Quaderni
CNR IRCrES
Temi e problemi di sostenibilità sociale, economica, ambientale

Cybersecurity and data protection in the electricity sector

State-of-the-art of the literature and evaluation methods

edited by

Elena Ragazzi
Ugo Finardi
Jeanne C.M. Vallette d'Osia

CNR - Consiglio Nazionale delle Ricerche
IRCrES - Istituto di Ricerca sulla Crescita Economica Sostenibile
ISSN (online) 2499-6661 ISSN (print) 2499-6955

Cybersecurity and data protection in the electricity sector

State-of-the-art of the literature and evaluation methods

edited by

Elena Ragazzi
Ugo Finardi
Jeanne C.M. Vallette D'Osia

CNR-IRCrES

Quaderni IRCrES
Temi e problemi di sostenibilità sociale, economica, ambientale

Direttrice	Elena Maria Ragazzi
Direzione	CNR-IRCrES Istituto di Ricerca sulla Crescita Economica Sostenibile Strada delle Cacce 73, 10135 Torino, Italy Tel. +39 011 3977612 segreteria@ircres.cnr.it www.ircres.cnr.it
Sede di Roma	Via dei Taurini 19, 00185 Roma, Italy Tel. +39 06 49937809 / Fax +39 06 49937808
Sede di Milano	Via Corti 12, 20121 Milano, Italy Tel. +39 02 23699505 / Fax +39 02 23699530
Sede di Genova	Corso Ferdinando Maria Perrone 24, 16152 Genova, Italy Tel. +39 010 6598798

Copertina: elaborazione grafica a cura di Serena Fabrizio.

redazione@ircres.cnr.it
www.ircres.cnr.it/index.php/it/produzione-scientifica/pubblicazioni

Quaderni IRCrES 24
http://dx.doi.org/10.23760/2499-6661.2025.24

ISBN 978-88-98193-39-4

Contents

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

Chapter 1
The economic perspective on cybersecurity

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

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
This chapter of the Quaderno IRCrES *Cybersecurity and data protection in the electricity sector: state-of-the-art of the literature and evaluation methods* reviews the literature on two main aspects, the concepts on which the economic analysis of cybersecurity is built on, and the methods, both theoretical and empirical, developed to assess the value of cybersecurity. Itis therefore divided in two parts. First, regarding the broad perspective of economics applied to cybersecurity, we tackle the discussion on the nature of cybersecurity as a public good, the market failures hampering the right allocation of resources within investment in cybersecure systems, and thus, the regulation policies and general awareness on the topic. Then, we review the approaches and models developed for cybersecurity estimations, followed by a focus on the studies addressing cybersecurity's value within critical infrastructure sectors. The review demonstrates a literature on the topics of cybersecurity economics already significant, revealing different schools of economics employed in cybersecurity, as well as multidisciplinary approaches and, in turn, various models for cybersecurity investment. Yet, developing economically viable cybersecurity strategies still calls for representative data on cyberattacks as well as the adaptation of evaluation techniques to individual behaviours, and system's complexity.

KEYWORDS: Cybersecurity, critical infrastructures, public good, market failures, estimation methods.

DOI: 10.23760/2499-6661.2025.24_01
ISBN: 978-88-98193-39-4
ISSN (online): 2499-6661

HOW TO CITE
Vallette d'Osia, J.C.M., 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

This chapter reviews and discusses a selection of research works related to the economic evaluation of cybersecurity. In specific, the first section covers the topics of the purposes, problems, and challenges of the economic analysis of cybersecurity, the challenges related to protecting the continuity of electricity service, and the regulation and awareness of socioeconomic factors. The second section delves deeper into the specific issue of estimating the value of cybersecurity. Consequently, it discusses the approaches and models developed to understand the economic value of cybersecurity and the evaluation of cybersecurity for critical infrastructures.

1 PREVIOUS RESEARCH ON THE ECONOMIC VALUE OF CYBERSECURITY

Economic studies tackle numerous topics related to the economic evaluation of cybersecurity. A non-exhaustive list of the main topics can be outlined as follows:

1. Economic studies on the appropriate level of investment in cybersecurity. These studies combine economic and engineering approaches to highlight the correct balance between investment in cybersecurity and expenditure, considering the diminishing marginal levels of cybersecurity with linearly increasing costs. The literature is eminently empirically driven.
2. Studies on the economic aspects related to regulation and policies for cybersecurity.
3. Studies related to cybersecurity metrics, both in terms of identifying economic metrics and considering the metrics themselves as leverage points for proper corporate or regulatory management of cybersecurity. Also in this case, the papers have an interdisciplinary focus, with numerous references to engineering and computer science.

However, most of these topics, along with others not explicitly listed, fall outside the specific focus of this work, which instead concentrates on the specific issue of evaluating and measuring the value assigned to cybersecurity by end-users. This is a specific topic aimed at providing data and evidence functional to policy design and the fine-tuning of regulation, and which can therefore, at least in a broad sense, fall into group 2.

This section will address some topics relevant to our discussion. It will begin with an analysis of the scientific literature related to the purposes, problems, and challenges of the economic analysis of cybersecurity (in general, regardless of the sector of application). The second subsection, in turn, will examine the topic of regulation and awareness of the socioeconomic aspects of cybersecurity.

1.1 Purposes, problems and challenges of the economic analysis of cybersecurity

The concept of cybersecurity has long been associated with the protection of Information Technology (IT) structures and the data they transmit, manage, and store, thus defining a set of predominantly technical studies. However, the complexity of its evolution and its crucial role in sectors such as electricity production and distribution have generated new challenges regarding understanding its value and the proper allocation of resources for its implementation. Cybersecurity also deals with protecting data from malicious use by third parties. Aligning with this view, Craigen, Diakun-Thibault & Purse (2014) define cybersecurity 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" (p. 17).

Since the academic field of cybersecurity is highly interdisciplinary, it is treated and discussed in numerous scientific sectors, approached through themes such as risk management, prevention, or public cybersecurity. The perspective and context in which it is studied influence its interpretation: the more or less pronounced characteristics of a public good with which it can be characterized depend precisely on the context.

In market-driven contexts, such as industrial sectors where data protection is closely tied to corporate strategies (i.e. companies for which information is a strategic input), sectors where

reputation is an essential competitive factor (e.g. banks), or sectors where cybersecurity is offered as an intrinsic feature of a sold product (i.e. when equipment is acquired with embedded cybersecurity), cybersecurity can be treated as a private good. However, in contexts such as national security or critical infrastructures, where legal, social, and ethical issues are at stake, the concept of cybersecurity as a public good better applies. Kianpour, Kowalski & Øverby (2022), advance the concept of cybersecurity as public good performing an agent-based modelling experiment. In this way they demonstrate that an important challenge for society as a whole is posed by the presence of free-riders, that is, actors who benefit from a (public) good without contributing to it, weakening the development and stability of the society of information.

