Introduction
Cybersecurity and electricity sector: relevance, features and challenges

ELENA RAGAZZI, UGO FINARDI, JEANNE C.M. VALLETTE D'OSIA

CNR-IRCrES, Consiglio Nazionale delle Ricerche – Istituto di Ricerca sulla Crescita Economica Sostenibile, Strada delle Cacce 73, 10135 Torino, Italia

Corresponding author: jeannecharlottemarievallettedosia@cnr.it

ABSTRACT
The growing dependence of individuals, organizations, and governments on digital ecosystems increases the exposure to cyber threats, leading cybersecurity to be a global issue in societal, political, and economic decision-making. The electricity sector is especially vulnerable due to its reliance on critical infrastructures embedded in large, interconnected networks. Hence, cyber-attacks on power grids can have catastrophic societal consequences by causing severe disruptions with long recovering times and lasting effects. "Cybersecurity and electricity sector: relevance, features and challenges" introduces the Quaderno IRCrES on *Cybersecurity and data protection in the electricity sector: state-of-the-art of the literature and evaluation methods.* It attempts to understand how citizens value cybersecurity when it comes to the essential good of electricity supply. The volume therefore starts from a review of the literature on Cybersecurity Economics' main features and evaluation methods, with a specific focus on Cost Benefit Analysis methodologies. Then, it surveys recent literature on digital sovereignty at the individual level. Concurrently, the Quaderno presents two practical works. First, it describes the ESSENCE project, providing an illustration of the evaluation of costs and benefits of implementing security standards to critical electric infrastructures. Secondly, it presents an experimental activity evaluating the price attached by the Italian population to a blackout and to a data theft, based on a Discrete Choice Experiment. This introductory chapter emphasizes the relevance of the topic, with a focus on the aspects of prudence and costs in regulation. Moreover, it describes broadly the features of the electrical grid and its critical infrastructures, leading to the mention of economic challenges in the sector. Ultimately, it gives the detailed plan of the Quaderno.

KEYWORDS: Cybersecurity, electricity sector, cost-benefit analysis, literature review.

DOI: 10.23760/2499-6661.2025.24_00
ISBN: 978-88-98193-39-4
ISSN (online): 2499-6661

HOW TO CITE
Ragazzi, E., Finardi, U., & Vallette d'Osia, J.C.M. (2025). Introduction. Cybersecurity and electricity sector: relevance, features and challenges. In Ragazzi, E., Finardi, U., & Vallette d'Osia, J.C.M. (eds.). *Cybersecurity and data protection. in the electricity sector. State-of-the-art of the literature and evaluation methods* (pp. 5-10). Quaderni IRCrES 24. CNR-IRCrES. http://dx.doi.org/10.23760/2499-6661.2025.24_00

1 INTRODUCTION

The Quaderno IRCrES *Cybersecurity and electricity sector: relevance, features and challenges* presents a comprehensive work carried out with the purpose of performing a study and analysis, aimed at reviewing the state of the art and making proposals to increase the awareness of the problems of economic evaluation of cybersecurity, through Cost Benefit Analysis (CBA) methods, with a specific focus on the energy sector. One of the goals of the study presented in this Quaderno IRCrES is also to perform a preliminary study to the realization, design and administration of a survey to estimate the economic value of cybersecurity in the electricity sector from the perspective of citizens.

Cybersecurity has become in the last years a relevant concern for both everyday life and scientific research, as well as a problem of social, economic and political relevance (Hansen & Nissenbaum, 2009) (Dunn Cavelty & Wenger, 2020). The continuous flow of sensitive data across the world digital nets, in fact, controls nowadays a large part of the aspects of industrial production, common life, science and technology (Mondejar et al., 2021) (Leng et al., 2021). These facts make the protection of data in the cyberspace a vital asset of paramount importance for the security of states and populations, as well as for the safety of citizens (Rizi & Seno, 2022).

As in most cases, also in that of cybersecurity, the correct and efficient allocation of resources is fundamental in order to obtain better protection against cyberattacks, data thefts and disruption of services, avoiding also overinvestment and bad investment. Allocating monetary and physical resources allows obtaining better protection at the same price, or equal protection at the same time sparing funds. In consequence of these facts, it is evident that economic evaluation of cybersecurity costs and of its value is fundamental in order to obtain efficiency in cyber protection of assets of any kind.

