun, Liyuan, Hongyun Zhang, and Chao Fang. "Data security governance in the era of big data: status, challenges, and prospects." *Data Science and Management* 2 (2021): 41-44.
17. Guan, Zhongqi. "Difficulties and Solutions for Industrial Data Security and Compliance Governance." *International Conference on Cloud Computing*. Cham: Springer Nature Switzerland, 2023.
18. Chevallier, Arnaud. *Strategic thinking in complex problem solving*. Oxford University Press, 2016.
19. Cronin, Patricia, Frances Ryan, and Michael Coughlan. "Undertaking a literature review: a step-by-step approach." *British journal of nursing* 17.1 (2008): 38-43.
20. Ferrari, Rossella. "Writing narrative style literature reviews." *Medical writing* 24.4 (2015): 230-235.
21. The Royal Academy of Engineering. "Industrial Systems: capturing value through manufacturing". *The Royal Academy of Engineering*, 2012. https://raeng.org.uk/media/yurbqhvx/industrial_systems_capturing_value_through_manufacturing.pdf (accessed 25 August 2024)
22. Jamil, Uzair, and Joshua M. Pearce. "Energy Policy for Agrivoltaics in Alberta Canada." *Energies* 16.1 (2022): 53.
23. Holler, Jan, et al. *Internet of things*. Academic Press, 2014.
24. Badiru, Adedeji, Abidemi Badiru, and Adetokunboh Badiru. *Industrial project management: Concepts, tools, and techniques*. CRC Press, 2007.
25. Luo, Changkun. "Application Prospect of Data Mining Technology in Intelligent Manufacturing." *Academic Journal of Science and Technology* 3.1 (2022): 41-43.

26. Urbani, Michele. "Maintenance policies optimization in the Industry 4.0 paradigm." (2021).
27. Veblen, Thorstein. *The theory of business enterprise*. New English Library, 2003.
28. Levine, Stephen H. "Comparing products and production in ecological and industrial systems." *Journal of industrial ecology* 7.2 (2003): 33-42.
29. Boons, Frank, Wouter Spekkink, and Yannis Mouzakitis. "The dynamics of industrial symbiosis: a proposal for a conceptual framework based upon a comprehensive literature review." *Journal of cleaner production* 19.9-10 (2011): 905-911.
30. Whitelock, Jeryl. "Theories of internationalisation and their impact on market entry." *International marketing review* 19.4 (2002): 342-347.
31. Riahi-Belkaoui, Ahmed. *Behavioral management accounting*. Bloomsbury Publishing USA, 2001.
32. Dai, Xuewu, and Zhiwei Gao. "From model, signal to knowledge: A data-driven perspective of fault detection and diagnosis." *IEEE Transactions on Industrial Informatics* 9.4 (2013): 2226-2238.
33. Qi, Saiyu, et al. "Cpds: Enabling compressed and private data sharing for industrial Internet of Things over blockchain." *IEEE Transactions on Industrial Informatics* 17.4 (2020): 2376-2387.
34. Huo, Cui Hua, and Li He Chai. "Physical principles and simulations on the structural evolution of eco-industrial systems." *Journal of Cleaner Production* 16.18 (2008): 1995-2005.
35. Bas, Gerben. "Resilient Industrial Systems: A Complex System Perspective to Support Business Decisions." (2017).
36. Macaulay, Tyson, and Bryan L. Singer. *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS*. CRC Press, 2011.
37. Bhardwaj, Akashdeep, et al. "Capturing-the-invisible (CTI): Behavior-based attacks recognition in IoT-oriented industrial control systems." *IEEE access* 8 (2020): 104956-104966.
38. Campilho, Raul DSG, and Francisco JG Silva. "Industrial Process Improvement by Automation and Robotics." *Machines* 11.11 (2023): 1011.
39. Javaid, Mohd, et al. "Exploring impact and features of machine vision for progressive industry 4.0 culture." *Sensors International* 3 (2022): 100132.
40. Campbell, Thomas, et al. "Could 3D printing change the world." *Technologies, Potential, and Implications of Additive Manufacturing, Atlantic Council, Washington, DC* 3.1 (2011): 18.
41. Liu, Dan, et al. "Communication Quality Indicator System of Industrial Communication Network and Related Diagnostic Evaluation." (2022).
42. Harmatos, János, and Markosz Maliosz. "Architecture integration of 5G networks and time-sensitive networking with edge computing for smart manufacturing." *Electronics* 10.24 (2021): 3085.
43. Gröger, Christoph. "Industrial analytics–An overview." *it-Information Technology* 64.1-2 (2022): 55-65.
44. Wang, Lihui. "From intelligence science to intelligent manufacturing." *Engineering* 5.4 (2019): 615-618.

45. Grewal, Dalvinder Singh. "A critical conceptual analysis of definitions of artificial intelligence as applicable to computer engineering." *IOSR Journal of Computer Engineering* 16.2 (2014): 9-13.
46. Perwej, Yusuf, et al. "The internet of things (IoT) and its application domains." *International Journal of Computer Applications* 975.8887 (2019): 182.
47. Helmiö, Petra. "Open source in industrial internet of things: A systematic literature review." (2017).
48. Liu, Yang, et al. "Review on cyber-physical systems." *IEEE/CAA Journal of Automatica Sinica* 4.1 (2017): 27-40.
49. D'Antonio, Gianluca, Joel Sauza Bedolla, and Paolo Chiabert. "A novel methodology to integrate manufacturing execution systems with the lean manufacturing approach." *Procedia Manufacturing* 11 (2017): 2243-2251.
50. Avramovic, B., and L. H. Fink. "Energy management systems and control of FACTS." *International Journal of Electrical Power & Energy Systems* 17.3 (1995): 195-198.
51. Paraschivescu, Andrei Octavian. "The advantages of the process of integrating quality management system." *Economy Transdisciplinarity Cognition* 19.2 (2016): 48.
52. International Organization for Standardization. *ISO 9000: 2015 quality management systems-fundamentals and vocabulary*. 2015.
53. Werbińska-Wojciechowska, Sylwia, and Klaudia Winiarska. "Maintenance performance in the age of Industry 4.0: A bibliometric performance analysis and a systematic literature review." *Sensors* 23.3 (2023): 1409.
54. Schwab, Wolfgang, and Mathieu Poujol. "The state of industrial cybersecurity 2018." *Trend Study Kaspersky Reports* 33 (2018).
55. Xu, Yin, et al. "Incentive mechanism for differentially private federated learning in industrial Internet of Things." *IEEE Transactions on Industrial Informatics* 18.10 (2021): 6927-6939.
56. Okoli, Chitu, and Kira Schabram. "A guide to conducting a systematic literature review of information systems research." (2015).
57. Rowe, Frantz. "What literature review is not: diversity, boundaries and recommendations." *European Journal of Information Systems* 23.3 (2014): 241-255.
58. Schryen, Guido. "Writing qualitative is literature reviews—guidelines for synthesis, interpretation, and guidance of research." *Communications of the Association for Information Systems* 37.1 (2015): 12.
59. Wu, Wenjia, Qi Qi, and Xiaosheng Yu. "Deep learning-based data privacy protection in software-defined industrial networking." *Computers and Electrical Engineering* 106 (2023): 108578.
60. Jiang, Bin, et al. "Privacy-preserving federated learning for industrial edge computing via hybrid differential privacy and adaptive compression." *IEEE Transactions on Industrial Informatics* 19.2 (2021): 1136-1144.
61. Sadique, Kazi Masum, Rahim Rahmani, and Paul Johannesson. "Enhancing data privacy in the Internet of Things (IoT) using edge computing." *International*

Conference on Computational Intelligence, Security and Internet of Things. Cham: Springer International Publishing, 2020.
62. Jiang, Bin, et al. "Differential privacy for industrial internet of things: Opportunities, applications, and challenges." *IEEE Internet of Things Journal* 8.13 (2021): 10430-10451.
63. Faujdar, Pramod Kumar, and Gurmandeep Kaur. "A Framework for Internet of Things Services that Enhances Privacy." *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*. IEEE, 2023.
64. Li, Xu, et al. "Federated transfer learning in fault diagnosis under data privacy with target self-adaptation." *Journal of Manufacturing Systems* 68 (2023): 523-535.
65. Huang, Keke, et al. "A federated dictionary learning method for process monitoring with industrial applications." *IEEE Transactions on Artificial Intelligence* 4.5 (2022): 1017-1028.
66. Zainudin, Ahmad, et al. "FedDDoS: An efficient federated learning-based DDoS attacks classification in SDN-enabled IIoT networks." *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 2022.
67. Hinojosa-Palafox, Eduardo A., et al. "An analytics environment architecture for industrial cyber-physical systems big data solutions." *Sensors* 21.13 (2021): 4282.
68. Tajanpure, Rupali, and Akkalakshmi Muddana. "Data analysis with performance and privacy enhanced classification." *Journal of Intelligent Systems* 32.1 (2023): 20220215.
69. Yang, Guang, et al. "Simulating industrial alarm systems by extending the public model of a vinyl acetate monomer process." *2020 39th Chinese Control Conference (CCC)*. IEEE, 2020.
70. Paul, Annie, and S. Emalda Roslin. "A Brief Study on Security Preserved Data Aggregation Approaches in WSN s." *2023 Advanced Computing and Communication Technologies for High Performance Applications (ACCTHPA)*. IEEE, 2023.
71. O'Donovan, Peter, et al. "A comparison of fog and cloud computing cyber-physical interfaces for Industry 4.0 real-time embedded machine learning engineering applications." *Computers in industry* 110 (2019): 12-35.
72. Yang, Wencheng, et al. "Multimedia security and privacy protection in the internet of things: research developments and challenges." *International Journal of Multimedia Intelligence and Security* 4.1 (2022): 20-46.
73. Pivoto, Diego GS, et al. "Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review." *Journal of manufacturing systems* 58 (2021): 176-192.
74. Zainudin, Ahmad, et al. "Federated learning inspired low-complexity intrusion detection and classification technique for sdn-based industrial cps." *IEEE Transactions on Network and Service Management* (2023).
75. Shi, Fangning, Zhongli Na, and Zhifeng Gao. "Configurable Rule Engine for Industrial Data Flow Scenarios." *2023 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*. IEEE, 2023.

76. Zhang, Yulei, et al. "VCLPKES: Verifiable certificateless public key searchable encryption scheme for industrial Internet of Things." *IEEE Access* 8 (2020): 20849-20861.
77. Abdel-Basset, Mohamed, Hossam Hawash, and Karam Sallam. "Federated threat-hunting approach for microservice-based industrial cyber-physical system." *IEEE Transactions on Industrial Informatics* 18.3 (2021): 1905-1917.
78. Das, Ayan Kumar, et al. "Macp: Multifactor authentication using physical unclonable function and fuzzy extractor based chebyshev polynomial for industrial internet of things devices." *Transactions on Emerging Telecommunications Technologies* 33.11 (2022): e4581.
79. Shrestha, Rakesh, et al. "Anomaly detection based on lstm and autoencoders using federated learning in smart electric grid." *SSRN* (2023)
80. Zhang, Weiting, et al. "Optimizing federated learning in distributed industrial IoT: A multi-agent approach." *IEEE Journal on Selected Areas in Communications* 39.12 (2021): 3688-3703.
81. Cao, Keyan, et al. "An overview on edge computing research." *IEEE access* 8 (2020): 85714-85728.
82. Huang, Fang, et al. "A Federated Domain Adaptation Algorithm Based on Knowledge Distillation and Contrastive Learning." *Wuhan University Journal of Natural Sciences* 27.6 (2022): 499-507.
83. Bokrantz, Jon, et al. "Maintenance in digitalised manufacturing: Delphi-based scenarios for 2030." *International Journal of Production Economics* 191 (2017): 154-169.
84. Ahmadi, Saeed, and Maliheh Salehfar. "Privacy-preserving cloud computing: ecosystem, life cycle, layered architecture and future roadmap." *arXiv preprint arXiv:2204.11120* (2022).
85. Yang, Fan, et al. "pDPoSt+ sPBFT: A high performance blockchain-assisted parallel reinforcement learning in industrial edge-cloud collaborative network." *IEEE Transactions on Network and Service Management* 20.3 (2022): 2744-2759.
86. Kumar, Veepan, Prem Vrat, and Ravi Shankar. "A graph-theoretic approach to evaluate the intensity of barriers in the implementation of Industry 4.0." *International journal of innovation and technology management* 18.08 (2021): 2150039.
87. Venkatesan, S., K. Raja Rajeshwari, and M. Ramakrishnan. "A lightweight searchable encryption and delegation mechanism with forward privacy for improving the security of industrial internet of things-cloud systems." (2022).
88. Li, Wenjie, et al. "PBFL: Privacy-Preserving and Byzantine-Robust Federated Learning Empowered Industry 4.0." *IEEE Internet of Things Journal* (2023).
89. Li, Qizhong, Yizheng Yue, and Zhongqi Wang. "Deep Robust Cramer Shoup delay optimized fully homomorphic for IIOT secured transmission in cloud computing." *Computer Communications* 161 (2020): 10-18.
90. Sharma, Durgesh M., Shishir Kumar Shandilya, and Suresh Chandra Satapathy. "Maximizing blockchain security: Merkle tree hash values generated through

advanced vectorized elliptic curve cryptography mechanisms." *Concurrency and Computation: Practice and Experience* 35.23 (2023): e7829.
91. Milicic, Ana, et al. "An autonomous system for PLM domain data exploitation." International Journal of Computer Integrated Manufacturing 30.1 (2017): 109-120.
92. Campbell, Heather. "Planning to change the world: Between knowledge and action lies synthesis." *Journal of Planning education and Research* 32.2 (2012): 135-146.
93. McMahan, Peter, and Daniel A. McFarland. "Creative destruction: the structural consequences of scientific curation." *American Sociological Review* 86.2 (2021): 341-376.
94. Potts, Colin, and Idris Hsi. "Abstraction and context in requirements engineering: toward a synthesis." *Annals of Software Engineering* 3.1 (1997): 23-61.