This perspective is extended by Taddeo (2019). Her work emphasizes the concept that critical infrastructures are enabled by the presence of robust systems, i.e., by those digital and information infrastructures that can remain functional notwithstanding the presence of attacks, or of errors. In this way they enhance social stability. The author studies data on cyberattacks, associating them with the specific state of cybersecurity, and then suggesting that cybersecurity should be framed within the scope of public good. Treating it as a club good (that is, the case of a good for which access is regulated by a cost, and thus excludable, but which is not rivalrous) in fact would not allow to consider properly its social implications. Nevertheless, the same author also put forward situations where cybersecurity is not a public good. It is the case of system resilience, which might undermine the privacy of users. The author concludes that "considering some of digital technologies or uses […] as public good will be a step in the right direction insofar as it done cautiously and to support policy and governance approaches that will foster tolerant […] and stable information societies" (p. 353, passim).

The role of governments in establishing contexts able to enhance cybersecurity, particularly supporting public cybersecurity is put forward by Asllani, White & Ettkin (2013), who compare cybersecurity with safety as a public good. The authors conclude that cybersecurity needs collective actions at all administration levels, besides a personal and organizational effort, in order to reach protection at national security level. Another parallel is performed by Mulligan & Schneider (2011) who propose treating cybersecurity as a public good adopting mechanisms similar to those used for public health. The target of public health, as well as of cybersecurity, is achieving a positive situation in a highly interdependent network. Moreover, authors highlight that the value of cybersecurity remained at the time of their work largely undetermined. In fact, both enterprises and clients were (and still are in most cases) neither able to attribute a price to confidentiality and integrity of information nor able to estimate the cost of the recovery from the effects of a cyberattack.

This first introductory step of our review, being a discussion of the public/private good dichotomy applied to cybersecurity, aims to help foster a better understanding of the core argument, as well as the related market failures highlighted by the economic losses generated by informatic violations. Moore (2010) in discussing the economics of cybersecurity, describes some important economic challenges: information asymmetries, misaligned incentives, and externalities. These three are relevant features of market failures, and as such deserve to be discussed.

The concept of misaligned incentives refers to situations where, in a transaction, the objectives of the different parties do not coincide. For example, a company may pay its subcontractors a fixed fee to secure their work, but the subcontractors may fail to complete the work on time precisely because of the certainty of receiving a fixed income.

Information asymmetries arise when, in an economic relationship, not all parties are aware of the same information. A typical case of information asymmetry is real estate transactions, where one party (the seller) is aware of all the information about the property's condition (including any structural or legal issues) that may not be disclosed to the buyer.

Externalities, finally, are defined as the effects of an activity that falls on an external party without the agent receiving compensation (positive externalities) or, conversely, that the party suffering harm receives compensation (negative externalities). A typical case of the former is knowledge spillovers, where those who produce knowledge, for example by studying a new production technology, see their invention partially exploited by others without receiving

compensation. Note that knowledge is a classic example of public good. A typical case of the latter is environmental issues, where, for example, a company that pollutes via its production process causes harm to the surrounding residents without them receiving compensation.

When dealing with information asymmetries, Moore (2010) underlines the fact that firms are not incentivized in sharing information, in particular when violations are involved, due to the possible problems in reputation or in exposing own vulnerabilities. This causes, in turn, a lack of reliable and transparent data, which might cause therefore a suboptimal level of investment in cyber protection. The context of insufficient circulation of information on cyberattacks, thus, might cause an incorrect allocation of resources regarding firms both using and producing cybersecurity assets. Organizations, in fact, might underestimate incidents and vulnerabilities; security system sellers, by their side, might invest at suboptimal level in reliable security measures, in particular if customers might not be willing to pay a price for protection. This, in turn, might create a situation where investments are misaligned with effective risk.

Accounting and market data can be used to measure the correlation existing between cybersecurity practices and firm performance. This strategy was followed by Al Amosh & Khatib (2024) on a sample of firms quoted in the Australian stock market. Results show a positive impact of increased cybersecurity disclosure on the performance. Transparency mitigates information asymmetry and consequently reduces conflicts between management and stakeholders. Information asymmetries existing between sellers and buyers engaged in electronic transactions can distort the security levels from those deemed adequate. This thesis is demonstrated by Nagurney & Nagurney (2015) through a game theory model.

A further challenge to the cybersecurity economy is relative to the presence of externalities. Different types of externalities can take place: for instance, network externalities, externalities of insecurity, and interdependent security (Moore, 2010). Network externalities depend on the growing benefit for each network member at the growth of the network dimension. This in turn causes a growth in the net value of the platform, favouring dominant firms. Network externalities might explain the presence of unsafe operating systems, as the competition among sellers arises before an emphasis on security is set. Moreover, security of an internet protocol depends also on the prompt update of one's system by part of all users once a problem arises. On the other side externalities of insecurity issues are generated when compromised sites endanger other ones. For instance, botnets cause more social than private losses, since their objective is not the single, network-connected PC, but routers and web servers. This fact might cause further underinvestment protection against social risk. Last but not least, interdependent security takes place when some actors benefit from protective actions put in action by other ones. This might cause freeriding and underinvestment.

Finally, as previously mentioned, the interdependence of security occurs when protective actions benefit some actors but may simultaneously discourage their investments, leading to a free-riding situation. Investments in security can also be discouraged by situations where the resilience of an entire network is equal to that of its weakest link: in a situation where companies are interconnected, they are discouraged from investing in security if they know that others are not doing so either. This, in turn, creates vulnerabilities at the network level.

Cybersecurity presents some features of public good that exacerbate the problem of incentives misalignment, notwithstanding the fact that security decisions are mainly taken by market actors. Bauer & van Eeten (2009) studied a methodology to understand how the markets of cybercrime and cybersecurity coevolve. In this way they examine the offer of security incentives for different stakeholders, in the context of interdependent communication and information systems. Interviewed actors in this context show conflicting incentives, as well as hindering externalities. The authors emphasize that actors in an ICT (Information and Communication Technology) ecosystem, such as internet service providers or software vendors, have in some cases expressed conflicting incentives. Moreover, in cases where the same actors shared common incentives toward improving security, these were hindered by the presence of externalities, since "end-users perceive no incentive to secure their machines" (p. 714).