In this context, some industrial sectors and industries present more critical aspects that make their cyber-protection even more important. It is the case, for instance, of the electricity production, transmission and distribution, and of the critical infrastructures that are one of its vital assets. Given the specific features of strong interconnection and interdependence of such infrastructures, in fact, a disruption only slightly above the safe level of redundance can easily cause a blackout of wide dimensions, possibly of the size of a country electric system. It is easily understandable, then, the strategic level of the protection of these systems (Ragazzi & Stefanini, 2019).

This Quaderno IRCrES, given the above-described relevance of the topic, attempts to outline the main themes related to it in a bird's eye view. In the following of this section two fundamental, introductory topics will be outlined in order to introduce the following chapters' content.

1.1 Prudence and costs

The importance of acquiring information on the economic aspects related to cybersecurity investments (costs and benefits) is tied to the concept of prudence. Regulators may apply prudence assessment to verify that costs claimed by regulated entities are reasonable and necessary, preventing overcharging of consumers. This principle is foundational to public action in Anglo-Saxon systems and echoes a concept typical of our legal framework, namely the "wisdom of the good family father". When investing in infrastructures consuming public resources, those who invest bear a responsibility to use these resources prudently, allocating them to the most critical uses, ensuring connected services, but without wasting money collected from citizens through taxes or utility bills on excessive investments. Prudence regulation ensures that utilities act in the public interest by providing reliable service at reasonable prices. Such decisions can be made with greater awareness if information is available on costs (expenses required to implement countermeasures, including both investments and ongoing expenses) and benefits (the economic value of damage caused by a cyberattack that can be avoided thanks to the aforementioned countermeasures).

But how much is (cyber)security worth to citizens when it comes to an essential good like electricity supply? This is perhaps the most complex aspect to estimate, as cybersecurity is not a good traded on the market at a price but is instead delivered through another good—electricity provision. The electricity system not only ensures that electricity reaches homes when needed but also that the continuity of this service is not compromised by the risk of a cyberattack. The value of cybersecurity cannot, therefore, be derived from available data or investigated through direct questions to consumers, who would likely struggle to assign an economic value to something they recognize as useful but have no direct awareness of. Hence, the need arises to identify investigation techniques, and subsequent data processing methods, that allow extrapolating an economic value from preferences indirectly revealed by respondents. These techniques are described in detail in Chapter 4 (Vallette d'Osia, Finardi & Ragazzi, 2025).

1.2 Relevant features of the electrical grid

Electricity production and distribution systems are an example of sectors where the interdependence of cybersecurity manifest significantly.

First, electrical grids are highly interconnected. Ragazzi & Stefanini (2019) have studied the highly heterogeneous landscape of countermeasures used to block cyberattacks and comply with security standards adopted across Europe. The authors highlight how an event occurring within an electrical grid in one country or macro-region can have repercussions on many other areas.

Moreover, electrical grids include various types of critical infrastructures, such as high-capacity production plants, high-voltage lines, and substations, which are themselves part of the complexity and interdependence of the electricity sector's infrastructure. The absence of the possibility of large-scale, high-voltage electricity storage and the dependence on grid synchronization amplify vulnerability. Consequently, significant security and maintenance efforts are required in electrical grid infrastructure, as imbalances and cyberattacks beyond redundancy levels could disrupt the entire network and lead to widespread blackouts.

Finally, companies that sell electricity possess their customers' personal data, which can lead to specific economic challenges relevant to cybersecurity. For example, information asymmetry could manifest through a potential lack of trust between the company and its customers or through inefficient decision-making due to a lack of understanding of how customer data might influence electricity prices or services. Additionally, the social cost of a cyberattack on critical infrastructure in the electrical grid is not entirely borne by the sector's companies. Considering the significant consequences that a cyberattack resulting in the theft of personal data (such as loss of privacy or identity theft) could have, there could be an underinvestment in cybersecurity related to the protection of consumer profiles. Consequently, cybersecurity measures are not only about protecting individual entities but also safeguarding the integrity of the entire system.

These characteristics, which involve the development of strong and sustainable protection strategies for electrical system infrastructure, require particular attention to the evaluation of cybersecurity to design effective protection strategies and avoid under- or over-investment. Furthermore, they highlight the need for a collective approach in terms of regulation or public intervention.