Realizing Cyberprivacy: A Comparative Study and Implementation Roadmap Based on Privacy by Design Framework, GDPR and ISO/IEC 27701

Bahaa Eltahawy [0000-0001-6372-7547], Duong Dang [0000-0002-9325-5496],

Shakila Bu-Pasha [0000-0002-3240-9498], and Heidi Kuusniemi [0000-0002-7551-9531]

University of Vaasa, Vaasa 65200, Finland
firstname.lastname@uwasa.fi

Abstract. Cyberprivacy has been considered one of the most critical issues recently as our identities and personal information may fall into the wrong hands. Recognizing these concerns and their substantial effects, concerned authorities, governments and standardization organizations have taken several steps to protect personal data, regulate, and standardize cyberprivacy. For example, the European Union's (EU) General Data Protection Regulation (GDPR) aims at protecting data and preserving privacy within the EU member states, while the International Organization for Standardization's (ISO) ISO/IEC 27701 standard aims at managing privacy controls and reducing risks to individuals' privacy rights within organizations globally. These regulations and standards have enabled effective privacy management measures. However, from the implementer point of view, the GDPR is too broad, and the adoption and enforcement of ISO/IEC 27701 are relatively low. In this study, we propose the use and realization of the concepts of Privacy by Design (PbD) framework to achieve cyberprivacy. For this, a comprehensive and comparative study of the GDPR and ISO/IEC 27701 is conducted, and mapping to the PbD framework principles is performed. Accordingly, potential similarities and differences that might hinder the realization of cyberprivacy in practice are highlighted. Moreover, a practical implementation roadmap that meets the requirements of both the GDPR and ISO/IEC 27701 is proposed.

Keywords: Cyberprivacy, GDPR, ISO/IEC 27701, Privacy by Design.

1 Introduction

Advances in Information and Communication Technology (ICT) and fields of data science have brought many benefits, seen in better decision making, target group outreach, and personalization and customization of services. Data proliferation on the other hand has posed many threats to individuals, through invading their rights [1] via monitoring [2], conducting aggressive marketing and similar unwanted activities, and processing and sharing their personal information. Information security measures [3], i.e., Confidentiality, Integrity and Availability (CIA Triad), followed by the main cybersecurity

standards, e.g., ISO/IEC 27001, NIST, ENISA, etc. [4], have addressed the issue of data security. However, privacy, data control and sharing, could not be adequately addressed. First, because security measures deal with data in its raw form [3] without paying attention to the data context. Second, because of the current blurring between personal rights, against the capabilities, benefits, and potential of cyberization and the use of digital identity [5]. Although previous attempts tried to address this issue, e.g., the EU Data Protection Directive of 1995 [6] [7], they were outdated and insufficient, considering the rapid and unprecedented technological developments and capabilities.

With the increased awareness of personal rights, and the increase in privacy breaches and their subsequent effects, the issue of cyberprivacy became central to addressing. Privacy by Design (PbD) framework [8] was one of the fundamental and robust initiatives to encourage the design of systems, services, and products that consider privacy at their core and across all levels. The General Data Protection Regulation (GDPR) [9] [10] later has taken the issue of privacy to a different level by incorporating and unifying the regulatory perspective regarding privacy. However, first, the GDPR is a regulatory act, thus it only offers compliance and recommendations without actual means for implementation and enforcement [11]. Second, the GDPR is very broad, which makes practical realization challenging. This gap was addressed by the introduction of ISO/IEC 27701 privacy extension, which aims at standardizing privacy technology by means of improving Information Security Management Systems (ISMS) through incorporating means for maintaining and controlling data, thus leading to an effective Privacy Information Management System (PIMS). Still, the standard is relatively new, not widely adopted, and not well covered. It is worth mentioning that as of this writing, the European Commission has already made a proposal for the new e-Privacy Regulation [12], which will collaborate with the GDPR [13] and target cyber and online privacy by controlling processing, tracking and monitoring technologies.

In this study, we assess the GDPR and ISO/IEC 27701 standards with the aim of achieving cyberprivacy by realizing the principles of PbD framework from both regulatory and technical perspectives. The remainder of this paper is as follows: Section 2 presents the background and theoretical frameworks. Section 3 introduces the research method. Section 4 comprehensively introduces the GDPR and ISO/IEC 27701. In Section 5, a comparative analysis of the GDPR and ISO/IEC 27701, as well as a mapping with the PbD framework principles, are provided. Section 6 moves with the discussion and the suggested roadmap. Finally, Section 7 concludes and suggests future work.

2 Background and Theoretical Frameworks

2.1 Cyberprivacy

Previous work [14] has highlighted how the right to privacy being unobserved is currently one of the most complex issues to addressing. This is due to the proliferation of data, differences between stakeholders and their views while dealing with personal data, and the benefits against the concerns arising from the use of more accurate and sensitive data. With the issue of cyberprivacy, the most related concepts are cyberspace,

cybersecurity, data privacy or data protection, and Personally Identifiable Information (PII) [15], which are defined as follows:

1. Cyberspace is the global domain within the information environment consisting of the interdependent networks, processors and controllers of information technology infrastructures.
2. Cybersecurity is the organization, processes, and structures used to protect cyberspace and cyberspace-enabled systems.
3. Data privacy is the protection of an entity's data that is being collected, stored, and shared. Relevant to consider, while the term 'data privacy' is mostly used in the U.S., 'data protection' is used in the EU to imply an almost similar meaning. The GDPR is all about provisions for the protection of personal data. In spite of many overlaps and similarities between the rights to privacy and personal data protection, those terms are referred independently and separately in the EU and related recent legal instruments [16].
4. PII is any representation of information that permits the identity of an individual to whom the information applies to by either direct or indirect means. In this context, it is worth to mention here, this specification is a narrower version of the definition of 'personal data' stated in Article 4(1) of the GDPR which implies "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" [17].

To remove any ambiguity, it is important to clarify that cyberprivacy differs from cybersecurity, since they have distinct objectives, and that cybersecurity does not protect against tracking, processing, identifying, and sharing of PII. Additionally, cyberprivacy is more specific than data privacy, targeting individuals and PII, whereas data privacy is holistic. To make it clearer, as presented in our previous research, cyberprivacy can be defined and addressed through four lenses, as shown in Table 1 below.

Table 1. Cyberprivacy definitions [14].

Concept	Definition
Technical view	An extension of the domain of physical privacy in cyberspace, thus following the reasoning of what is permitted and what is not in physical domains
Socio-technical view	The collective set of norms and measures necessary to protect and control the activities and characteristics of cyber-identity in cyberspace and related domains
Rights view	concept that aims to maintain the rights to privacy, freedom, self-expression, self-determination, and reasonable behavior across cyberspace, and thus it is the intellectual ownership and accountability for storing, processing, and sharing information in cyberspace
Legislation view	

protection layer that aims to raise awareness against misuse of personal data, enforce control, and seek to amend data and attributes of pre-established relationships when needed

2.2 Privacy by Design Framework

Privacy by Design (PbD) [8] is a framework that encourages proactive privacy and the integration of data protection considerations into the design and operation of information systems, processes, and policies. PbD seeks to integrate privacy and data protection measures into the core of the design phase, promoting organizations to proactively identify and address potential privacy risks throughout all phases and processes, rather than dealing with such issues and risks later.

Article 25 (along with Recital 78) of the GDPR is considered one of the most important provisions requiring data protection by design and by default with implementing appropriate technical and organizational measures from the onset of a service and as a default feature. Such a practice from the data controllers' (companies and organizations) side will be beneficial, time-saving and cost-efficient as well as can promote safe and secured online environment for the data subjects [18]. Pseudonymization [Art.4(5) GDPR] and data protection impact assessment (Art. 35 GDPR) for example are two GDPR-suggested measures to implement data protection by design [19].

PbD encompasses activities like conducting privacy impact assessments, using privacy-enhancing technologies, implementing robust data security measures, and ensuring transparency and accountability in data handling practices. This approach can accordingly safeguard and preserve individuals' privacy and personal data while enabling organizations to meet their goals. In Figure 1, the main principles of PbD are shown. As depicted in Figure 1, PbD encompasses seven key principles, which consider privacy from the outset. These principles include proactively planning for privacy and considering privacy as the default setting, embedding privacy into the design phase, ensuring full functionality of systems with minimal effects, implementing end-to-end security measures for data protection, establishing the foundation for consent, visibility, and transparency, and finally shifting controls to the end user's domain.

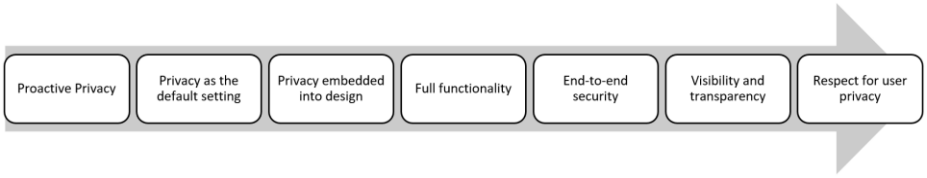


Fig. 1. Privacy by design framework principles [8].

2.3 Privacy by Design for Cyberprivacy

As seen from the definitions of cyberprivacy in Section 2.1, cyberprivacy is a complex concept that incorporates several divergent views. Accordingly, to achieve cyberprivacy, a holistic approach [14] that incorporates all these views, i.e., technical and social while considering rights and legislation perspectives, is needed. The GDPR and

ISO/IEC 27701 in particular can offer the means and controls for achieving cyberprivacy since they address the issue of privacy and PII from different angles, and provide technical and social, along with regulatory perspectives on the topic. However, since there is no explicit and unique guidance on how to apply these standards for achieving cyberprivacy, PbD can be used to provide such a rational and reliable implementation roadmap needed. In Figure 2, we show the suggested relationship between cyberprivacy, PbD, GDPR and ISO/IEC 27701. As suggested, measures from the GDPR and ISO/IEC 27701 are adopted by PbD to provide an implementation roadmap, and hence become a part of cyberprivacy.

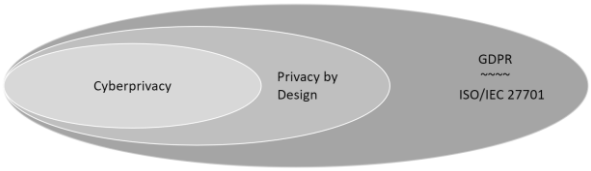


Fig. 2. The suggested relationship between cyberprivacy and Privacy by Design

3 Method

This work uses a qualitative comparative analysis [20] approach to study the GDPR and ISO/IEC 27701, with the aim of highlighting similarities, overlaps, and potential differences that might hinder full realization of cyberprivacy. For this task, the list of reports and standards given in Table 2 below, is used.

Table 2. Reports and standards used in this work

Standard	Source
GDPR	The EU General Data Protection Regulation – Official Journal of the EU
	Guidelines of the European Data Protection Board (EDPB)
	The EU Data Protection Directive
ISO/IEC 27701	ISO/IEC 27701:2019 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines
	ISO/IEC 27001:2022 Information Security Management Systems
	ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls

4 The GDPR and ISO/IEC 27701

4.1 The General Data Protection Regulation – GDPR

In order to address the increased privacy and personal data protection concerns of the Internet and digital platforms users, the EU introduced in 2016 its unanimous

regulation, the General Data Protection Regulation (GDPR), which came into effect in May 2018. Influenced by other regulations and standards as shown in Figure 3, the GDPR aims to expand existing data protection principles while introducing new measures to protect PII within organizations. In its 11 chapters comprising 99 articles, the regulation outlines how organizations can collect data, provides use cases, and addresses the sharing of PII outside their intended scope. The key principles of the GDPR include: ensuring lawfulness, fairness and transparency; setting and defining intended purposes; minimizing and controlling data; maintaining accurate and up-to-date personal data; limiting storage duration and purposes; ensuring data security and confidentiality; and enforcing accountability and responsibility for compliance. The GDPR covers several concepts [9], including: requiring consent and limiting data processing; encouraging data encryption; effective fines and penalties; defining personal data; ongoing privacy assessments; designing preserving privacy systems incorporating Privacy Enhancing Technologies (PET); specifying reasons for gathering and processing data; defining use cases for existing and processed records; requiring consent for changes; providing the right to delete own data; and outlining conditions for sharing data outside the use area. In Figure 4, we show how data is handled according to the GDPR.

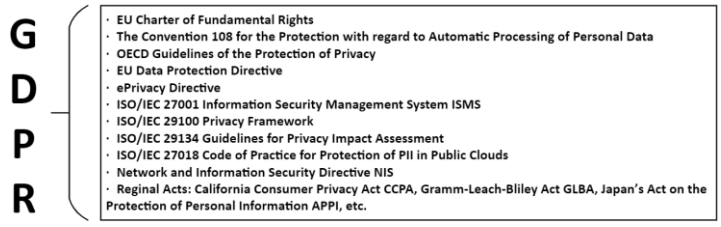


Fig. 3. Regulations and standards influenced the GDPR [21]

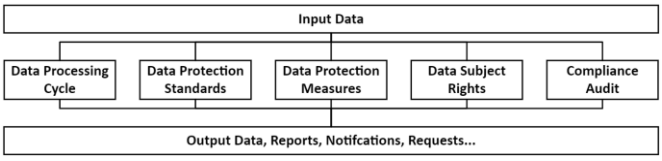


Fig. 4. The GDPR as a framework

In figure 4, the input data is all data that has been collected and processed, including PII. The data processing cycle is the steps that organizations must consider while collecting, using and storing PII in compliance with the GDPR. Data protection standards are the technical standards and measures used to protect data, including encryption, data minimization and retention. Other standards might be used here depending on the sector, e.g., ISO 27001. For the data protection measures, the GDPR specifically refers to the protection of personal data from unauthorized access, disclosure, damage or loss. The GDPR offers a range of rights on the individuals or data subjects and controls over own data, such as accessing own data, the right to prevent the processing of data, and

the right to be removed from a system and requesting deletion of own data. Compliance audit is the processes of reviewing and assessing an organization and its compliance with the GDPR. Finally, the output data is all the data generated, e.g., compliancy reports, incidents, breaches, countermeasures, notifications, requests, etc.

4.2 ISO/IEC 27701

ISO/IEC 27701:2019 [22] standard aims at standardizing privacy protection practices by mandating measures and controls for Privacy Information Management System (PIMS). ISO/IEC 27701 is basically an extension to ISO/IEC 27001 – ISMS – and ISO/IEC 27002 – Code of practice for information security controls – standards. The standard incorporates requirements for privacy controls through the addition of 8 supplementary clauses, thus adopting the structure and integrating the controls found in these standards into its clauses and annexes. Regarding its structure, ISO/IEC 27701 starts with clause 4 which provides the position of the additional requirements, then clause 5 which provides specific PIMS requirements by adopting 21 controls from ISO/IEC 27001 as well as enhancing 5 controls, and clause 6 which provides specific PIMS guidance by adopting 144 controls from ISO/IEC 27002 while enhancing 32 controls. Clauses 7 and 8 focus directly on the concept of privacy by providing guidance for PII controllers and processors, respectively, and introducing new 49 controls. Finally, the standard follows with 6 annexes that specify explicitly PIMS control objectives and controls for both controllers and processors; provide mapping with ISO/IEC 29100 privacy framework, the GDPR, ISO/IEC 27018 code of practice for protection of PII in public clouds acting as PII processors, ISO/IEC 29151 code of practice for PII protection; and lastly show how the standard applies to ISO/IEC 27001 and 27002. In Figure 5, a schematic diagram of ISO/IEC 27701 and associated standards, is shown.