Dacus & Yannakogeorgos (2016) also elaborate an incentive structure apt at motivating defence cybersecurity agents to put a larger effort into securing their environments. The authors

underline also the fact that information asymmetries (different priorities between cybersecurity service suppliers and customers) and incentive misalignment (misaligned motivations between the two) can generate moral hazard. In other words, this can happen when the priorities of cybersecurity service providers differ from those of their clients, and when their motivations are not aligned. In their case study, related to contractual operators of the U.S. Department of Defense, the effort dedicated to security codes or network defence is lower than desired by the government.

In conclusion, cybersecurity presents characteristics and social implications similar to those of public security or public health, which are commonly defined as "public goods". Moreover, the economic challenges, specifically misaligned incentives, information asymmetries, and externalities, of cybersecurity lead to market failures, limiting the optimal level of investment in secure systems. In addition to causing an underestimation of the concept of cybersecurity as a public good, these market failures highlight the need for public intervention.

1.2 Regulation and awareness of socioeconomic aspects

An emblematic case in terms of public intervention to mitigate market failures as well as cyber risk is that of the General Data Protection Regulation (GDPR)[1] implemented in the European Union. Aimed at harmonizing the legislation on data protection at the global level (for every Member State of the European Union) in 2016, the GDPR has since been criticized for imposing a significant administrative burden, particularly due to extensive bureaucratic requirements. This, in turn, stems from a lack of transparency in the logic underlying some provisions, even in cases where data usage is easily understandable. In this context, Li et al. (2023) conducted a systematic review of empirical evidence on the evaluation and revision of the GDPR. Their synthesis mentions other common criticisms of the GDPR, such as the lack of enforcement against big tech companies, the inadequacy of imposed sanctions, and design flaws (including for instance excessive reliance on consent). Although the GDPR is far from being a general failure, their work shows that the complexity and internal contradictions among its various components can lead to conflicts and inefficiencies during implementation.

It is instead Moore (2010) who examines two different regulatory approaches to cybersecurity, the ex-ante and the ex-post strategies, as possible solutions to the economic barriers it must face. Ex-ante strategies entail the proactive adoption of security policies by the firms. The lack of information on risks or standards (in particular in a continuously evolving horizon) makes often this approach ineffective. Ex-post strategies, on the other hand, design regulation considering firms as responsible for failures and adverse outcomes. The problem here is that of unreliability and immaturity of firms towards implementing adequate prevention strategies, or of lack of financial capability to refund damages. To address these shortcomings, Moore proposed improving information disclosure to reduce information asymmetry, which must be considered the main obstacle to effective regulation. He also argued that information disclosure can motivate companies to improve their practices, support the common right to knowledge, and create publicly available data on security incidents. This, in turn, could foster collective awareness. Despite these benefits, it is important to note that, as demonstrated by the GDPR experience, the presence of regulations is not sufficient to achieve full disclosure of cyberattack information by companies. As discussed in the previous section, misaligned incentives among different parties, fear of losing trust and reputation, and the increased risk of hackers exploiting disclosed information to discover system vulnerabilities all significantly hinder the disclosure of specific attack information. Therefore, disclosure cannot be considered a condition for regulatory effectiveness but must itself be the subject of regulation and incentivization, also leveraging the results of research activities on information technologies for secure data sharing.

[1]G.D.P. Regulation (GDPR) (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 L 119, p. 1-88).

A more precise and relevant field to study for the purpose of this Quaderno is the regulation of cybersecurity within the electricity sector as the final aim is to understand the value of cybersecurity when it comes to electricity supply.

The introduction of new forms of regulation, distinct from state ownership and monopoly control, for the electricity sector, is a relatively recent development. It is not only justified by the essential nature of the service for daily life and the fact that electricity is a strategic input for all production processes; as long as this service was managed by vertically integrated companies directly or indirectly controlled by the state, regulation was minimal, and priority management occurred through executive acts. Only with the start of the privatization process and the introduction of competition in certain stages of the process did it become necessary to produce regulations (defining foundational principles) and technical regulatory acts (what is required of market operators) and economic acts (in simple terms, "who pays for what") to protect collective social and economic interests. The issue of cybersecurity became the subject of this regulatory activity somewhat out of order on the basis that most facilities are now managed through remote controls.

Technical regulation is based on a series of prescriptions derived from the state of the art of technological knowledge, but it often neglects to consider the implications that economic and human aspects, such as costs or awareness, can have on the implementation process. For example, when the NERC-CIP standard was imposed as mandatory for electric operators in North America, the cost of compliance for less mature operators proved to be extremely high, to the point that some reportedly preferred to pay the substantial fines imposed on non-compliant entities rather than immediately bear the cost of compliance.

Regulation of the electric power systems is particularly needed in those situations where the different components – production, transmission, distribution – are unbounded and subject to the free market. In this situation the strategic nature of electricity compels policy makers to regulate the market, as well as the technical issues. The presence of norms, defining fundamental principles, technical regulations, defining what market operators must do, and economic regulations, defining who pays for what, ensures the protection of collective social and economic interests. Cybersecurity is obviously one of the objects of such normative activity, due to its strategic nature in the contemporary context of dependence of critical infrastructures from cyber networks. In these contexts of competition and free market the task of regulating energy markets is entrusted to specific bodies which, together with other tasks, also have to deal with the regulation of cybersecurity.

These facts suggest that policymakers should carefully balance regulatory demands with sector-specific incentives, paying particular attention to situations where short-term costs (especially those borne by companies) may outweigh long-term benefits (especially systemic ones). There is a need for regulatory frameworks that enforce compliance with rules but also create positive incentives for utilities to invest in long-term resilience and innovation. Indeed, this would improve both economic efficiency and system reliability.

A specific work on the topic of cybersecurity regulation within the electricity sector has been undertaken by Ragazzi, Stefanini, Benintendi, Finardi & Holstein (2020) who elaborated a set of guidelines for energy regulators. The authors highlighted two main typologies of regulation that regulators can use in order to regulate investments in cybersecurity. The first one is the Performance-based regulation (PBR). PBR is based on incentives, as it emphasizes the achievement of specific results, measured with the use of metrics. Regulators establish ex-ante target results of security, while operators design strategies apt at achieving the target, which are verified ex-post. The second one is the Cost-of-service regulation. In this case regulators identify ex-ante protection strategies and then approve the strategic plans of the utilities, which make expenses. PBR entails the presence of mature operators, able to self-protect their assets. Cost of service, on the other hand, while assuring coverage of expenses leaves the decision of the protection strategy to the regulator. PRB can be also designed to reduce operational costs and promote efficiency of service and investments, as well as energy efficiency.