2 THE CHAPTERS OF THIS QUADERNO

This introductory chapter of this Quaderno details the main research interests that motivate it. As described above, we will try in this Quaderno to focus on the challenges related to the protection of the continuity of electricity service, specifically from cyber threats, exposing why concrete solutions for developing strong and sustainable protections strategies for the power sector are of crucial importance,

The first chapter (Vallette d'Osia, Finardi & Ragazzi, 2025) describes the unique features and challenges of the economic analysis of cybersecurity. Taking a broad perspective, we discuss the market failures, known as misaligned incentives, information asymmetries, and externalities, that hamper the right allocation of resources when attempting to allocate an optimal level of

investment in secure system. Closely linked to the elucidation of these challenges, the literature also questions the nature of cybersecurity. We therefore provide some insights regarding the discussion of the characterization of cybersecurity as a public good. In addition, we question the role played by regulation and common awareness in this context, specifying how regulatory activity towards the cybersecurity facet within the electricity sector is specifically difficult due to the presence of market failures. Building on this theoretical observation of cybersecurity, we investigate the state-of-the-art of the literature on the various economic approaches and models used to measure the value assigned to cybersecurity by end-users, from investment and cost estimation models to managerial and consulting approaches. We analyse theoretical, multidisciplinary and empirical methods that intend to do so, first regardless of the sector of application, then focusing on studies tackling cybersecurity's value within critical infrastructure sectors.

The second chapter (Vallette d'Osia, Finardi & Ragazzi, 2025) delves into the topic of digital sovereignty, as its evaluation is often ambiguous. More specifically, we will have a specific target on the valuation of individuals' digital privacy preferences. In fact, as it can be the case for the continuity of electricity service, secure online privacy is often perceived as a fundamental societal need, which tends to blur individuals' ability to assign them a clear or consistent value. Data sovereignty could either be regarded as a right, thus something to be guaranteed by institutions or firms, requiring no direct engagement from individuals, or as a good, entailing production costs and a willingness to pay. To assess the conditions and extent to which individuals' perceptions of online privacy are subject to instability, we review literature that tackles the behavioural biases that hampering data users' appraisal of privacy risks and preferences. In a second stage, we analyse also the literature on personal data privacy, especially studies that aim at measuring how people perceive data breaches in specific contexts and for diverse types of data (e.g., personal characteristics, financial information, or data collected on smartphone app), leading us to investigate the debate around what scholars define as the Privacy Paradox.

The third chapter (Bruno & Erbetta, 2025) is then dedicated to the re-examination of the ESSENCE (Emerging Security Standards to the EU power Network controls and other Critical Equipment) project, which evaluated the costs and benefits of implementing security standards to critical electric infrastructures. Specifically, two case studies, in Italy and in Poland, were used to gauge the benefits of not suffering an electricity blackout caused by a cyber-attack. This chapter acts as an illustration both for the topic of implementing cybersecurity standards to the electric system and the inherent evaluation methods that can be used to measure the economic value of the continuity of electricity service.

To root our theoretical findings to a practical aspect, we devote the fourth chapter (Vallette d'Osia, Finardi & Ragazzi, 2025) of this Quaderno to the review of CBA methodologies. These approaches allow for the economic valuation of non-market goods, such as security, and thus support balanced decision-making regarding investments or regulatory actions needed to achieve efficient and sustainable cybersecurity measures. Stemming from CBA methodologies, we place particular emphasis on Stated Preference (SP) methods, which encompass Discrete Choice Experiments (DCE) and Contingent Valuation (CV) methods, as we argue they are better suited to the topic of cybersecurity than revealed preference approaches. The latter assume that individuals can easily assign a value to the good or service being evaluated, which, as previously noted, we argue is not the case with cybersecurity. We provide a review of the specific application of CBA methods to the electric sector, which mainly relies on conceptual frameworks based on Willingness to Pay (WTP) to avoid blackouts, or Willingness to Accept (WTA) a compensation for outages or lower quality of power service. We note the lack of studies that tackle challenges of cybersecurity in ensuring the security of electrical systems.

The fifth chapter (Vallette d'Osia, Finardi & Ragazzi, 2025) of this work serves as a concrete application of the findings summarized in the previous chapters. It presents in fact the survey we conducted on a representative sample of the Italian population to study the value citizens place on electricity continuity and digital sovereignty in the electricity power sector. A secondary aim of the study was also to raise awareness of cyber threats in the sector, which was achieved by including questions implying such risks throughout the questionnaire. We provide a detailed

explanation of the design chosen for the survey instrument, as well as the administration method used to carry it out.

Finally, the last chapter (Vallette d'Osia, Finardi & Ragazzi, 2025) provides a summary of the findings deriving from our past experimental experience, as well as from our extensive literature review and present experimental activity. The concluding remarks give ground for the representative survey we carried in order to understand how individuals value their personal data within the electrical energy sector. We recall why this survey was legitimate and essential to carry, both from a theoretical and practical point of view, as the topic of cybersecurity has shown to have been of great interest to respondents, while acknowledging some remaining challenges and the need to extend the survey to other countries.