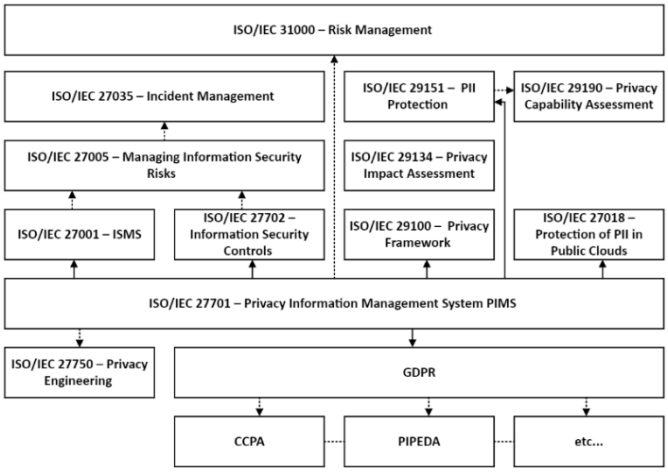


Fig. 5. ISO/IEC 27701 associated standards

8

In Figure 5, alongside the abovementioned standards directly linked and represented by **solid arrows**, ISO/IEC 27701 places a strong emphasis on risk assessment by incorporating practices from ISO/IEC 31000 – risk management, ISO/IEC 27005 – managing information security risks, ISO/IEC 27035 – information security incident management, ISO/IEC 29134 – privacy impact assessment, and ISO/IEC 29190 – privacy capability assessment model, which are indicated by **dashed arrows**. Practices of these standards help identify and assess privacy risks, implement controls for risk mitigation, and monitor the effectiveness of the deployed controls. ISO/IEC 27701 encompasses also provisions for establishing and maintaining privacy policies, defining roles and responsibilities for privacy management, and ensuring that privacy requirements are considered by third-party service providers. Finally, through its alignment with the GDPR, the standard serves as an enabler for seamless integration with other regional privacy regulations, e.g., CCPA and GLBA, as seen in Figure 3.

5 Comparative Analysis and Results

In this section, we proceed with a comprehensive analysis of both the GDPR and ISO/IEC 27701, pursuing two main objectives. First, to highlight the similarities and areas of overlap between the two, along with their distinctive features and potential conflicts. Second, to map them with the PbD framework principles.

5.1 Similarities and Overlaps

From interpreting, analyzing and comparing the GDPR and ISO/IEC 27701, it was found that one article from the GDPR can match one or more clauses from ISO/IEC 27701, depending on the context and interpretation. This can result in increased complexity when considering both standards simultaneously. To facilitate adoption and integration between the two, we have highlighted the similarities and overlaps between the different articles and clauses, and marked them with three labels, "**Not applicable**" which denotes that the concept or section was absent, "**Directly related**" which indicates an explicit match, and finally "**Indirectly related**" which means that the concept lacked an explicit match but was understood from the context, as follows:

1. GDPR Chapter 1, General Provisions: **Not applicable to ISO/IEC 27701**
2. GDPR Chapter 2, Principles: **Directly related to ISO/IEC 27701** 6.3.2.1 Mobile device policy; 6.5.2.1 Classification of information; 6.5.2.2 Labelling of information; 6.5.3.1 Management of removable media; 6.5.3.2 Disposal of media; 6.5.3.3 Physical media transfer; 6.6.2.1 User registration and de-registration; 6.6.2.2 User access provisioning; 6.6.4.2 Secure log-on procedures; 6.8.2.7 Secure disposal or reuse of equipment; 6.8.2.9 Clear desk and clear screen policy; 6.9.3.1 Information backup; 6.9.4.1 Event logging; 6.9.4.2 Protection of log information; 6.10.2.1 Information transfer policies and procedures; 6.10.2.4 Confidentiality or non-disclosure agreements; 6.11.1.2 Securing application services on public networks; 6.11.3.1 Protection of test data; 6.12.1.2 Addressing security within supplier agreements; 6.13.1.1 Responsibilities and procedures; 6.15.1.1 Identification of applicable

legislation and contractual requirements; 6.15.1.3 Protection of records; 7.2.1 Identify and document purpose; 7.2.2 Identify lawful basis; 7.2.3 Determine when and how consent is to be obtained; 7.2.4 Obtain and record consent; 7.2.6 Contracts with PII processors; 7.2.8 Records related to processing PII; 7.3.2 Determining information for PII principals; 7.3.3 Providing information to PII principals; 7.3.4 Providing mechanism to modify or withdraw consent; 7.3.6 Access, correction and/or erasure; 7.4.1 Limit collection; 7.4.3 Accuracy and quality; 7.4.4 PII minimization objectives; 7.4.5 PII de-identification and deletion at the end of processing; 7.4.6 Temporary files; 7.4.8 Disposal; 7.4.9 PII transmission controls; 8.2.2 Organization's purposes; 8.2.3 Marketing and advertising use; 8.4.1 Temporary files; 8.4.3 PII transmission controls

3. GDPR Chapter 3, Rights of the data subject: **Directly related to ISO/IEC 27701** 7.2.2 Identify lawful basis; 7.3.1 Determining and fulfilling obligations to PII principals; 7.3.2 Determining information for PII principals; 7.3.3 Providing information to PII principals; 7.3.4 Providing mechanism to modify or withdraw consent; 7.3.5 Providing mechanism to object to PII processing; 7.3.6 Access, correction and/or erasure; 7.3.7 PII controllers' obligations to inform third parties; 7.3.8 Providing copy of PII processed; 7.3.9 Handling requests; 7.3.10 Automated decision making; 7.4.7 Retention; 7.5.1 Identify basis for PII transfer between jurisdictions; 7.5.2 Countries and international organizations to which PII can be transferred; 8.3.1 Obligations to PII principals
4. GDPR Chapter 4, Controller and processor: **Directly related to ISO/IEC 27701** 5.2.1 Understanding the organization and its context; 5.2.2 Understanding the needs and expectations of interested parties; 5.2.3 Determining the scope of the information security management system; 5.2.4 Information security management system; 5.4.1.2 Information security risk assessment; 5.4.1.3 Information security risk treatment; 6.2.1.1 Policies for information security; 6.3.1.1 Information security roles and responsibilities; 6.4.2.2 Information security awareness, education and training; 6.5.2.1 Classification of information; 6.5.3.1 Management of removable media; 6.5.3.3 Physical media transfer; 6.7.1.1 Policy on the use of cryptographic controls; 6.9.3.1 Information backup; 6.10.2.4 Confidentiality or non-disclosure agreements; 6.11.1.2 Securing application services on public networks; 6.11.2.1 Secure development policy; 6.12.1.2 Addressing security within supplier agreements; 6.13.1.1 Responsibilities and procedures; 6.13.1.5 Response to information security incidents; 6.15.1.1 Identification of applicable legislation and contractual requirements; 6.15.1.3 Protection of records; 6.15.2.1 Independent review of information security; 6.15.2.3 Technical compliance review; 7.2.1 Identify and document purpose; 7.2.5 Privacy impact assessment; 7.2.6 Contracts with PII processors; 7.2.7 Joint PII controller; 7.2.8 Records related to processing PII; 7.4.2 Limit processing; 7.4.5 PII de-identification and deletion at the end of processing; 7.5.1 Identify basis for PII transfer between jurisdictions; 7.5.2 Countries and international organizations to which PII can be transferred; 7.5.3 Records of transfer of PII; 7.5.4 Records of PII disclosure to third parties; 8.2.1 Customer agreement; 8.2.2 Organization's purposes; 8.2.4 Infringing instruction; 8.2.5 Customer obligations; 8.2.6 Records related to processing PII; 8.3.1 Obligations to PII principals; 8.4.2 Return, transfer or

disposal of PII; 8.5.2 Countries and international organizations to which PII can be transferred; 8.5.3 Records of PII disclosure to third parties; 8.5.4 Notification of PII disclosure requests; 8.5.6 Disclosure of subcontractors used to process PII; 8.5.7 Engagement of a subcontractor to process PII; 8.5.8 Change of subcontractor to process PII

5. GDPR Chapter 5, Transfers of personal data to third countries or international organizations: **Directly related to ISO/IEC 27701** 7.5.1 Identify basis for PII transfer between jurisdictions; 8.5.1 Basis for PII transfer between jurisdictions; 8.5.5 Legally binding PII disclosures
6. GDPR Chapter 6, Independent supervisory authorities: **Indirectly related to ISO/IEC 27701** 5.3.1 Leadership and commitment; 5.3.2 Policy; 5.3.3 Organizational roles, responsibilities and authorities
7. GDPR Chapter 7, Cooperation and consistency: **Indirectly related to ISO/IEC 27701** 5.2.1 Understanding the organization and its context; 5.2.2 Understanding the needs and expectations of interested parties; 5.3.1 Leadership and commitment
8. Chapter 8, Remedies, liability and penalties: **Indirectly related to ISO/IEC 27701** 5.7.1 Monitoring, measurement, analysis and evaluation; 5.8.1 Nonconformity and corrective action
9. GDPR Chapter 9, Provisions relating to specific processing situations: **Indirectly related to ISO/IEC 27701** 7.2.2 Identify lawful basis; 7.4 privacy by design and privacy by default
10. GDPR Chapter 10, Delegated acts and implementing acts: **Not applicable to ISO/IEC 27701**
11. GDPR Chapter 11, Final provisions: **Not applicable to ISO/IEC 27701**

It was clear from this analysis that the concepts of the GDPR and ISO/IEC 27701 do not always align seamlessly, which is inherently due to their distinct natures, one as a regulatory act while the other as a technical and implementation standard.

5.2 Features and Differences

In Table 3 [9] [11] [22], the main features and differences between the GDPR and ISO/IEC 27701, are shown.

Table 3. Features and differences between the GDPR and ISO/IEC 27701 [9] [11] [22]

Feature	GDPR	ISO 27701
Objective	Protects personal data of EU residents	Provides a framework for managing PII
Scope	Applies to all EU data subjects and controllers	Applies to all organizations with PII
Requirements	Requires organizations to comply with several data protection principles and implement technical and organizational measures to protect personal data	Requires organizations to implement a Privacy Information Management System (PIMS) based on risk management approach and best practices

Applicability	Applicable to organizations that process personal data of EU residents, regardless of their location	Applicable to any organization that processes PII, regardless of its location or industry sector
Legal Basis	Based on EU Regulation	Not legally enforceable
Penalties	Can result in fines up to €20 million or 4% of global annual turnover, whichever is higher	No specific penalties, but non-compliance may affect an organization's ability to obtain certification or partner with other organizations
Data Subject Rights	Includes the right to access, rectify, erase, restrict, and object to processing of personal data	Includes the same rights as GDPR, with rights such as the right to portability and the right to object to automated decision-making
Third-Party Management	Requires organizations to ensure that third-party processors also comply with GDPR	Requires organizations to have a process in place to evaluate and manage the risks associated with third-party access to PII
Certification	Offers a certification scheme for compliance with GDPR	Offers a certification scheme for compliance with ISO 27701
Key Benefits	Increases trust and transparency for EU data subjects, improves data security, and helps organizations avoid fines and legal action	Helps organizations implement best practices for PII management, improve data protection, and demonstrate compliance to stakeholders
Objective	Protects personal data of EU residents	Provides a framework for managing PII
Scope	Applies to all EU data subjects and controllers	Applies to all organizations with PII
Requirements	Requires organizations to comply with several data protection principles and implement technical and organizational measures to protect personal data	Requires organizations to implement a Privacy Information Management System (PIMS) based on risk management approach and best practices

Several issues exist between the GDPR and ISO/IEC 27701, as they handle certain aspects differently. Below is a list of the most potential differences:

1. Data Subject Rights: The GDPR gives individuals the right to access, rectify, and erase their personal data. ISO/IEC 27701 however requires organizations to retain personal data to meet legal, regulatory, or business requirements.
2. Data Minimization: The GDPR requires organizations to only collect and process the minimum amount of personal data necessary to achieve a specific purpose. ISO/IEC 27701 on the contrary requires organizations to maintain an inventory of personal data processing activities.
3. Risk Assessment: The GDPR requires organizations to conduct risk assessments to identify and mitigate privacy risks, which is not an explicit requirement for ISO/IEC 27701.

4. Incident Response: The GDPR mandates that organizations notify authorities of data breaches within 72 hours of becoming aware of a breach. ISO/IEC 27701 requires organizations to have a documented incident management process to address data breaches, but it does not specify a timeframe for notification. This may create a conflict regarding notification.
5. Third-Party Management: The GDPR and ISO/IEC 27701 both mandate that organizations ensure third-party service providers processing personal data meet privacy requirements. However, ISO/IEC 27701 does not explicitly reference the GDPR, potentially causing compliance confusion if an organization adopts both.