These results are outlined by Brown & Sappington (2023) in their assessment of the impact of incentive-based regulations in the electricity sector. The assessment is performed by observing

the effects of PBR on items such as network reliability, efficiency of investments on the network, or promotion of environmental objectives.

Leszczyna (2019), in his work "Cybersecurity in the Electricity Sector", outlines guidelines for a systematic approach to cyber protection in electrical system facilities. In this work, the author emphasizes how a lack of awareness among stakeholders in the electricity sector can have negative impacts. For example, he explains how the acceptance of significant investments in secure and reliable technologies depends on the awareness, among both company managers and consumers, of the benefits, costs, and risks associated with modern electricity systems. Indeed, regulators will find it more difficult to approve increases in electricity tariffs aimed at enhancing the cybersecurity of electrical systems when consumers are unaware of the importance of more secure technologies, which are consequently linked to higher energy prices. The same author argues that to efficiently protect the IT resources of entities, consumers must take their role as active observers seriously (i.e., being able to report unusual activities), and employees must be aware of the potential risks associated with their activities. These behaviours can be fostered through appropriate training interventions within companies and adequate consumer information and awareness tools. The data collected through the survey methodology presented in this report can also be used to understand such awareness in the population and, if collected systematically through repeated surveys over time, the effectiveness of awareness campaigns.

Another problem related to the lack of awareness lies in the accountability and evaluation of regulators. For example, there is no performance evaluation framework for the Data Protection Authorities (DPAs) of the GDPR. Buckley, Caulfield & Becker (2024) have studied what professionals consider to be the objectives of data protection regulators and how their efficiency is evaluated. The results show a discrepancy between the presumed objectives attributed to regulators and the criteria used to evaluate them in current practice.

To sum up, the GDPR exemplifies the challenges of public intervention in cybersecurity, revealing the need for an harmonious legal framework as a condition for a European market for data while generating important administrative burdens and implementation inefficiencies. Especially in the sector-specific case of the electricity industry, the public good characteristics of cybersecurity motivate the need for regulation as well. More precisely, regulatory strategies must address the core issue of information asymmetry. First, regulated entities often possess better information than regulators regarding the actual conditions of industrial sectors. Consequently, especially in mature electrical systems like Italy's, regulatory methods must be designed to induce regulated companies to use their information to achieve regulatory objectives and beyond. A second consideration must be made on the issue of risk awareness within the different parts of regulated organizations, which is a necessary condition for an efficient regulatory framework. The broad scope of these challenges suggests significant parsimony in regulatory production, especially in mature electrical systems, considering the possibility of acting on other levers, such as the valorisation and promotion of technological innovations, participatory approaches for sharing regulatory objectives with regulated entities, or the collaborative construction of guidelines.

2 METHODS TO MEASURE AND UNDERSTAND THE ECONOMIC VALUE OF CYBERSECURITY

This section enters more deeply into the core of this review. Its purpose, in fact, is to discuss the different approaches dealing with the problems of the economic evaluation of cybersecurity. In doing so, it reviews the content of a selection of works, trying to describe the state-of-the-art of scientific research on the topic of the economic value of cybersecurity. As the following of this section will show, several methods apt at this scope exist. These methods entail different models of cost and investment estimation. A part of such models is theoretical and concentrated on specific aspects. Nevertheless, they are still noteworthy for their contribution to the general framework. An initial introductory subsection will describe the existing approaches and models aimed at understanding this value. The second subsection, on the other hand, will go into greater

detail by addressing the challenges of evaluating cybersecurity for critical infrastructures, with particular attention to those in the electrical system. Table 1 summarizes the literature review, highlighting the approaches and main contributions of each selected study.

2.1 Approaches and models for understanding the economic value of cybersecurity

This section provides a review of selected works aimed at describing the state of the art in scientific production on the topic of the economic value of cybersecurity. Currently, there is a wide range of methods useful for this purpose, implemented primarily through various investment models and cost estimations of cybersecurity. Many of these models are theoretical, developed using game theory approaches, and focus on very specific aspects, which are nonetheless noteworthy for their contribution to the general picture.

Both Haapamäki & Sihvonen (2019) and Kianpour, Kowalski & Øverby (2021) have conducted literature reviews on the topic of cybersecurity.

Kianpour et al. (2021) adopt a broader perspective. Doing so, they examine the economics of cybersecurity as an interdisciplinary field and highlight its evolution toward dynamic and generalizable models. Indeed, they categorize the models into four different approaches: financial analysis, microeconomics, managerial approaches, and combinatorial approaches. Financial analysis often employs theoretical decision-making methods based on traditional risk assessment but is limited by its inability to capture the strategic nature of cybersecurity. It is often considered that game theory models, part of the microeconomic approach, are more robust. This is so because these methods account for interactions between companies and those carrying out strategic attacks or interdependent organizations. The authors also highlight a limitation of game theory models, which aim to maximize utility while practical cybersecurity decisions must also address cyber risk mitigation, compliance, profitability requirements, and cultural adaptation.

As for Haapamäki & Sihvonen (2019), they focus on the topic of accounting, organizing the work around specific themes: cybersecurity and information sharing, investments in cybersecurity, internal audits and cybersecurity controls, disclosure of cybersecurity activities, and security threats and breaches.

Despite their different focuses, both articles emphasize the critical need for practical insights aimed at improving decision-making for professionals and policymakers. Both also highlight the value of interdisciplinary approaches and demonstrate how the interaction between operational and macroeconomic considerations is crucial in defining effective cybersecurity practices.

To grasp the diversity of disciplines seeking to elicit the economic value of cybersecurity, the analysis of these theoretical approaches will primarily focus on game theory-based articles that analyse specific aspects and obstacles to cybersecurity, as explained in Section 1.1, and secondarily on studies adopting risk management approaches, which include both the topic of optimal amount of investments as well as strategic and organizational issues regarding how firms deal with cybersecurity risks.

In the realm of game theory, Nagurney & Nagurney (2015) developed a game theory model applicable in cases of information asymmetry. More specifically, their model applies to electronic transactions between sellers and buyers at the time of product purchase. Sellers are aware of their investment in cybersecurity, while buyers are only aware of the average security of sellers. Additionally, sellers compete with each other by maximizing their expected profits and investing in cybersecurity. However, it should be noted that their model does not consider the impacts of imposing minimum requirements, for example, by a regulatory body.