3 BIBLIOGRAPHY

Bruno, C., & Erbetta, F. (2025). The ESSENCE Project: A Re-Examination Guided by Emerging Academic Contributions. In Ragazzi, E., Finardi, U., & Vallette d'Osia, J.C.M. (eds.). *Cybersecurity and data protection. in the electricity sector. State-of-the-art of the literature and evaluation methods* (pp. 45-52). Quaderni IRCrES 24. CNR-IRCrES. http://dx.doi.org/10.23760/2499-6661.2025.24_03

Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), pp. 5-32. https://doi.org/10.1080/13523260.2019.1678855

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, *53*(4), pp. 1155-1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Leng, J., Wang, D., Shen, W., Li, X., Liu, Q., & Chen, X. (2021). Digital twins-based smart manufacturing system design in Industry 4.0: A review. *Journal of manufacturing systems*, 60, pp. 119-137. https://doi.org/10.1016/j.jmsy.2021.05.011

Mondejar, M.E., Avtar, R., Diaz, H.L.B., Dubey, R.K., Esteban, J., Gómez-Morales, A., Hallam, B., Mbungu N.T., Okolo C.C., Prasad K.A., She, Q., & Garcia-Segura, S. (2021). Digitalization to achieve sustainable development goals: Steps towards a Smart Green Planet. *Science of The Total Environment*, 794, art. 148539. https://doi.org/10.1016/j.scitotenv.2021.148539

Ragazzi, E., Finardi, U. & Vallette d'Osia, J.M.C. (2025). Concluding remarks. In Ragazzi, E., Finardi, U., & Vallette d'Osia, J.C.M. (eds.). *Cybersecurity and data protection. in the electricity sector. State-of-the-art of the literature and evaluation methods* (pp. 71-73). Quaderni IRCrES 24. CNR-IRCrES. http://dx.doi.org/10.23760/2499-6661.2025.24_06

Ragazzi, E., & Stefanini, A. (2019). Are security standards for electricity infrastructure a good choice for Europe? Evidence on cost and benefits from two case studies. *International Journal of Critical Infrastructures*, *15*(3), pp. 206-229. https://doi.org/10.1504/IJCIS.2019.100425

Rizi, M.H.P., & Seno, S.A.H. (2022). A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city. *Internet of Things*, 20, art. 100584. https://doi.org/10.1016/j.iot.2022.100584

Vallette d'Osia, J.M.C., Ragazzi, E., & Finardi, U. (2025). The economic perspective on cybersecurity. In Ragazzi, E., Finardi, U., & Vallette d'Osia, J.C.M. (eds.). *Cybersecurity and data protection. in the electricity sector. State-of-the-art of the literature and evaluation methods* (pp. 11-25). Quaderni IRCrES 24. CNR-IRCrES. http://dx.doi.org/10.23760/2499-6661.2025.24_01

Vallette d'Osia, J.M.C., Ragazzi, E., & Finardi, U. (2025). Digital sovereignty: a new perspective focused on data control. In Ragazzi, E., Finardi, U., & Vallette d'Osia, J.C.M. (eds.). *Cybersecurity and data protection. in the electricity sector. State-of-the-art of the literature and evaluation methods* (pp. 27-43). Quaderni IRCrES 24. CNR-IRCrES. http://dx.doi.org/10.23760/2499-6661.2025.24_02

Vallette d'Osia, J.C.M., Finardi, U., & Ragazzi, E. (2025) Methods to assess the economic value of cybersecurity. In Ragazzi, E., Finardi, U., & Vallette d'Osia, J.C.M. (eds.). *Cybersecurity*

and data protection. in the electricity sector. State-of-the-art of the literature and evaluation methods (pp. 53-62). Quaderni IRCrES 24. CNR-IRCrES. http://dx.doi.org/10.23760/2499-6661.2025.24_04

Vallette d'Osia, J.M.C., Finardi, U., & Ragazzi, E. (2025). An empirical approach to assess the value assigned by individuals to cybersecurity and data protection. In Ragazzi, E., Finardi, U., & Vallette d'Osia, J.C.M. (eds.). *Cybersecurity and data protection. in the electricity sector*. *State-of-the-art of the literature and evaluation methods* (pp. 65-70). Quaderni IRCrES 24. CNR-IRCrES. http://dx.doi.org/10.23760/2499-6661.2025.24_05