5.3 The GDPR and ISO/IEC 27701 Vs. Privacy by Design Framework

Regarding the PbD Framework, the GDPR explicitly refers to PbD, e.g., Article 25 – Data Protection by Design and by Default [21], which is not the case with ISO/IEC 27701 (ISO, 2019). Nevertheless, ISO/IEC 27701 still aligns with and incorporates key PbD principles. Following is how the GDPR Articles (A) and ISO/IEC 27701 can align with the PbD Framework, utilizing the same notations used in Section 5.1:

1. PbD Principle 1, Proactive not reactive privacy
   GDPR: **Directly related** A:35 - Data Protection Impact Assessment (DPIA) Indirect: A:24 - Responsibility of the controller; A:25 - Data protection by design and by default; A:32 - Security of processing; A:5 - Principles relating to processing of personal data
   ISO/IEC 27701: 5.2- Context of the organization; 5.5.3- Awareness; 5.6.1- Operational planning and control; 5.6.2- Information security risk assessment; 6.13- Information security incident management; 7.2.5- Privacy impact assessment
2. PbD Principle 2, Privacy as the default setting
   GDPR: **Directly related** A:5 - Principles relating to processing of personal data; A:25 - Data protection by design and by default; Recital 78 - Data protection by design and by default; A:3 - Security of processing; A:89 - Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; Indirect A:6 - Lawfulness of processing; A:9 - Processing of special categories of personal data; A:22 - Automated individual decision-making, including profiling; A:30 - Records of processing activities
   ISO/IEC 27701: 5.4.2- Information security objectives and planning to achieve them; 6.6- Access control; 7.2.1- Identify and document purpose; 7.2.4- Obtain and record consent;7.4- Privacy by design and privacy by default for PII controllers; 7.5- PII sharing, transfer, and disclosure for controllers; 8.4- Privacy by design and privacy by default for PII processors; 8.5- PII sharing, transfer, and disclosure for processors
3. PbD Principle 3, Privacy embedded
   GDPR: **Directly related** A:5 - Lawfulness, fairness, and transparency; A:25 - Data protection by design and by default; A:32 - Security of processing; A:35 - Data protection impact assessment; A:36 - Prior consultation; A:42 – Certification Indirect

A:6 - Legitimate interests; A:9 - Processing of special categories of personal data; A:17 - Right to erasure ('right to be forgotten'); A:30 - Records of processing activities; A:35 - Data protection impact assessment
ISO/IEC 27701: 5.2.1 Understanding the organization and its context; 5.6.3- Information security risk treatment; 7.2.5- Privacy impact assessment; 7.4- Privacy by design and privacy by default for PII controllers; 8.4- Privacy by design and privacy by default for PII processors

4. PbD Principle 4, Full functionality
GDPR: **Directly related** A:25 - Data protection by design and by default; A:32 - Security of processing; A:35 - Data protection impact assessment; Recital 78 - Data protection impact assessment **Indirectly related** A:5 - Principles relating to processing of personal data; A:6 - Lawfulness of processing; A:32 - Security of processing; A:35 - Data protection impact assessment
ISO/IEC 27701: 5.2- Context of the organization; 5.3- Leadership; 5.4- Planning; 5.5.2- Competence; 5.6.1- Operational planning and control; 5.7- Performance evaluation; 7.3.1- Determining and fulfilling obligations to PII principals
5. PbD Principle 5, End-to-end security
GDPR: **Directly related** A:5 - Lawfulness, fairness, and transparency; A:24 - Responsibility of the controller; A:32 - Security of processing; A:35 - Data protection impact assessment; A:36 - Prior consultation **Indirectly related** A:25 - Data protection by design and by default; A:28 – Processor; A:30 - Records of processing activities; A:45 - Transfers on the basis of an adequacy decision; A:49 - Derogations for specific situations
ISO/IEC 27701: 5.3.2- Policy; 5.3.3- Organizational roles, responsibilities and authorities; 5.4.2- Information security objectives and planning to achieve them; 6.2- Information security policies; 6.6- Access control; 6.7- Cryptography; 6.8- Physical and environmental security; 6.9- Operations security; 6.10- Communications security; 7.4- Privacy by design and privacy by default for PII controllers; 8.4- Privacy by design and privacy by default for PII processors
6. PbD Principle 6, Visibility and transparency
GDPR: **Directly related** A:5 - Lawfulness, fairness, and transparency; A:12 - Transparent information, communication and modalities for the exercise of the rights of the data subject; A:13 - Information to be provided where personal data are collected from the data subject; A:14 - Information to be provided where personal data have not been obtained from the data subject; A:15 - Right of access by the data subject; A:21 - Right to object; A:22 - Automated individual decision-making, including profiling; A:25 - Data protection by design and by default; A:32 - Security of processing **Indirectly related** A:6 - Lawfulness of processing; A:9 - Processing of special categories of personal data; A:17 - Right to erasure; A:20 - Right to data portability; A:35 - Data protection impact assessment
ISO/IEC 27701: 5.3- Leadership; 5.5.2- Competence; 5.5.3- Awareness; 5.5.4- Communication; 5.6.3- Information security risk treatment
7. PbD Principle 7, Respect for user privacy
GDPR: **Directly related** A:5 - Principles relating to processing of personal data; A:6 Lawfulness of processing; A:9 Processing of special categories of personal data;

14

A:21 Right to object; A:25 Data protection by design and by default **Indirectly related** A:24 - Responsibility of the controller; A:28 - Processor; A:32 Security of processing; A:35 Data protection impact assessment; A:36 Prior consultation
ISO/IEC 27701: 7.2- Conditions for collection and processing for PII controllers; 7.3- Obligations to PII controllers principals; 8.2- Conditions for collection and processing for PII processors; 8.3- Obligations to PII processors principals

6 Discussion and Implementation Roadmap

Cyberprivacy is an open question that keeps receiving much attention due to its importance and implications once private data gets exposed or misused [14]. The issue has been noticed and attempts are being taken continuously to address it; however, as technologies advance and expand their capabilities, the situation gets more challenging. The most challenging issue with cyberprivacy is that it is not a technical issue, but is a set of interconnected issues, ranging from technical, social and legal, that need a holistic solution to address them simultaneously. With the GDPR [21] and ISO/IEC 27701 [22], the standard for privacy has moved to a more advanced level. Now, organizations increasingly focus on the GDPR and ISO/IEC 27701, to achieve compliance, obtain certification, and unlock additional opportunities and benefits. However, when it comes to practical terms, the GDPR lacks certain elements that ISO/IEC 27701 can provide, such as technical means and the explicit mention of measures and controls. Still, attempting to adopt both standards may lead to redundancy and excessive burden. Yet, the two do not substitute each other or cover all aspects of data privacy and PII individually.

In this endeavor, we propose adopting a governance framework and a process model, as in [23] and [24], while utilizing the principles of PbD framework, to provide a rational and reliable implementation roadmap for cyberprivacy incorporating the GDPR and ISO/IEC 27701, as detailed below:

1. **Assess Current State**: Evaluate current privacy practices, data processing activities, and associated risks; Identify gaps and areas for improvement to align with the GDPR and ISO/IEC 27701; Conduct a comprehensive data inventory to identify personal data holdings and associated risks; Identify existing ISMS systems.
2. **Establish Data Protection Governance**: Appoint responsible individuals for overseeing compliance; Develop and communicate a privacy policy outlining commitment to the GDPR and PbD; Establish processes and procedures for handling data subject rights requests, data breaches, and Privacy Impact Assessments (PIAs).
3. **Develop a Privacy Governance Framework**: Define policies, procedures, and guidelines in accordance with GDPR and ISO 27701; Incorporate PbD principles.
4. **Conduct Data Mapping and Inventory**: Identify all personal data collected, processed, stored, and shared across the organization; Document data flows, purposes, legal bases, and third-party involvement.
5. **Enhance Consent and Transparency**: Review and update consent mechanisms to meet the GDPR requirements; Develop clear and accessible privacy policies.
6. **Implement Privacy by Design**: Embed privacy considerations into design, processes, and products; Apply pseudonymization, data minimization, and PETs.

7. **Establish Data Subject Rights Processes**: Implement mechanisms to exercise privacy rights (access, rectification, erasure, etc.); Develop procedures for responding to data subject requests within the GDPR timelines.
8. **Conduct Privacy Impact Assessments**: Perform PIAs for high-risk processing activities and new initiatives; Mitigate identified privacy risks and ensure compliance.
9. **Enhance Security and Incident Response**: Align information security practices with ISO/IEC 27001; Develop incident response procedures.
10. **Implement Supplier Management Practices**: Evaluate and update third-party vendor contracts to include the GDPR; Assess third-party compliance.
11. **Conduct Training and Awareness**: Provide comprehensive privacy training; Raise awareness of the GDPR, ISO/IEC 27701, and PbD principles.
12. **Continuous Monitoring, Reviewing, and Improvement**: Regularly review and update privacy policies, procedures, and controls; Perform regular audits and reviews to assess ongoing compliance; Monitor, measure, and enhance the effectiveness of practices, controls, and privacy risk management processes based on lessons learned.

7 Conclusion, Limitations, and Future Work

This work has attempted to achieve the concept of cyberprivacy by realizing the principles of PbD framework through incorporating the GDPR and ISO/IEC 27701 simultaneously. The main contributions of this study include: 1) conducting comprehensive reviews of the GDPR and ISO/IEC 27701, 2) proposing the use of PbD to achieve cyberprivacy, 3) showing similarities and potential differences between the GDPR and ISO/IEC 27701, 4) mapping the GDPR and ISO 27701 with PbD framework, 5) finally, proposing a detailed roadmap to help achieve cyberprivacy. The key takeaways from this work are: 1) cyberprivacy is a list of interconnected abstract concepts, and thus requires other means, frameworks, and measures to help achieve it, 2) while the objectives of the GDPR and ISO/IEC 27701 closely align, these standards are not interchangeable. On the limitation side, it is important to note that the analysis and the roadmap have relied on desk research, utilizing standards and official documents as primary resources. Finally, in a continuation of this work, next steps include: 1) applying the proposed roadmap into different sectors, to gain insights on the application and develop further guidelines, 2) and, using a socio-technical theory as a theoretical lens to examine the topic of privacy, instead of the current technical and management ones.

References

1. Demchak, C.C. and Fenstermacher, K.D., 2009. Institutionalizing Behavior-Based Privacy. Administration & Society, 41(7), pp.783-814.
2. Magnani, L., 2009. CHAPTER SEVEN KNOWLEDGE AS A DUTY: THE ETHICAL SIGNIFICANCE OF THE INTEREST. Computing and Philosophy in Asia, p.108.
3. Russell, D., Russell, D., Gangemi, G.T. and Gangemi Sr, G.T., 1991. Computer security basics. " O'Reilly Media, Inc.".

16

4. Leszczyna, R., 2018. Cybersecurity and privacy in standards for smart grids–A comprehensive survey. Computer Standards & Interfaces, 56, pp.62-73.
5. Magnani, L., 2011. Structural and technology-mediated violence: Profiling and the urgent need of new tutelary technoknowledge. International Journal of Technoethics (IJT), 2(4), pp.1-19.
6. Robinson, N., Graux, H., Botterman, M. and Valeri, L., 2009. Review of the European data protection directive. Rand Europe.
7. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31
8. Cavoukian, A., 2009. Privacy by design.
9. Voigt, P. and Von dem Bussche, A., 2017. The EU General Data Protection Regulation (GDPR). A Practical Guide, 1st Ed., Cham: Springer International Publishing, 10(3152676), pp.10-5555.
10. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1
11. Lachaud, E., 2020. ISO/IEC 27701 Standard: Threats and Opportunities for GDPR Certification. Eur. Data Prot. L. Rev., 6, p.194.
12. Santos, C. and Pandit, H.J., 2023. How could the upcoming ePrivacy Regulation recognise enforceable privacy signals in the EU?.
13. European Commission, 'Proposal for an ePrivacy Regulation' <https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation>
14. Eltahawy, B. and Dang, D., 2022. Understanding Cyberprivacy: Context, Concept, and Issues.
15. Hitachi Systems Security Inc., 2019. Is Cybersecurity the Same as Data Privacy?, Available at: https://www.hitachi-systems-security.com/blog/is-cybersecurity-the-same-as-data-privacy/ (Accessed:5 May 2023)
16. Juliane Kokott and Christoph Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' (2013) 3.4 International Data Privacy Law. See also Articles 7 and 8 of the Charter of Fundamental Rights of the European Union where both rights have been recognized with separate provisions. The Charter is a binding and primary EU law.
17. Ralph O'Brien, '6 ways that U.S. and EU data privacy laws differ', (*Infosec*, 12 April 2022) <https://resources.infosecinstitute.com/topics/management-compliance-auditing/6-ways-that-u-s-and-eu-data-privacy-laws-differ/>
18. European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default', Version 2.0, Adopted on 20 October 2020.
19. Shakila-Bu-Pasha, 'The Controller's Role in Determining "high risk" and Data Protection Impact Assessment (DPIA) in Developing Digital Smart City' (July 2020) 29.3 Information & Communications Technology Law.
20. Greckhamer, T., Furnari, S., Fiss, P.C. and Aguilera, R.V., 2018. Studying configurations with qualitative comparative analysis: Best practices in strategy and organization research. Strategic Organization, 16(4), pp.482-495.
21. GDPR.eu (no date) GDPR Archives - GDPR.eu. Available at: https://gdpr.eu/tag/gdpr/.
22. International Organization for Standardization (2019) ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

23. Veiga, A. D., & Eloff, J. H., 2007. An information security governance framework. Information systems management, 24(4), pp. 361-372.
24. Nicho, M., 2018. A process model for implementing information systems security governance. Information & Computer Security, 26(1), pp. 10-38.

Resilient or Vulnerable Twin Transition? A Multi-System Perspective on the Intersection of Sustainability and the Electricity-Based Digitalized Energy System

Bahaa Eltahawy* Petra Berg Linda Turtola Mazaher Karimi

University of Vaasa, Wolffintie 34, 65200 Vaasa, Finland

*Corresponding author

Abstract. As the European Union advances its green transition goals, it recognizes the need for digitalizing energy systems to support its initiatives. The twin transition, combining sustainability and digitalization, has transformed energy systems into complex Socio-Technical Systems (STS) that are increasingly interconnected and data-driven. This transformation has enabled more advanced trajectories toward sustainable systems; however, it has also introduced new systemic and operational challenges by exposing the energy system to the cyber domain. In this work, the development of the Electricity-Based Digitalized Energy System (EBDES) and the convergence of information and operational technologies in the context of sustainability are investigated through a multi-system interactions perspective, to understand how this STS transition shapes both the resilience and the vulnerability of the emerging energy landscape. Here, a narrative review, together with a qualitative case study on the Nordic energy system incorporating data from three workshops and a panel session, are used to explore these dynamics. The study identifies interactions and specific tensions between digitalization and resilience, showing how the modern energy system expands through new interfaces, dependencies, and relationships. It also reveals a gap in current sustainability frameworks, which often overlook the role of cybersecurity and emerging technologies. Finally, the study highlights sector insights and points toward directions for future sustainability strategies and research. Altogether, addressing sustainability transitions requires confronting not only technological and policy challenges, but vulnerabilities introduced through digitalization, thereby reframing how resilience and sustainability are understood in future energy systems.

Keywords: Cybersecurity; Energy resilience; Multi-system interactions; Sustainability; Twin transition

1. Introduction

1.1. Overview

As the European Union focuses on sustainability and green transition goals (Fetting, 2020), it recognizes the role of digitalizing energy systems – particularly the electricity sector – as a cornerstone for achieving its objectives. The twin transition, combining sustainability and digitalization, has been reshaping energy systems, making them more interconnected and data-driven (Benedetti, Guarini, and Laureti, 2023). This transformation represents a unique shift in Socio-Technical Systems (STS), driven by the integration of advanced technologies and the convergence of Information Technology (IT) and Operational Technology (OT) within smart grid systems, all supported by policies and market incentives (Erlinghagen, and Markard, 2012). A key outcome of this shift is the transition from traditional energy systems to the more advanced and broader STS, the Electricity-Based Digitalized Energy System (EBDES), where electricity serves as the main energy source and digitalization acts as an enabler of sustainability (Negi, 2024). While this transition offers significant benefits, such as optimal resource utilization, increased efficiency, and support for other ongoing technological and social shifts, it also introduces new challenges and complexities. The convergence of IT and OT, in particular, has expanded the energy system's exposure to threats emerging from the cyber domain. For instance, reports showed that in 2022, 10.7% of cyberattacks targeted the energy sector (Ryu *et al.,* 2024), and in 2023, over 200 cyber incidents were recorded against the sector, with more than half affecting European countries (ENISA, 2024). These incidents point to the growing risks and challenges facing modern societies, especially as smart electricity systems become core services increasingly integrated with other critical infrastructure. This calls for closer examination of current and emerging shifts at the intersections of energy transitions and evolving cybersecurity risks, as they lead to new system configurations and introduce emerging sustainability challenges (Antal, Mattioli, and Rattle, 2020).