Companies that are part of an interconnected network are vulnerable to the propagation of third-party risk through weak nodes in supply chains. Therefore, Dash, Sarmah, Tiwari, Jena & Glock (2024) studied the optimal cybersecurity investment strategy in a two-tier supply chain. To this end, they examined a model where retailers are interconnected with a single supplier. This work is also based on game theory and aims to improve companies' ability to manage complexities in practical situations. Consequently, they explore the possible connections between different types of cyberattacks, the interconnected nature of companies, and the role of mandatory

cybersecurity insurance. The results confirm that optimal levels of cybersecurity investment are higher in the case of targeted attacks, such as denial of service or website defacement, compared to opportunistic attacks, such as spam emails or viruses.

For instance, also Ghadge, Weiß, Caldwell & Wilding (2019) deal with cyber risk in supply chains from another perspective. In order to respond to their research question on "how can organisations manage cyber risk on supply chains?" (p. 224) they perform a systematic literature review with an apt methodology, and a thematic analysis of the reviewed works. As a result, authors propose an integrated model of cybersecurity and advocate the role of organization processes in this model.

For their part, Franco, Künzler, von der Assen, Feng & Stiller (2024) developed a metric called "Real Cyber Value at Risk" (RCVaR). It is based on real information from public cybersecurity reports. This information is used in combination with economic methods to predict the costs and risks associated with cyberattacks on companies. This approach provides individualized and quantitative monetary estimates of the impacts of cybersecurity and addresses the limitations of the original CVaR metric, initially proposed by the Cyber Resilience Initiative of the World Economic Forum in 2015. In particular, the RCVaR metric addresses the drawback of probability-based estimates induced by CVaR by conducting cost and risk estimates for real organizations.

The quantification and communication of cyber risk should be carried out through quantitative methods. This idea underlies the work by Bentley, Stephenson, Toscas & Zhu (2020). Their article addresses two specific gaps in literature. The first concerns the lack of use of open data on cyber incidents, while the second concerns the lack of quantitative research on the effect of mitigation strategies. Their first model is therefore adapted to "real-world" data. The authors, in fact, developed a multivariate model that quantifies losses resulting from cybersecurity risks. In specific, this model accounts for different types of attacks and the interdependence between them. Additionally, the authors constructed a second model in this work. This second model aims to separate the frequency and severity of attacks to focus instead on the effect of different mitigations. This approach is extremely useful for professionals and policymakers who wish to optimize mitigation strategies toward specific objectives.

Wang, Neil & Fenton (2020) also propose a quantitative model for cyber risk assessment. In this article, the authors develop an extension of the existing Factor Analysis of Information Risk (FAIR) model (Jones, 2006) to make it more flexible and extensible. The FAIR model alone provides a methodology and tool for calculating and analysing cyber risk. However, the model has limitations in managing causal reasoning for all types of defence-attack contexts and in dealing with different statistical distributions and functions. To address these issues, the authors implemented the FAIR model using Bayesian Networks (FAIR-BN). These networks are known for their broad applicability in probabilistic reasoning. Furthermore, they constructed a combined approach incorporating a process-oriented model and a defence-attack game, called Extended FAIR-BNs (EFBNs). This series of models allowed them to remain consistent and compatible with the original model while providing better insights into the causal mechanisms underlying cyber events and their associated economic consequences.

A further strategy can be found in the guidelines for managers. It is the case of the work of Lee (2021) who develops a cyber risk management instrument. This instrument is organized into four levels, relative to the "cyberecosystem layer" (the external cyber-environment), the "cyberinfrastructure layer" (technological and human aspects of cybersecurity management), the "cyber risk assessment layer" (risk identification, quantification, analysis) and the "cyberperformance layer" (implementation and improvement). The model highlights the need for organizations to understand not only the internal structure of cybersecurity but also the external environment. In this way, the author provides tools for organizations to increase their awareness of changes in cybersecurity trends at the industry level. Consequently, this enables their response strategies to be faster and more efficient. Finally, the author discusses a cyber risk assessment process and provides a real-world example to illustrate continuous performance improvement and cost analysis for cybersecurity.

In conclusion, this section shows that there is a range of works, not extensive but significant, aimed at discussing economic approaches to security evaluation. However, it is important to

emphasize that, within the various specific topics addressed so far, research on the economics of cybersecurity in critical infrastructures remains relatively scarce and scattered across highly differentiated specific topics. This fact must be highlighted given the primary role of critical infrastructures at the societal level. According to Gordon, Loeb, Lucyshyn & Zhou (2015), for example, a cybersecurity breach could shut down an entire sector connected to a critical infrastructure, endangering the entire economy and national defence of a country. This leads us to examine the topic more deeply in the following section.

2.2 Cybersecurity assessment within critical infrastructures

In 2019, the OECD published a report titled Good Governance for Critical Infrastructure Resilience (OECD, 2019). In this report, the OECD defines critical infrastructures as those that enable the delivery of key services in sectors such as telecommunications, energy, water supply, transportation, or finance; these are key systems that represent the "backbone of the functioning of our modern and interconnected societies" (p. 18). The European Union, for its part, defines critical infrastructures as follows: "'critical infrastructure' an element, system or part thereof located in the Member States that is essential for the maintenance of vital societal functions, health, safety, security and economic and social well-being of citizens and whose disruption or destruction would have a significant impact in a Member State due to the impossibility of maintaining such functions.". Additionally, the more restrictive concept of 'European critical infrastructure' or 'ECI' is also introduced, defined as "critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States" (Council Directive 2008/114/EC, 2008). This definition underscores the transnational nature that certain infrastructures can have. Eleven sectors have been identified (energy, transportation, banking, health, drinking water, wastewater, digital infrastructures, public administration, space, and food production, processing, and distribution) whose infrastructures, falling within this definition, will need to be catalogued by 2026. Among these, energy infrastructures are likely to be the most represented on the list due to their wide-ranging impacts.

Cyberattacks on critical infrastructures, if successful, can have repercussions on society as a whole, even at a transnational level, resulting in significant social costs. At the same time, as reported in the previous section, this may not be the case for entities or companies that are not integrated into large-scale networks. To verify whether the scientific literature has addressed this issue, we will now examine studies that focus on the economic evaluation of cybersecurity in the context of critical infrastructures.

The body of literature studying the economic efficiency of measures aimed at making critical infrastructures more resilient is relatively scarce. To address this gap, Rulleau (2023) uses a Discrete Choice Experiment (DCE), conducted through a survey, to evaluate the preferences of residents of the "Eurometropolis" of Strasbourg (France) regarding the resilience of their drinking water distribution network in the event of a cyberattack. Using an econometric model, the author concluded that most respondents positively valued resilience measures aimed at mitigating some effects of cyberattacks. Another important observation is the lack of knowledge and familiarity among the general public regarding the functioning of the drinking water distribution network. This issue, potentially extendable to other critical infrastructure sectors, could compromise the accuracy of the economic evaluation of cybersecurity in these contexts.