Despite the considerable attention – which we acknowledge – given to the technical benefits and challenges of digitalizing energy systems, the specific impact of cybersecurity on STS transitions within these systems remains underexplored in transitions and sustainability literature (Mäkitie *et al.,* 2023). As this topic sits at the intersection of sustainability, digitalization, and cybersecurity, this gap underscores the need for more interdisciplinary research to address these topics collectively and holistically. As Andersen *et al*. (2021) emphasize, broadening transition research to include multiple disciplines and system-level analyses is essential for understanding how new technologies contribute to sustainability transitions. While transition studies have traditionally focused on meso-level factors and their role in the diffusion of innovations (Geels, 2020), there is growing recognition that the complexity of sustainability transitions requires system-wide analysis across multiple levels (Köhler *et al.*, 2019). This need is especially clear in the case of EBDES, where sustainable and digital innovations are integrated within the smart grid, which itself operates as part of the cyber domain. As a result, systems that were once separate, such as grid control

systems, are now becoming tightly coupled with broader digital networks, expanding both technical capabilities and exposure to new types of cyber risks. These shifts illustrate that the twin transition is not only a technological change, but also one of evolving interdependencies. To better understand the consequences of such a transformation, there is a need for a multi-system perspective that captures how interactions between these interconnected systems shape emerging risks, trade-offs, and sustainability outcomes (Rosenbloom, 2020).

1.2. Motivation, Research Question, and Contributions

Motivated by the importance of the twin transition and the challenges facing the energy sector in its move towards EBDES, this work examines existing transition literature, frameworks, policies, practices, and qualitative findings to address the central question: "*How does the Electricity-Based Digitalized Energy System shape sustainability outcomes from a multi-system perspective?"* By adopting a multi-system perspective (Rosenbloom, 2020), we focus on the smart grid as an interface between EBDES and other systems and apply Breitschopf *et al.*'s (2023) framework to analyze EBDES, exploring its impact and identifying potential issues related to the twin transition.

The main contributions of this study are twofold: 1) Contributing to sustainability transitions by addressing the underexplored intersections of digitalization (*Mäkitie et al.*, 2023) and security (Sivonen and Kivimaa, 2024) in energy systems, specifically the impact of cybersecurity on STS transitions; and 2) Advancing research on multi-system interactions (Rosenbloom, 2020) (Breitschopf *et al.*, 2023) by analyzing and assessing the impacts of system interactions on the twin transition.

1.3. Organization

The rest of this work is organized as follows. Section 2 reviews the background on twin transitions, EBDES, and cybersecurity. Section 3 introduces the multi-system approach and the adopted framework. Section 4 outlines the methodology and describes the data collection procedure. Section 5 presents insights, framework application, and related analyses. Finally, Section 6 discusses the findings and provides concluding remarks.

2. Background

In this section, we conduct a preliminary narrative rapid review to build and support our view on the topic (Candyce *et al.*, 2021). We combine this by a progressive narrowing approach, as shown in Figure 1, to move from the main topic to narrower, more focused aspects that support our analysis and serve the objectives of the study.

Figure 1: The structure of the review

2.1. Twin Transition – General Sustainability and Digitalization Discussions

The growing importance of energy and digitalization has drawn increasing attention in transitions research (Andersen *et al.*, 2021) (Rosenbloom, 2020) (Mäkitie *et al.*, 2023), particularly regarding their systemic impacts on sustainability (Geels, 2020) and the potential outcomes they may introduce (Antal, Mattioli, and Rattle, 2020). Markard (2020) emphasizes a dynamic and global perspective within STS transitions, highlighting how technological innovations often emerge in small-scale, more specialized sectors before scaling up to influence and reshape dominant systems. As these innovations develop, they form clusters of complementary technologies that drive broader system transformations, as visualized in Figure 2. This dynamic process applies not only to energy and digitalization transitions, but also aligns with the broader framework of sustainability transitions.

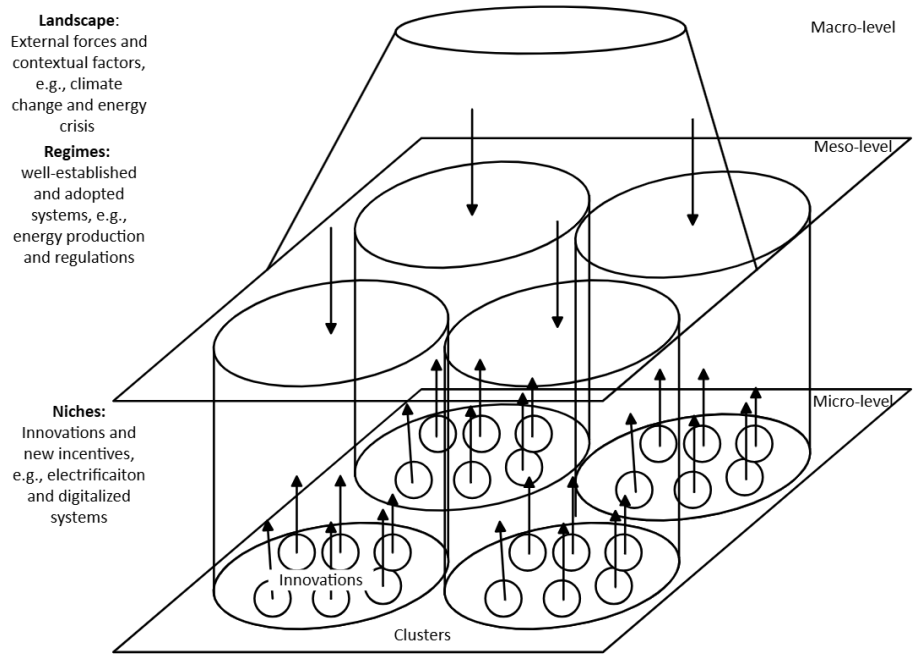


Figure 2: MLP framework [Adopted and edited from Geels and Schot (2007)]

The fundamental expectations of sustainability transitions are based on balancing social, environmental, and economic outcomes to ensure benefits for both current and

future societies (Grin, Rotmans, and Schot, 2010). However, complex issues such as the transition of energy systems and the adoption of new practices and habits, require more than mere technological solutions; they demand radical shifts toward new types of social norms and STS (Geels, 2020). To understand and address the dynamics of these required changes, the Multi-Level Perspective (MLP) framework, introduced first by Geels (2004), offers a comprehensive approach for analyzing how structural transformations in STS take place. As shown in Figure 2, Geels and Schot (2007) argue that changes in STS emerge from the interaction of processes across three pressing interconnected levels: landscape, regime, and niche. The regime, or meso-level, represents the dominant system, encompassing established structures, rules, practices, and systems (e.g., current energy production systems and infrastructure). The landscape, or macro-level, represents external forces or contextual factors that influence broader changes and trends in well-established systems (e.g., climate change and the need for sustainability). Finally, the niche, or micro-level, represents radical innovations that have the potential to transform the regime and address landscape pressures (e.g., prototypes and experimental projects).

An STS, also described as the co-evolution of society and technology, encompasses societal functions, such as urban electricity production and distribution. It is realized through a combination of elements including technology, regulations, markets, infrastructure, supply networks, and user experience (Geels, 2004; Sarrica *et al.*, 2018). The regime, a central part of the STS, is challenged by pressures from the landscape and niche innovations addressing them. Changes within STS are rarely initiated by a single group of actors or external forces; rather, they require significant pressure and interactions across all three levels. These dynamics can lead to shifts ranging from minor adjustments to more substantial transformations or even a complete transition (Geels, 2010).

Given these dynamics, energy transitions can be viewed as transformations across multiple levels, involving shifts from one STS to another. These transitions often take place within the context of the ongoing move toward renewable energy, with multiple STS evolving simultaneously, either independently or in interaction. Energy-related STS generally follow established trajectories due to their deep integration with technological advancements and institutional structures (Verbong and Geels, 2007) (Geels, 2010). As a result,, transitions such as the shift toward EBDES can have far-arching implications for societal structures. Additionally, since production, distribution, and consumption are interdependent, the current shift integrating all EBDES actors in cyberspace carries significant socio-cultural implications (Georgiadou, Michalitsi-Psarrou, and Askounis, 2023).

2.2. Information Technology/Operational Technology Integration

Previously, IT and OT had long existed as separate entities, each focusing on specific criteria and distinct goals (Hahn, 2016) (Negi, 2024). On the one hand, IT systems concern data and the flow of information between digital assets, ensuring efficient processing and data handling, secure storage, and seamless communication between

users, applications, and networks. These systems come in many forms, from simple consumer systems such as web servers used for accessing information and webpages, to organizational and commercial tools, such as Customer Resource Management (CRM) and Enterprise Resource Planning (ERP) systems. They also include advanced systems, such as Machine Learning, Deep Learning, and Artificial Intelligence (AI), which make use of data, extract information and useful patterns, analyze intricate scenarios, simplify automation, and support decision making processes. On the other hand, OT systems concern the service sector, industrial systems, and critical infrastructure, which have different demands and come in completely different sizes and forms. Unlike IT, OT is centered around the monitoring, control, and automation of physical processes. OT includes a wide range of technologies, from simple Programmable Logic Controllers (PLCs) used in manufacturing and utility operations to complex Supervisory Control and Data Acquisition (SCADA) systems essential for managing large-scale industrial processes. OT systems are essential in general sectors such as energy, water management, transportation, and healthcare, where real-time control, reliability, and safety are critical. That is the reason why in contrast to IT systems, which prioritize the confidentiality and integrity of data, OT focuses on ensuring the availability of services and data when needed.

With the increased demands, the need for more optimized systems, awareness of environmental impacts, and the transition to sustainability and more sustainable systems, OT has increased the adoption of digital technologies and is becoming more integrated with IT (Berardi *et al.*, 2023). This, in turn, has led to a complete transformation of the OT sector, bringing greater control and device management, availability, efficiency, improved scalability, enhanced security, better data analytics, and increased operability. Figure 3 shows the distinction between IT and OT systems, and the benefits resulting from their convergence.

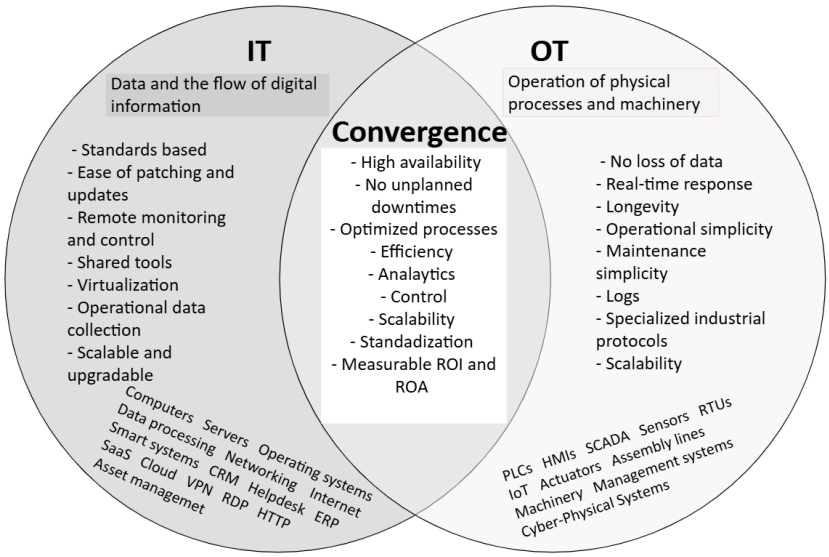


Figure 3: IT, OT, and their convergence [Adopted and edited from Rinaldi (2020)]

2.3. The Transition Towards Electricity Based Digitalized Energy Systems (EBDES)

Previously, utility energy systems relied on fossil fuels as the main energy source, consisted of central generation and distribution facilities, and operated in a unidirectional manner to deliver energy (electricity and thermal) to end-consumers with minimal data exchange and limited optimization functionalities (Fang *et al.*, 2012). However, during the mid to late 20th century, utilities developed and incorporated early grid interconnections, automation, digital control systems, and the initial integration of Renewable Energy Sources (RES) (Amin, and Wollenberg, 2005). These developments accelerated in the 21st century, driven by increased demand, rapid industrialization, the growth of industrial automation systems, advancements in engineering, the interplay between IT and OT, and increasing awareness of environmental concerns. Today, energy systems are diverse and flexible, ranging from small-scale microgrids to large interconnected national and regional networks. These systems are increasingly decentralized and smart, prioritizing adaptability, responsiveness, and efficiency while aligning with sustainability and green transition goals. Figure 4 shows a schematic comparison of utility energy systems before and now.

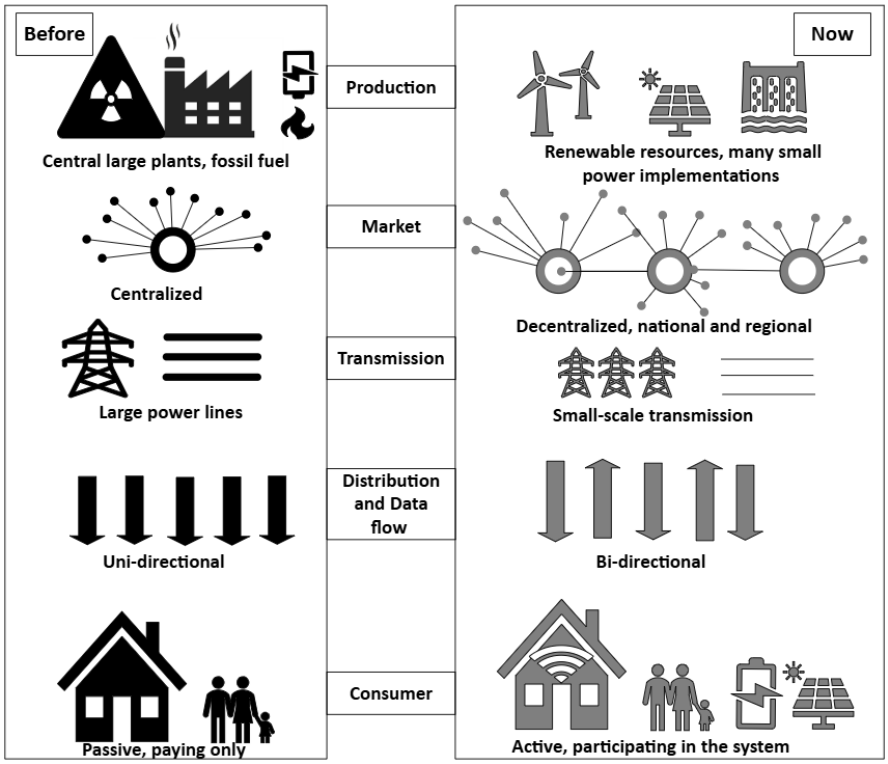


Figure 4: Schematic comparison of utility energy systems before and now, [adopted and modified from Stelmashchuk (2023)]

Building on this transformation, the Electricity-Based Digitalized Energy System (EBDES) emerged as a transformative approach to energy networks, promoted specifically through the convergence of information and operational technologies (Negi, 2024). EBDES places electricity across all energy interfaces and leverages advanced digital technologies to optimize energy production, distribution, and consumption. Unlike traditional systems, it employs decentralized, dynamic, and flexible infrastructure to address modern demands and challenges. Central to EBDES is the smart grid, developed to provide real-time monitoring and two-way communication between producers and consumers, enhancing grid reliability, facilitating the integration of renewable energy sources, and enabling advanced functionalities through data-driven analytics. Smart grids rely on intelligent automation, replacing conventional control mechanisms while adapting to variations in supply and demand using data from sensors and meters (Gungor, Lu, and Gerhard, 2010). The integration of smart meters and Advanced Metering Infrastructure (AMI) supports this by enabling demand response and dynamic pricing (Fang et al., 2012). Additionally, technologies and tools such as real-time analytics, Artificial Intelligence (AI), and the Internet of Things (IoT) contribute to forecasting demands, adjusting operations, and maintaining grid stability. These capabilities enable EBDES to seamlessly integrate Distributed Energy Resources (DERs), supporting resilience and sustainability. Through such intelligent resource coordination, EBDES enhances efficiency, reduces waste, minimizes environmental impacts, and ensures reliable and cost-effective energy supply.

2.4. Cybersecurity

As the convergence of IT and OT systems advances and the energy sector transitions toward digitalization, it faces numerous challenges, including cyber-attacks and the need for effective protection schemes (Pirta-Dreimane *et al.*, 2024). Cybersecurity plays a critical role in this context, as the rapid expansion of connected energy sources and devices, along with increased connectivity and automation, widens the attack surface and increases potential cybersecurity risks (Chobanov & Doychev, 2022). Cybersecurity is defined as "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights" (Craigen *et al.*, 2014). Cybersecurity aims at protecting assets and data from intentional and accidental events that may cause harm or disruption. Cyber-attacks, including social manipulation, espionage, and sabotage, can harm the energy sector and disrupt critical societal functions (Martti, 2022). These attacks come in various forms, such as energy theft, false data injection, sensitive data leaks, and large-scale disruptions (Georgiadou, Michalitsi-Psarrou, and Askounis, 2023) (Palleti *et al.*, 2021), affecting a wide range of entities, from individual smart meters to entire national energy infrastructures (Keleba, Tabona, and Maupong, 2022). Such attacks can have varying consequences depending on their scale, methods, and existing security measures. These can range from simple manipulation of energy consumption through compromised smart meters

(Sun *et al.,* 2020) to more sophisticated regional blackouts that disrupt essential services and lead to human and economic losses (Sun, Hahn, and Liu, 2018). Moreover, due to the interconnected nature of critical infrastructure, cyber-attacks on the energy system can trigger cascading effects that escalate risks and extend disruptions across other systems (Palleti *et al.*, 2021).

Given these factors, enhancing the security and – more specifically – the cyber resilience of energy systems is critically important (Milevskyi *et al.*, 2023). This includes the ability to withstand, adapt to, and recover rapidly from incidents and attacks, while ensuring the continuity of critical infrastructure operations (Sun, Hahn, and Liu, 2018). Achieving this, however, involves not only strengthening defense mechanisms and developing flexible and adaptive security measures, but also requires proactive risk management and collaboration across various sectors. Furthermore, cybersecurity, the energy system, and the entire transition, should be considered holistically (Sivonen and Kivimaa, 2024) to identify the most effective defense approaches.

3. Introduction to multi-system interactions

Previous studies have explored interconnected STS and recognized smart energy systems as an emerging domain within sustainability transitions, positioned at the intersection of electricity, OT, and IT (Breitschopf *et al.*, 2023). To examine how cybersecurity threats from the digitalization of energy systems could impact the sustainability transition, we follow Rosenbloom's (2020) recommendations for adopting a multi-system perspective in our analysis, as it "draws attention to the present functional and structural couplings that link systems of interest; emerging sites of interaction that could bring systems further into contact; along with the patterns marking system interactions and their implications for sustainability transitions". For this analysis, we apply the multi-system interactions framework introduced by Breitschopf *et al.*, (2023).

Breitschopf *et al.*, (2023) propose a framework for identifying interactions between STS and their potential impacts on transitions. The framework is centered around four key pillars: 1) Identifying **interfaces** between systems, 2) Defining the interaction **relationships** between systems, 3) Assessing changes in interaction **intensities** over time, and 4) Evaluating the potential **impacts** on systems and their components. According to the authors, STS interactions occur only when these dimensions are fully met. First, systems interact only when they have interfaces in between, e.g., a shared element. Second, systems interact when they establish some form of connection or exchange between each other. Third, for systems to have a significant impact, they must reach a certain level of interaction intensity. Finally, these interactions driven by interfaces, relationships, and intensity, impact and shape STS, driving transitions and transformations. In Table 1, a detailed overview of these dimensions and their descriptions is provided.

Breitschopf *et al.*, (2023) demonstrated the relevance and applicability of their conceptual framework by using it to analyze case studies such as the interactions

between heating and electricity systems, as well as the automotive and Information and Communication Technology (ICT) systems. These applications provided deeper insights into system transitions and their dynamics. The framework has also been applied in studies focusing on sustainable energy systems, net-zero energy transitions, and related fields. The framework could similarly be used here as it offers a useful lens for examining EBDES as an innovative system shaping STS and influencing processes.

Table 1: Dimensions of STS multi-system interactions [adapted from Breitschopf *et al.*, (2023)]

Dimension	Type	Description
Interface	Actors	Individuals, Organizations, or a group of actors sharing common characteristics or functions at the macro-level
	Institutions	Rules, culture, policies
	Infrastructure	Physical, financial, knowledge
	Technology	Technology or technical parts
	Knowledge	Know-how, expertise, skills, knowledge, experience, information
	Natural resources	Resources such as water, fossil fuels, etc.
	Goods and services	Input or output of an industry and belonging systems and services
Relationship	Competing – two-way interaction	Similar systems characterized by scarcity, opposing interests or needs
	Cooperative – Two-way interaction	Systems affecting each other with non-rivalries interfaces
	Integrative – One-way interaction	Systems depending on each other's outputs
	Spill-over – One-way interaction	Systems affected by changes in other systems unintendedly
	Neutral – No direction	Co-existence without any impact
Intensity	Increasing the use of interface	Usage and sharing of an interface in terms of volume and frequency
	Growing the number of interfaces	Interactions resulting in changes in number of interfaces and relationship
	Involvement of system's components	Number of components of levels of the system possibly affected over the time
Impact	Within systems	Changes of a components, elements, and the emergence of new structures
	Between Systems	Changes of interfaces, relationships, and intensities
	Transformative	Causing transformations, replacements, dealignments, and reconfigurations within systems

Partial	Causing merging, emerging, disappearing, or coexisting changes between systems
Direction	Contributing or hindering
Speed	No progress, slowing down, or accelerating

4. Methodology and Sources

4.1. The Nordic EBDES – Case Study

To deepen our understanding of the transition toward EBDES, current challenges, and associated system interactions, we followed Rosenbloom's (2020) recommendations for conducing multi-system perspective analysis. Accordingly, we employed a multidisciplinary approach, integrating the research expertise of four scholars across marketing and business, industrial economics, information systems, and electrical engineering domains. This collaborative effort was established through the common research project, REDISET – Resilient Digital Sustainable Energy Transition – to address the need for better understanding of the security aspects of a fully digitalized future Nordic electricity system. Nordic countries have set ambitious national targets for transitioning to sustainable energy, and are already global pioneers in green and renewable energy solutions. However, unique challenges persist and are widely recognized. To address these, Nordic governments and research institutions continuously collaborate with public and private actors to accelerate the transition by supporting numerous innovative pilot projects (Nordic Energy Research, 2022), including this one.

4.2. Data Description

This work incorporates two research methods: desktop research in the form of rapid review, and qualitative research through workshops and a panel session. The rapid review method (Candyce *et al.*, 2021) was used to gather information on current trends and challenges in sustainability and related topics in the Nordic energy sector. Findings from the review shaped the case study and guided the design of semi-structured workshops (Chen, and Yu, 2024) (Thoring, Mueller, and Badke-Schaub, 2020) and a storytelling panel session, where experts discussed and shared their perspectives, providing additional insights. Figure 5 shows a schematic diagram of the research methodology employed. Table 2 presents a description of workshops and participants.

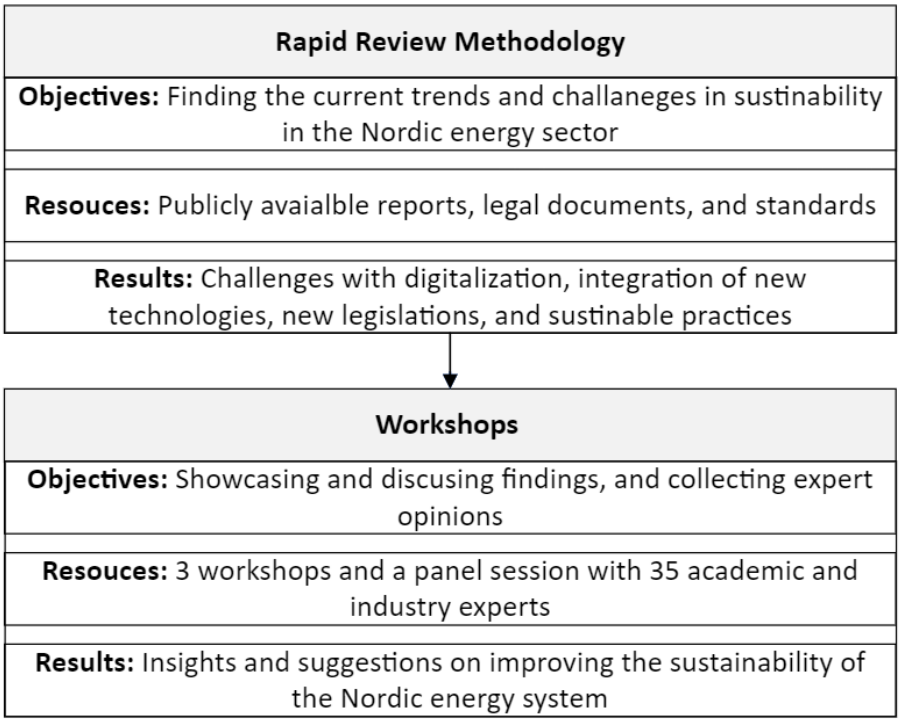


Figure 5: Methodology and data description

Table 2: Workshops and panel session descriptions

Attribute	Description
Dates	October 9, 2023; March 6, 2024; March 8, 2024; March 12, 2024 (Panel session)
Type of activity	3 Workshops at University of Vaasa, Finland; KTH Royal Institute of Technology, Sweden; and Statnett, Norway. 1 Panel session at Vaasa City Hall, Finland
Countries involved	Sweden, Finland, and Norway
Research institutions involved	KTH, Sweden; University of Vaasa, Finland; FFI, Norway; and NTNU, Norway
Outer organizations involved	ABB, Wartsila, Fortum, Statnett, Hitachi Energy, Huld, Bird & Bird, and Aalto University
Total number of participants, present and online	35
Academic participants	12
Industrial participants	23

5. Analysis and Insights

5.1. Part 1 – Framework Application

While smart grids are not yet fully deployed, they exemplify the growing coupling and interactions between electricity systems and the ICT sector. Currently, there is growing shift toward broader smart grid implementations, driven by the twin transition and EBDES initiatives represented by the European Green Deal and the Digital Europe Programme (DIGITAL) directions (Fetting, 2020) (European Commission, 2021). This marks a distinct shift in energy STS, integrating advanced technologies, market incentives, regulatory frameworks, and evolving societal behaviors and practices. Here, to better understand EBDES, we apply Breitschopf *et al.*'s (2023) multi-system interactions framework as a lens for analyzing the growing interconnection between electricity, ICT, and sustainability-related systems. For this, we focus on smart grids as a central interface of EBDES. Table 1 and the case study material (see Table 2) form the foundation of our analysis.

5.1.1. Interfaces: Cross-System Integration

The interfaces outlined by Breitschopf et al. reveal the depth of EBDES integration across multiple systems. For instance:

- **Actors**: the actors' interface emphasizes this integration through the interaction between diverse individual and collective agents, including end-users such as consumers, producers, and prosumers, alongside energy sector operators ranging from data scientists and advisors to workers and grid operators, as well as organizations such as energy utilities, telecommunications providers, ICT firms, and central regulatory organizations.
- **Institutions**: similarly, this reflects the growing entanglement of rules, norms and policies. Institutional interfaces of EBDES include regulatory frameworks, market rules, digital governance policies, sustainability authorities, and broader socio-cultural norms that societal behavior.
- **Infrastructure**: this demonstrates the assets and foundations enabling system convergence. Infrastructure includes physical components such as electricity grids, data networks, smart meters, and storage systems; financial channels that support energy-ICT investments; and knowledge institutions that bridge distinct domains through driving innovations, training, and research.
- **Technologies**: in particular, smart meters, digital platforms, and intelligent grid systems form the technological interface, fostering integration and blurring the boundaries between EBDES, ICT and sustainability systems.
- **Knowledge**: EBDES is critically driven by knowledge interfaces, where expertise in systems thinking, digital tools, energy markets, and sustainability transitions form a shared cognitive infrastructure.

- **Resources**: resources extend the interface scope, with materials used in battery and storage manufacturing, ICT components, and electricity generation liking systems and creating environmental and geopolitical dependencies.
- **Goods and services**: this reflects the exchange of value across systems. The interface includes smart grid services, cloud-based platforms, and integrated ICT services exchanged between sectors and systems.