On their side, Lis & Mendel (2019) opt for an approach centred on critical infrastructure system operators. The authors emphasize how cybersecurity implementation efforts should aim to ensure the availability, reliability, efficiency, and self-healing of critical infrastructures. As a tool to achieve these objectives, they propose an application of the Return on Security Investment (ROSI) indicator to evaluate the efficiency of cybersecurity efforts within a critical infrastructure. However, they also highlight that the lack of data on cyberattacks prevents the estimation of the costs and benefits associated with such attacks. Additionally, they propose an organizational methodology, "Identify, Protect, Detect, Respond, and Recover" (IPDRR). This methodology is designed to serve as a guide for critical infrastructure providers and policymakers and "consists

of a set of activities and outcomes that are common across the critical infrastructure sector." (p. 38). This framework could also help capture the costs and benefits resulting from cyber breaches. Finally, the authors conclude with a recommendation to implement blockchain technologies to better protect critical infrastructures from cyber threats.

As previously mentioned, the body of literature analysing investment models and cost estimation of cybersecurity in the context of critical infrastructures is not particularly extensive. However, thanks to the interdisciplinary nature of cybersecurity, some studies have approached the problem from other perspectives, such as risk management frameworks (Paté-Cornell, Kuypers, Smith & Keller, 2018; Kure & Islam, 2019). Both works focus on risks quantification rather than cybersecurity value assessment as they stress the importance of systematically identifying and analysing risks and vulnerabilities to protect the organization's key assets.

Addressing another aspect of the economics of cybersecurity in critical infrastructures, Massacci, Ruprai, Collinson & Williams (2016) explored the topic of regulation. To this end, they developed a game theory model that examined the effectiveness of different regulatory systems and the optimal social outcome for public policymakers. This model, linked to public policies on cybersecurity, captures the hybrid nature of regulations for critical infrastructure operators, which vary between risk-based and rule-based systems. The first type of system is based on fines imposed by policymakers in the event of a security breach, leaving operators to decide their own security investment profile. The second, on the other hand, is based on the role of policymakers, who are tasked with conducting a risk assessment and imposing sanctions on operators for non-compliance. The authors clarify that, depending on the combination of incentives, operators might stop investing in cybersecurity and focus solely on compliance (and vice versa). Furthermore, the authors conclude that the maturity threshold of a Critical National Infrastructure Operator (CNIO) is important in choosing the regulatory system. In their view, more mature CNIOs in terms of security should be subject to a risk-based framework, while less secure ones should follow rules.

To summarize, the literature emphasizes the critical importance of cybersecurity measures in ensuring the resilience of critical infrastructures. However, significant challenges remain in quantifying the economic efficiency of such measures, primarily due to the scarcity of representative data on cyberattacks. Regulatory frameworks, through their role in providing risk assessment tools, could help clarify the value of cybersecurity in critical infrastructures.

Since the primary focus of our project is on the specific case of the electricity sector, chapter 4 of this Quaderno IRCrES (Vallette d'Osia, Finardi & Ragazzi, 2025) concentrates on an overview of approaches and methodologies studying the economic value of cybersecurity within that specific sector.

3 CONCLUSIONS

Overall, the reviewed literature highlights that cybersecurity exhibits some features of a public good, creating conditions for market failures such as misaligned incentives, externalities, and information asymmetries. These dynamics justify some form of public intervention. At the same time, the electricity sector provides a particularly complex case: while cybersecurity can be framed as a regulatory concern similar to other dimensions of electricity service (such as service continuity), the design of effective policies is hindered by information asymmetry, a lack of risk awareness, and a lack of a clear regulation typology with accountable and evaluated regulators.

Despite growing recognition of the economic relevance of cybersecurity, contributions that explicitly address the role of cybersecurity in critical infrastructures, and especially in power systems, remain relatively limited. This is notable given the systemic importance of such infrastructures. Furthermore, while the literature emphasizes the resilience benefits of cybersecurity, the economic value of protective measures remains difficult to assess, largely due to limited availability of data on cyber incidents and their impacts.

Taken together, these insights suggest that future research and policy must focus on better integrating economic analysis into the study of cybersecurity in critical infrastructures. This involves not only addressing persistent information asymmetries and data gaps (which could prove impossible in real world conditions) but also exploring regulatory and collaborative approaches that foster innovation, risk awareness, and efficient investment in security. By doing so, the field can move toward a more systematic understanding of the value of cybersecurity and its essential role in safeguarding critical infrastructures.

Table 1. Summary of analyzed studies regarding the economic value of cybersecurity

Study	Approach	Main contribution
Section 2.1. Approaches and models for understanding the economic value of cybersecurity		
Haapamäki & Sihvonen (2019)	Systematic literature review	Focus on accounting, identifies a framework made of 4 research themes: cybersecurity and information sharing, investments in cybersecurity, internal audits and cybersecurity controls, disclosure of cybersecurity activities, and security threats and breaches.
Kianpour, Kowalski & Øverby (2021)	Systematic literature review	Critical assessment of the literature on economics of cybersecurity, under 4 approaches: financial analysis, microeconomics, managerial approaches and combinatorial approaches. Cybersecurity is an interdisciplinary field evolving towards dynamic and generalizable models.
Ghadge, Weiß, Caldwell & Wilding (2019)	Systematic literature review	This work investigates cyber risk management in supply chain contexts and develops a conceptual model of cybersecurity. Authors advocate raising risk awareness, standardized policies, collaborative strategies and empirical models for creating supply chain cyber-resilience.
Nagurney & Nagurney (2015)	Game theory model	Authors build a model applicable in cases of security information asymmetry which provides the equilibrium product transactions between sellers and buyers (on the Internet), and the security levels of the sellers.
Dash, Sarmah, Tiwari, Jena & Glock (2024)	Game theory model	This paper explores the possible connections between different types of cyberattacks, the interconnected nature of companies, and the role of mandatory cybersecurity insurance. The results confirm that optimal levels of cybersecurity investment are higher in the case of targeted attacks, compared to opportunistic ones.
Franco, Künzler, von der Assen, Feng & Stiller (2024)	Quantitative metric, "Real Cyber Value at Risk"	The authors predict the costs and risks associated with cyberattacks on companies. This approach provides individualized and quantitative monetary estimates of the impacts of cybersecurity and addresses the limitations of the original CVaR metric shift from probability estimations to quantitative data computation).
Bentley, Stephenson, Toscas & Zhu (2020)	Quantitative model for risk assessment	Investigates different types of cyber incidents and the effect of mitigation strategies. The best mitigation strategy depends on whether the objective is to avoid extreme damages or to reduce average losses. The methodology allows for estimating the costs of cyberattacks and provides guidance in selecting the most effective mitigation measures.

Wang, Neil & Fenton (2020)	Quantitative model for risk assessment	Extension of a model that provides a methodology and tool for calculating and analyzing cyber risk. Provides both a methodology and a tool for cybersecurity risk analysis and calculation.
Lee (2021)	Quantitative model for risk assessment	Proposes a cyber risk management framework based on 4 layers (cyber ecosystem / cyber infrastructure / cyber risk assessment / cyber performance), which gives tools for organizations to increase their awareness of changes in cybersecurity trends at the industry level.
Section 2.2. Cybersecurity assessment within critical infrastructures		
Rulleau (2023)	Discrete Choice Experiment	This article presents an assessment of the preferences of individuals regarding the resilience of their drinking water distribution network which is subject to a cyber-attack. The results show: - a lack of knowledge and familiarity with the functioning of the distribution network might compromise the accuracy of economic valuation exercises, - regarding individual characteristics, the main factors influencing choices are linked risk perception, - desirability of mitigating measures against cyber-attacks.
Lis & Mendel (2019)	Return on Security Investment (ROSI) quantitative indicator & organizational risk management framework	Provides a methodology and recommendations to follow for blockchain technologies for critical infrastructure providers and policymakers to capture the costs and benefits resulting from cyber breaches.
Paté-Cornell, Kuypers, Smith & Keller (2018)	Quantitative model for risk assessment	Proposes a general cyber risk analysis framework with its application through three examples (database analysis, smart grid optimization, dynamic software management), showing how to quantify risks and identify optimal mitigation strategies.
Kure & Islam (2019)	Conceptual risk management framework	Focuses on three major aspects of risk management (assets identification, vulnerability, and threat assessment and risk identification) and uses an example from the SCADA system of a power grid.
Massacci, Ruprai, Collinson & Williams (2016)	Game theory model	Discusses the effectiveness of different regulatory systems for critical infrastructure operators and the optimal social outcome for public policymakers.

4 BIBLIOGRAPHY

Al Amosh, H., & Khatib, S.F.A. (2024a). Cybersecurity Transparency and Firm Success: Insights From the Australian Landscape. *Australian Economic Papers*, *64*(2), pp. 189-204. https://doi.org/10.1111/1467-8454.12385

Asllani, A., White, C.S., & Ettkin, L. (2013). Viewing cybersecurity as public good: the role of governments, businesses, and individuals. *Journal of Legal, Ethical and Regulatory Issues*, *16*(1), pp. 7-14.

Bauer, J.M., & Van Eeten, M. J. G. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, *33*(10-11), pp. 706-719. https://doi.org/10.1016/j.telpol.2009.09.001

Bentley, M., Stephenson, A., Toscas, P., & Zhu, Z. (2020). A Multivariate Model to Quantify and Mitigate Cybersecurity Risk. *Risks*, *8*(2), art. 61. https://doi.org/10.3390/risks8020061

Brown, D.P., & Sappington, D.E.M. (2023). D*esigning Incentive Regulation in the Electricity Sector*. [WP-2023-20. Research Brief]. MIT Center for Energy and Environmental Policy Research. https://ceepr.mit.edu/wp-content/uploads/2023/11/MIT-CEEPR-WP-2023-20-Brief.pdf

Buckley, G., Caulfield, T., & Becker, I. (2024). GDPR and the indefinable effectiveness of privacy regulators: Can performance assessment be improved? *Journal of Cybersecurity*, *10*(1), art. https://doi.org/10.1093/cybsec/tyae017

Council of the European Union. (2008). Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance). *Official Journal of the European Union*, L 345, pp. 75-82. http://data.europa.eu/eli/dir/2008/114/oj

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), pp. 13-21. https://doi.org/10.22215/timreview/835

Dacus, C., & Yannakogeorgos, P. A. (2016). Designing Cybersecurity into Defense Systems: An Information Economics Approach. *IEEE Security & Privacy*, *14*(3), pp. 44-51. https://doi.org/10.1109/MSP.2016.49

Dash, A., Sarmah, S.P., Tiwari, M.K., Jena, S.K., & Glock, C.H. (2024). Cybersecurity investments in supply chains with two-stage risk propagation. *Computers & Industrial Engineering*, 197, art. 110519. https://doi.org/10.1016/j.cie.2024.110519

Franco, M.F., Künzler, F., Assen, J. von der, Feng, C., & Stiller, B. (2024). RCVaR: An Economic Approach to Estimate Cyberattacks Costs using Data from Industry Reports. *Computers & Security*, 139, art. 103737. https://doi.org/10.1016/j.cose.2024.103737

Ghadge, A., Weiß, M., Caldwell, N.D., & Wilding, R. (2019). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal*, *25*(2), pp. 223-240. https://doi.org/10.1108/SCM-10-2018-0357

Gordon, L.A., Loeb, M.P., Lucyshyn, W., & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*, *1*(1), pp. 3-17. https://doi.org/10.1093/cybsec/tyv011

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, *34*(7), pp. 808-834. https://doi.org/10.1108/MAJ-09-2018-2004

Jones, J. A. (2006). An Introduction to Factor Analysis of Information Risk (FAIR). *Norwich University Journal of Information Assurance (NUJIA)*, *2*(1).