5.1.2. Relationships: Complex Interdependencies

EBDES has dynamic relationships with ICT and sustainability systems, characterized by as a complex mix of interdependencies and systemic imbalances, including:
- **Structural coupling**: a mutual-reliance and foundational relationship between EBDES and ICT systems, where each shapes and contributes to the evolution of the other. Smart grids exemplify this through two-way interactions that integrate ICT capabilities within energy systems.
- **Cooperative relationships**: this is evident where EBDES, ICT, and sustainability systems align toward shared sustainability objectives driven by strategies and meta-level policies. However, such alignment often brings underlying tensions related to implementation and differing sectoral logics.
- **Functional coupling**: this reflects a one-way form of inter-system influences. For instance, ICT and digital tools often support energy system operations and ongoing transformations by bringing advanced capabilities, such as AI-enabled optimization, without being significantly transformed themselves.
- **Spill-over effects**: Innovations and triggers from ICT systems can affect energy systems configurations and sustainability settings, e.g., cybersecurity incidents and strategies. This can lead to uneven dependencies and unintended restructuring.
- **Neutral relationships**: these persist in legacy infrastructure and uncoordinated policy areas, where integration remains limited.

5.1.3. Intensity: Deeper Interconnections

EBDES interfaces engage in different types of interactions, with intensity reflecting a shift toward more structured and interdependent relationships, including:
- **Greater use of interfaces**: particularly, the growing integration of digital infrastructures and ICT systems within energy systems, along with the increased deployment of smart devices, sensors, and digital platforms, highlights a stronger reliance on shared operational mechanisms.
- **Growth of interfaces and relationships**: the involvement of broader range of actors, technologies, and institutions linking electricity, ICT, and sustainability systems reflects the growth of cross-system connections across cognitive, cultural, and behavioral domains.
- **Involvement of system components**: this extends beyond traditional organizational boundaries, with increasing participation of distributed actors and flexible

infrastructures, where deeper integration of technical, institutional, and actor-based elements drives broader systemic convergence and transformation.

5.1.4. Impacts: Reconfiguring Systems and Redefining Boundaries

The cumulative outcome of such interactions is the emergence of multi-dimensional transformations and more advanced STS. Impacts include:
- **Within-systems impacts**: these include the transformation of electricity systems into data-driven, decentralized networks, along with ICT systems adapted to energy-specific applications.
- **Inter-system impacts**: these reflect system reconfigurations driven by shifts in institutional directions, changing settings, and development trajectories shaped by growing technological convergence.
- **Transformative impacts**: these include changes in system components and dimensions, such as the digitalization of grid operations and the emergence of new institutional logics, that lead to fundamental restructuring. As interfaces between systems become more interdependent, system boundaries blur and transformation extends across systems.

5.1.5. Remarks: Shifting Boundaries and Transition Dynamics

In addition to the current interactions, EBDES also contributes to broader shifts in the boundaries between electricity and ICT systems. As electricity firms continue to develop their own digital capabilities, they may end up resembling ICT firms in their structures, services, and business models. This includes incorporating other stages of the value chain than traditional roles (e.g., generation, transmission, and distribution), expanding into new service areas and sectors, and aligning more closely with digital platforms. The adoption of service-oriented practices within the electricity sector is reshaping how services are delivered and how firms operate. These shifts are not only influencing developments, but also redefining roles, structures, and underlying logics across sectors. Looking ahead, existing regulatory frameworks and governance approaches will need to adapt to these emerging cross-sectoral and hybrid changes.

5.2. Part 2 – Empirical Insights

This part covers findings discussed in workshops and the panel session, emphasizing sustainability, energy, and cybersecurity strategies in the Nordic context.

5.2.1. Sustainability expectations of digitalizing energy systems in the Nordics on a policy level

Finland's national climate and energy strategy (Huttunen *et al.,* 2022) outlines expectations for energy systems, with digital technologies playing a key role in optimizing efficiency to achieve carbon neutrality targets. Efforts focus on flexible consumption and production, and on encouraging active participation in the electricity market through smart solutions. Finland is also closely involved in international cooperation through the Clean Energy Ministerial (CEM), a forum where G20 and Nordic countries share approaches to accelerate the global clean energy transition. Finland participates in CEM initiatives on electric vehicles, smart grids, bioenergy, carbon capture, hydrogen, renewable energy, efficiency, and sustainable development. In heating, fossil fuels are expected to be replaced by electricity-based smart solutions, with consumers also acting as producers to increase flexibility and decentralization .

Sweden's draft integrated national energy and climate plan (2019) highlights its forum for smart grids. Sweden participates in EU-level groups focusing on Ocean Energy, Smart Solutions for Consumers, Smart Cities, Energy Systems, Energy Efficiency, Batteries, Renewable Fuels, and Carbon Capture Utilization and Storage. The move toward decentralized systems and smart networks involves more, smaller actors in the energy market, increasing reliance on information technology. As a result, future energy supply could become more vulnerable to IT-related threats. Sweden has also dedicated research areas for smart energy and smart grids.

Norway's climate action plan for 2021–2030 (2021) emphasizes the role of municipalities in spatial planning, which affects consumption, energy use, emissions, and carbon removal. Biogas is promoted for cutting emissions and reducing waste. Technological development is seen as vital for climate targets. Energy integration is highlighted as key for the green transition, covering storage, smart grids, demand response, digitalization, hydrogen, and renewable heat. Energy efficiency is prioritized across all sectors, with smart meters supporting demand response and enabling solutions such as smart charging. Grid development is viewed as essential for electrification. Table 3 shows a comparison of strategic goals and sustainability expectations in the energy sector as reflected in cybersecurity, climate, and energy strategies of Finland, Sweden, and Norway.

Table 3. Comparison of strategic goals and sustainability expectations of energy sector in cybersecurity strategies and energy strategies of the Nordics.

Strategy	Country and Description
Climate and Energy	**Finland**: 1. Carbon neutrality by 2035 2. Reduction of Greenhouse Emissions and carbon sinks 3. Promoting renewable energy 4. Hydrogen and electro fuels 5. Promoting energy efficiency

	6. Energy delivery reliability and security of supply 7. Use of nuclear energy 8. Development of energy market 9. Research and innovation, 10. Taxation 11. Strengthening climate change adaption 12. Influence within the EU **Sweden**: 1. Decarbonization 2. Renewable energy 3. Energy efficiency 4. Energy security 5. Internal energy market 6. Research, innovation and competitiveness **Norway**: 1. Cutting green-house gas emissions 2. Reducing ETS and non-ETS emissions 3. Green tax shift with increased carbon pricing. 4. Sector specific measures (transport, buildings, agriculture) 5. Support for Innovation and Green Growth 6. Alignment with EU Climate Policies Sustainable Investments
Cybersecurity	**Finland**: 1. Advancing international cooperation. 2. Improving coordination of cybersecurity management. 3. Developing cybersecurity competence **Sweden**: 1. Securing a systematic and comprehensive approach in cybersecurity efforts 2. Enhancing network, product, and system security 3. Enhancing capability to prevent, detect and manage cyberattacks and other IT incidents 4. Increasing the possibility of preventing and combating cybercrime 5. Increasing knowledge and promoting expertise 6. Enhancing international cooperation **Norway**: 1. Norwegian companies digitalize in a secure and trustworthy manner, and are able to protect themselves against cyber incidents 2. Critical societal functions are supported by a robust and reliable digital infrastructure 3. Improved cybersecurity competence aligned with the societal needs 4. Society has improved ability to detect and handle cyber attacks Authorities have strengthened their ability to prevent and combat cyber crime

5.2.2. Legislative differences of the Nordics and the EU

Finland, Sweden, and Norway share geographic and institutional similarities as EEA members, and all three are part of the North Atlantic Treaty Organization (NATO) (Norway, 2014) (Nato, 2024). Legislatively, Finland and Sweden, as EU members, must comply with EU law (European Commission, 2022). Norway, outside the EU, maintains alignment mainly through the EEA, which forms the framework for its cooperation with the Union.

In terms of cybersecurity, the EU and NATO cooperate on cyber threats and protection of critical infrastructure (Nato, 2025). National strategies, however, differ from NATO approaches (Štitilis, Pakutinskas, and Malinauskaitė, 2017). The EU combines sustainability goals, such as smart meter deployment, with cybersecurity priorities (European Commission, 2019) (European Commission, 2024a). Yet the links between cybersecurity and digitalizing energy systems are less visible in Nordic climate and energy strategies. While Nordic cybersecurity strategies stress cooperation, education, and infrastructure protection, it should be noted that they are older than the EU's current cybersecurity strategy, and thus require careful consideration to address current issues and updating.

The EU announced its new cybersecurity strategy in 2020, followed by legislative reforms. In January 2023, the Revised Network and Information Security Directive (NIS2) and the Critical Entities Resilience Directive (CER) entered into force. NIS2 sets measures for a high common level of cybersecurity, while CER identifies essential services across eleven sectors (European Commission 2023) (European Commission 2024b). In 2024, the Cyber Resilience Act (CRA) was adopted to supplement existing rules, especially NIS2 (European Commission, 2025).

5.2.3. Cybersecurity strategies

Finland's Cybersecurity Strategy (2019) focuses on international cooperation, improved coordination of management and preparedness, and enhanced expertise. It highlights the interdependencies of digital environments, requiring integrated cybersecurity structures. Critical service continuity is prioritized, and education and research are emphasized for long-term capabilities (Finland, 2019).

Sweden's Cybersecurity Strategy (2017) recognizes the energy sector as critical infrastructure. A systematic approach is promoted to strengthen awareness and risk management across authorities, municipalities, companies, and organizations. This involves collaboration, information sharing, and stricter measures for industrial control systems such as PLC and SCADA. Priorities include improving defenses against cyberattacks, strengthening law enforcement capacity, preventing cybercrime, and building knowledge through education, research, and training. International cooperation is also central (Sweden, 2017).

Norway's Cybersecurity Strategy (2019) stresses international, public-private, and civilian-military cooperation. With growing digitalization, robust cybersecurity is seen as essential for protecting ICT systems and digital services in the public sector. Priority

areas include preventive cybersecurity, resilience in critical societal functions, competence development, attack detection and response, and combating cybercrime (Norway, 2019).

5.2.4. National climate and energy strategies on cybersecurity

National climate and energy strategies address cybersecurity differently. Finland's strategy explicitly mentions the cybersecurity of energy systems as part of energy delivery reliability and security of supply, with initiatives including joint ventures, projects, and possible legislation. Sweden's draft integrated national energy and climate plan (Sweden, 2019) does not mention cybersecurity directly but acknowledges risks of IT-related threats to energy supply. Finally, Norway's climate action plan 2021–2030 (2021) recognizes digitalization as central to energy integration and demand response but does not address cybersecurity explicitly.

5.2.5. Addressing cyber safety of critical energy infrastructure in the Nordics

In Finland and Sweden, the security of critical infrastructure was incorporated into national law through the CER and NIS2 Directives in October 2024. Norway has adopted the original NIS Directive, though it is unclear when NIS2 will be implemented (Norway, 2021). The EU's CER Directive, adopted in 2022, replaced the earlier European Critical Infrastructure Directive. The shift from Critical Infrastructure to Critical Entity reflects a move from sector-level to operator-level resilience (Pursiainen & Kytömaa, 2023). By July 2026, member states must identify essential entities in each sector and require them to strengthen resilience (European Commission, 2023).

In Finland, CER implementation may create a new "Act for the Protection of Critical Infrastructure and Improvement of Disruptive Resilience in Society," with ministries responsible for identifying critical actors. Supervision would be organized by sectoral authorities (Huttunen *et al.,* 2022). In Sweden, the Ministry of Defense is preparing CER and NIS2 implementation in parallel, with the MSB (Swedish Civil Contingencies Agency) as coordinator and supervisory authority. The CER Directive will also expand sanctioning powers of supervisory bodies.

Finally, Norway's Security Act of 2019 (Norway, 2018) already gives the National Security Authority (NSM) supervisory responsibility over critical information and infrastructure, covering both state and private actors through a risk-based approach. Unlike the CER Directive, Norway's system is decentralized, with ministries responsible for their own sectors. The Directorate for Civil Protection (DSB) maintains national risk assessments. Norway does not directly implement CER since it is outside the EU.

6. Discussion

The security perspective of Electricity-based Digitalized Energy Systems is central to understanding how the twin transition will shape sustainability outcomes. Digitalization does not simply add features to existing systems, it creates new interfaces – technology, infrastructure, institutions, actors, knowledge, and resources – whose growing intensity reconfigures both opportunities and risks. Smart grids and EBDES enable flexibility, two-way energy flows, and advanced features, but they also increase dependencies and expand attack surfaces across the electricity–ICT interface. The multi-system interactions framework, adopted from Breitschopf, helped make those dynamics visible, translating scattered policy material and workshop insights into a tractable set of systemic tensions that link technical design to governance choices and future strategies.

Applying the framework to the Nordic case, the pattern becomes clear. Stronger coupling between electricity and ICT accelerates the possibilities of electrification through demand response, smart charging, and distributed resources. Finland's explicit linking of cybersecurity to energy delivery reliability illustrates clearly this enabling function. At the same time, the same coupling comes with own vulnerabilities. Decentralization brings many small actors into the market, supports sustainable development, and increases innovation. However, it also increases heterogeneity in cyber-capability in a way that regulators and supervisors struggle to accommodate. Sweden's recognition of IT-related risks in the energy sector without explicit cyber measures, and Norway's emphasis on digitalization without a clear cyber thread in its climate plan, expose institutional gaps the framework and insights highlight.

This mismatch between energy and cyber planning creates practical tensions. Intensified interfaces increase spill-over risks: a cyber incident in a control node can cascade into service failures with lasting sustainability impacts, including increased emissions, economic losses, and compromised social services. The regulatory shift from sector-level critical infrastructure to operator-level critical entities reframes responsibility for resilience but raises implementation challenges for smaller actors with limited resources. The new regulations, such as NIS2, also impose stringent constraints that may render compliance difficult for these smaller entities. Security measures can further conflict with social and environmental goals. Overly centralized or non-transparent controls risk undermining privacy, access, and procedural fairness, which are core concerns of energy justice and future energy systems.

One of the most difficult challenges lies in enhancing the cyber-capabilities of the future workforce, not least because of the merging of IT and OT. The determination of required control measures for securing smart systems in societal functions with highly heterogeneous consumer segments is not a simple task. Safety is directly linked to the disparities in awareness and knowledge at both the individual and collective level. The workshops repeatedly identified these gaps as central. Education, training, and career channels remain uneven, leaving practical detection, response, and secure operation vulnerable despite ongoing efforts and political commitments.

The framework proved useful in clarifying scale effects and showing where trade-offs appear. It does not provide probabilities or cost estimates, but it is a powerful tool

for tracing who stands at critical intersections and how disturbances propagate. That strength points directly to what governance should – and must – do: integrate cyber objectives into energy planning, design national implementations around NIS2 and CER to support resilient electrification rather than impede it, and rethink obligations so smaller actors can participate without being overly burdened by compliance costs. Mandating resilience must be combined with the need for capacity building – funding, technical assistance, and balanced regulations – so that the transition does not become exclusive.

Human capability and supply-chain dependencies also emerged as foundational vulnerabilities. Closing the cyber-capability gap requires sustained investment in multidisciplinary education, cross-sector training, and joint ventures that bring IT and OT practitioners together. Procurement and supply-chain rules that demand transparency and resilience from ICT and battery component vendors are equally important, as material dependencies can bypass national safeguards. Technical measures that promote resilience-by-design, such as segmentation, redundancy, and islanding, reduce the chance that a single cyber incident escalates into a system-wide blackout.

Finally, the analysis also reinforces that security and sustainability are co-constructed outcomes. Resilience measures that overlook social and environmental consequences can reshape outcomes in ways that weaken social acceptance and long-term sustainability. Examples such as forced shutdowns of production and tightened central controls that restrict civil liberties, are plausible outcomes that would affect decarbonization trajectories if left unaddressed or loosely managed. Treating resilience and justice as co-equal concerns is therefore a condition for a durable sustainable transition, not an optional add-on.

7. Conclusion, Contributions, Limitations, and Future Work

This paper addressed the digitalization of electricity systems and showed how central it is to Nordic sustainability goals and the broader electricity-based energy transition. The transition, however, reconfigures system interfaces and intensifies dependencies between electricity and ICT systems, which results in various gains as well as new and increased vulnerabilities. National strategies vary in how explicitly they address such challenges and cybersecurity in energy planning, which need alignment with recent EU and related sustainability reforms. To secure sustainability and electrification benefits, governance must require integrated cyber-energy planning, balanced implementations of NIS2 and CER directives, and systemic capacity building for workforce and supervisory authorities.

This work contributes in four main ways. First, it provides a systemic integration of sustainability, digitalization, energy transition, and cybersecurity in the Nordic context. Second, it applies Breitschopf's framework to EBDES to better understand the ongoing transition. Third, it offers an empirical synthesis of Finland, Sweden, and Norway's energy, sustainability, and cybersecurity strategies. Finally, it identifies system tensions and links sustainability with energy justice.

On limitations, this study draws on a narrative review, three workshops, and a panel session; it is qualitative and context-specific to the Nordic case, with findings reflecting the perspectives of participating experts and policy documents available at the time of analysis. Combining a structured framework with document analysis and practitioner engagement proved productive, but the framework has limits: it is primarily qualitative and structural, highlighting where to focus and what to prioritize, while requiring complementarity with quantitative risk modelling, scenario analysis, and actor-centered institutional work to estimate cascade probabilities, compliance burdens, and time-sequenced impacts.

Finally, future work should quantify how cyber incidents propagate across multi-system interfaces and their overall effect on sustainability indicators. Empirical work is needed to address the needs of small actors and the regulatory adjustments required for their participation. Research into justice-aware security measures is required to reconcile emergency security needs with privacy and access rights. Long-term studies of workforce development and multidisciplinary training will also be essential to the resilient operation of EBDES.

Acknowledgements

1. A shorter version of this paper was accepted and presented at the IST2024 conference in Oslo, Norway, June 2024.
2. This work is part of REDISET project, which examines future energy systems and expected threat scenarios. The project is funded by Business Finland, NordGrid Energy Research, and the Swedish Energy Agency, with partners from the University of Vaasa, Finland; KTH Royal Institute of Technology, Sweden; the Norwegian Defense Research Establishment (FFI); and the Norwegian SmartGrid Center, Norway.

Declaration of generative AI and AI-assisted technologies in the writing process

During the preparation of this work the author(s) used Open AI's ChatGPT in order to improve the language, readability, and flow. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the publication.

References

[1] Amin, S. Massoud, and Bruce F. Wollenberg. "Toward a smart grid: power delivery for the 21st century." *IEEE power and energy magazine* 3.5 (2005): 34-41.
[2] Andersen, Allan Dahl, et al. "On digitalization and sustainability transitions." Environmental Innovation and Societal Transitions 41 (2021): 96-98.
[3] Antal, Miklós, Giulio Mattioli, and Imogen Rattle. "Let's focus more on negative trends: A comment on the transitions research agenda." Environmental innovation and societal transitions 34 (2020): 359-362.
[4] Benedetti, Ilaria, Giulio Guarini, and Tiziana Laureti. "Digitalization in Europe: A potential driver of energy efficiency for the twin transition policy strategy." Socio-Economic Planning Sciences 89 (2023): 101701.
[5] Berardi, Davide, et al. "When operation technology meets information technology: challenges and opportunities." *Future Internet* 15.3 (2023): 95.
[6] Breitschopf, Barbara, et al. "Towards understanding interactions between socio-technical systems in sustainability transitions." Energy Research & Social Science 106 (2023): 103323.
[7] Chen, Yushi, and Zhen Yu. "Digitalization, trust, and sustainability transitions: Insights from two blockchain-based green experiments in China's electricity sector." *Environmental Innovation and Societal Transitions* 50 (2024): 100801.
[8] Chobanov, Vesselin, and Ivan Doychev. "Cyber Security impact on energy systems." *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*. IEEE, 2022.
[9] Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse. "Defining cybersecurity." *Technology innovation management review* 4.10 (2014).
[10] ENISA. "Cyber Europe Tests the EU Cyber Preparedness in the Energy Sector." ENISA, 2024, www.enisa.europa.eu/news/cyber-europe-tests-the-eu-cyber-preparedness-in-the-energy-sector.
[11] Erlinghagen, Sabine, and Jochen Markard. "Smart grids and the transformation of the electricity sector: ICT firms as potential catalysts for sectoral change." Energy Policy 51 (2012): 895-906.
[12] European Commission. Critical Entities' Resilience, Press release IP/23/3992, 25 July 2023, ec.europa.eu/commission/presscorner/detail/en/ip_23_3992.
[13] European Commission. Critical Entities' Resilience, Press release IP/23/3992, 25 July 2023, ec.europa.eu/commission/presscorner/detail/en/ip_23_3992.
[14] European Commission. Critical Infrastructure and Cybersecurity, Directorate-General for Energy, European Union, 30 July 2024a, energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en
[15] European Commission. Cyber Resilience Act, Directorate-General for Communications Networks, Content and Technology, European Union, 6 Mar. 2025, digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.
[16] European Commission. EU Cybersecurity Policies, Directorate-General for Communications Networks, Content and Technology, European Union, 30 July 2024b, digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies.

[17] European Commission. Implementing EU Law, European Union, 2022, commission.europa.eu/law/application-eu-law/implementing-eu-law_en.
[18] European Commission. The Digital Europe Programme. Shaping Europe's Digital Future, European Commission, 2021, updated 16 May 2025, digital-strategy.ec.europa.eu/en/activities/digital-programme.
[19] European Commission. The European Green Deal, COM(2019) 640 final, 11 Dec. 2019, eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019DC0640.
[20] Fang, Xi, et al. "Smart grid—The new and improved power grid: A survey." *IEEE communications surveys & tutorials* 14.4 (2011): 944-980.
[21] Fetting, Constanze. "The European green deal." ESDN report, December 2.9 (2020): 53.
[22] Fetting, Constanze. "The European green deal." *ESDN report, December* 2.9 (2020): 53.
[23] Finland. Finland's Cyber Security Strategy 2019. Government Resolution, 3 Oct. 2019, Secretariat of the Security Committee, ISBN 978-951-663-055-0, www.turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf
[24] Geels, Frank W. "From sectoral systems of innovation to socio-technical systems: Insights about dynamics and change from sociology and institutional theory." Research policy 33.6-7 (2004): 897-920.
[25] Geels, Frank W. "Micro-foundations of the multi-level perspective on socio-technical transitions: Developing a multi-dimensional model of agency through crossovers between social constructivism, evolutionary economics and neo-institutional theory." Technological Forecasting and Social Change 152 (2020): 119894.
[26] Geels, Frank W. "Ontologies, socio-technical transitions (to sustainability), and the multi-level perspective." Research policy 39.4 (2010): 495-510.
[27] Geels, Frank W., and Johan Schot. "Typology of sociotechnical transition pathways." Research policy 36.3 (2007): 399-417.
[28] Georgiadou, Anna, Ariadni Michalitsi-Psarrou, and Dimitris Askounis. "A security awareness and competency evaluation in the energy sector." Computers & Security 129 (2023): 103199.
[29] Grin, John, Jan Rotmans, and Johan Schot. Transitions to sustainable development: new directions in the study of long term transformative change. Routledge, 2010.
[30] Gungor, Vehbi C., Bin Lu, and Gerhard P. Hancke. "Opportunities and challenges of wireless sensor networks in smart grid." *IEEE transactions on industrial electronics* 57.10 (2010): 3557-3564.
[31] Hahn, Adam. "Operational technology and information technology in industrial control systems." *Cyber-security of SCADA and other industrial control systems*. Cham: Springer International Publishing, 2016. 51-68.
[32] Hamel, Candyce, et al. "Defining rapid reviews: a systematic scoping review and thematic analysis of definitions and defining characteristics of rapid reviews." Journal of clinical epidemiology 129 (2021): 74-85.

[33] Huttunen, Riku, et al. "Carbon neutral Finland 2035–national climate and energy strategy." (2022).
[34] Keleba, Habeenzu, Oteng Tabona, and Thabiso Maupong. "Developing a Cyber-resilience state in Botswana's Energy Industry." *2022 International Conference on Smart Applications, Communications and Networking (SmartNets)*. IEEE, 2022.
[35] Köhler, Jonathan, et al. "An agenda for sustainability transitions research: State of the art and future directions." Environmental innovation and societal transitions 31 (2019): 1-32.
[36] Lehto, Martti. "Cyber-attacks against critical infrastructure." *Cyber security: Critical infrastructure protection*. Cham: Springer International Publishing, 2022. 3-42.
[37] Mäkitie, Tuukka, et al. "Digital innovation's contribution to sustainability transitions." Technology in Society 73 (2023): 102255.
[38] Markard, Jochen. "The life cycle of technological innovation systems." Technological forecasting and social change 153 (2020): 119407.
[39] Milevskyi, Stanislav, et al. "Development of The Sociocyberphysical Systems multi-Contour Security Methodology." Eastern-European Journal of Enterprise Technologies 127.9 (2024).
[40] Negi, Mansi. "Towards the integration of IT/OT technologies in Electricity Based Digitalized Energy Systems." (2024).
[41] North Atlantic Treaty Organization. Cyber Defence, NATO, 30 July 2024, www.nato.int/cps/en/natohq/topics_52044.htm
[42] North Atlantic Treaty Organization. Relations with the European Union, NATO, 20 June 2025, www.nato.int/cps/en/natohq/topics_49217.htm
[43] Norway. “Ten Facts about the EEA.” Regjeringen.no. Ministry of Foreign Affairs, Dec. 2014, www.regjeringen.no/globalassets/departementene/ud/vedlegg/europapolitikk/eea_facts.pdf
[44] Norway. Climate Action Plan for 2021–2030 (Meld. St. 13 2020–2021). Regjeringen.no, Government of Norway, January 2021, contentassets.a78ecf5ad2344fa5ae4a394412ef8975/en-gb/pdfs/stm202020210013000engpdfs.pdf.
[45] Norway. Lov om nasjonal sikkerhet (sikkerhetsloven). LOV-2018-06-01-24, Justis- og beredskapsdepartementet, 1. juni 2018, lovdata.no/dokument/NLE/lov/2018-06-01-24.
[46] Norway. National Cyber Security Strategy for Norway. Government of Norway, Ministry of Justice and Public Security, Ministry of Defence, Jan. 2019, www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf
[47] Palleti, Venkata Reddy, et al. "Cascading effects of cyber-attacks on interconnected critical infrastructure." *Cybersecurity* 4.1 (2021): 8.
[48] Pirta-Dreimane, Rūta, et al. "Enhancing smart grid resilience: an educational approach to smart grid cybersecurity skill gap mitigation." *Energies* 17.8 (2024): 1876.

[49] Pursiainen, Christer, and Eero Kytömaa. "From European critical infrastructure protection to the resilience of European critical entities: what does it mean?." *Sustainable and Resilient infrastructure* 8.sup1 (2023): 85-101.
[50] Rinaldi, John. "The IT/OT Network Divide." *RTA's Blog*, Real Time Automation, Inc., 23 June 2020, https://www.rtautomation.com/rtas-blog/the-it-ot-network-divide/.
[51] Rosenbloom, Daniel. "Engaging with multi-system interactions in sustainability transitions: A comment on the transitions research agenda." Environmental Innovation and Societal Transitions 34 (2020): 336-340.
[52] Ryu, Dojin, et al. "Enhancing cybersecurity in energy IT infrastructure through a layered defense approach to major malware threats." Applied Sciences 14.22 (2024): 10342.
[53] Sarrica, Mauro, et al. "A multi-scale examination of public discourse on energy sustainability in Italy: Empirical evidence and policy implications." Energy Policy 114 (2018): 444-454.
[54] Sivonen, Marja Helena, and Paula Kivimaa. "Securitization of Energy Transitions in Estonia, Finland and Norway." International Political Sociology 18.3 (2024): olae017.
[55] Stelmashchuk, Kateryna. "How to Ensure Successful Digital Transformation in Energy Industry." N-iX Blog, 22 Dec. 2023, www.n-ix.com/digital-transformation-energy-industry/
[56] Štitilis, Darius, Paulius Pakutinskas, and Inga Malinauskaitė. "EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis." *Security journal* 30.4 (2017): 1151-1168.
[57] Sun, Chih-Che, Adam Hahn, and Chen-Ching Liu. "Cyber security of a power grid: State-of-the-art." *International Journal of Electrical Power & Energy Systems* 99 (2018): 45-56.
[58] Sun, Chih-Che, et al. "Intrusion detection for cybersecurity of smart meters." *IEEE Transactions on Smart Grid* 12.1 (2020): 612-622.
[59] Sweden. A National Cyber Security Strategy (Skr. 2016/17:213)." Government.se, Ministry of Justice, Government of Sweden, 22 June 2017, www.government.se/legal-documents/2017/11/skr.-201617213
[60] Sweden. Draft on Integrated National Energy and Climate Plan. Government.se, Government of Sweden, Ministry of Climate and Enterprise, 17 Jan. 2019, www.government.se/reports/2019/01/swedens-draft-integrated-national-energy--and-climate-plan/
[61] Thoring, Katja, Roland Mueller, and Petra Badke-Schaub. "Workshops as a research method: Guidelines for designing and evaluating artifacts through workshops." (2020).
[62] Verbong, Geert, and Frank Geels. "The ongoing energy transition: Lessons from a socio-technical, multi-level analysis of the Dutch electricity system (1960–2004)." Energy policy 35.2 (2007): 1025-1037.