Kianpour, M., Kowalski, S. J., & Øverby, H. (2021). Systematically Understanding Cybersecurity Economics: A Survey. *Sustainability*, *13*(24), art. 13677. https://doi.org/10.3390/su132413677

Kianpour, M., Kowalski, S.J., & Øverby, H. (2022). Advancing the concept of cybersecurity as a public good. *Simulation Modelling Practice and Theory*, 116, 102493. https://doi.org/10.1016/j.simpat.2022.102493

Kure, H.I., & Islam, S. (2019). Assets focus risk management framework for critical infrastructure cybersecurity risk management. *IET Cyber-Physical Systems: Theory & Applications*, *4*(4), pp. 332–340. https://doi.org/10.1049/iet-cps.2018.5079

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, 64(5), pp. 659–671. https://doi.org/10.1016/j.bushor.2021.02.022

Leszczyna, R. (2019). *Cybersecurity in the Electricity Sector: Managing Critical Infrastructure*. Springer International Publishing. Cham. ISBN:978-3-030-19538-0. https://doi.org/10.1007/978-3-030-19538-0

Li, W., Li, Z., Li, W., Zhang, Y., & Li, A. (2023). Mapping the Empirical Evidence of the GDPR's (In-)Effectiveness: A Systematic Review. *Available at SSRN*: http://dx.doi.org/10.2139/ssrn.4615186

Lis, P., & Mendel, J. (2019). Cyberattacks on Critical Infrastructure: An Economic Perspective. *Economics and Business Review*, *5*(2), pp. 24-47. https://doi.org/10.18559/ebr.2019.2.2

Massacci, F., Ruprai, R., Collinson, M., & Williams, J. (2016). Economic Impacts of Rules-versus Risk-Based Cybersecurity Regulations for Critical Infrastructure Providers. *IEEE Security & Privacy*, *14*(3), pp. 52-60. https://doi.org/10.1109/MSP.2016.48

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. International *Journal of Critical Infrastructure Protection*, *3*(3-4), pp. 103-117. https://doi.org/10.1016/j.ijcip.2010.10.002

Mulligan, D. K., & Schneider, F. B. (2011). Doctrine for Cybersecurity. *Daedalus*, 140(4), pp. 70-92. https://doi.org/10.1162/DAED_a_00116

Nagurney, A., & Nagurney, L. S. (2015). A game theory model of cybersecurity investments with information asymmetry. *NETNOMICS: Economic Research and Electronic Networking*, *16*(1-2), pp. 127-148. https://doi.org/10.1007/s11066-015-9094-7

OECD. (2019). *Good Governance for Critical Infrastructure Resilience*. OECD Reviews of Risk Management Policies, OECD Publishing, Paris. https://doi.org/10.1787/02f0e5a0-en

Paté-Cornell, M.-E., Kuypers, M., Smith, M., & Keller, P. (2018). Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies. *Risk Analysis*, *38*(2), pp. 226-241. https://doi.org/10.1111/risa.12844

Ragazzi, E., Stefanini, A., Benintendi, D., Finardi, U., & Holstein, D. K. (2020). *Evaluating the prudency of cybersecurity investments: Guidelines for Energy Regulators*. Washington DC: NARUC.

Rulleau, B. (2023). Household preferences for cyber-attack resilient water distribution networks: A latent class analysis of a discrete choice experiment in France. *Water Resources and Economics*, 43, art. 100230. https://doi.org/10.1016/j.wre.2023.100230

Taddeo, M. (2019). Is Cybersecurity a Public Good? *Minds and Machines*, *29*(3), pp. 349-354. https://doi.org/10.1007/s11023-019-09507-5

Vallette d'Osia, J.M.C., 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. 25-43). Quaderni IRCrES 24. CNR-IRCrES. http://dx.doi.org/10.23760/2499-6661.2025.24_02

Wang, J., Neil, M., & Fenton, N. (2020). A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. *Computers & Security*, 89, art. 101659. https://doi.org/10.1016/j.cose.2019.101659

Chapter 2
Digital sovereignty: a new perspective focused on data control

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

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
Assessing data preferences is challenging, since digital privacy is often perceived as a fundamental societal need or right, rather than a good with an assignable market value. "Digital sovereignty: a new perspective focused on data control" is the second chapter of the Quaderno IRCrES *Cybersecurity and data protection in the electricity sector: state-of-the-art of the literature and evaluation methods* presents a literature review of studies that aim to evaluate individuals' digital privacy preferences in order to address the topic of digital sovereignty, which is closely linked to cybersecurity as it encompasses the procedures that make the digital environment more secure. Specifically, this section of the volume seeks to clarify the key concepts and definitions underlying digital sovereignty, while also reviewing the current state of research on the evaluation of personal data. We examine the challenges, such as behavioural and cognitive biases, as well as context-specific factors, that hinder the users' ability to assess their privacy and risk preferences, leading to a discussion of what the literature has identified as the Privacy Paradox.

KEYWORDS: Digital sovereignty, data privacy, data preferences, privacy paradox, behavioural biases.

DOI: 10.23760/2499-6661.2025.24_02
ISBN: 978-88-98193-39-4
ISSN (online): 2499-6661

HOW TO CITE
Vallette d'Osia, J.C.M., 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

1 KEY CONCEPTS AND BEHAVIOURAL ECONOMICS: HOW IS DIGITAL SOVEREIGNTY PERCEIVED?

The aim of this literature review is to provide an overview of the theoretical and empirical literature on the economics of digital sovereignty, trying to answer the following question: how is digital sovereignty perceived at the individual level, and how can its value be assessed? This first section aims to describe, from an economic perspective, the key concepts and definitions underlying the research theme of digital sovereignty; in order to, in a second stage, support the review of studies that intend to measure it.

1.1 What is digital sovereignty and why is it important for economists?

The European Parliamentary Research Service (EPRS) defines digital sovereignty at the European level as: "Europe's ability to act independently in the digital word and should be understood in terms of both protective mechanisms and offensive tools to foster digital innovation (including in cooperation with non-EU companies)" (Madiega, 2020, p.1). In this way, digital sovereignty includes the notions of data storage, data process and data governance, entailing a regulatory power on the use of data and the access to digital infrastructure. In his book entitled "Sovranità Digitale"[1] (2025), the founder and first director of Italy's National Cybersecurity Agency (ACN), Roberto Baldoni, gives a definition of digital sovereignty at the country level, based on four principles:

- full authority over the data generated by a nation's citizens, government and businesses,
- ability to employ secure technologies and expert workforce,
- existence of international collaborations to proactively address threats, and finally
- awareness and education about risks in cyberspace at the society's level.

With those principles, Baldoni (2025) explains that this definition of digital sovereignty describes a static and ideal situation, while in reality digital sovereignty is a dynamic concept, by being at the intersection of digital, geopolitical and economic transformations. With the gap between a country's actual level of digital sovereignty and the ideal outlined by these principles being its systemic vulnerability to cyberthreats.

In the 2000s, The European Union (EU) faced a major challenge regarding the protection of personal data[2]: the internal market was highly fragmented due to the lack of uniformity among the Member States' legislation on data protection (European Commission, 2010). In order to tackle cross-border data protection matters and revise the existing legal framework, namely the 1995 Data Protection Directive[3] which aimed to harmonize data protection rules at the EU level, the European Parliament and the Council approved the Regulation (EU) 2016/679 in April 2016, creating the well-known General Data Protection Regulation (GDPR)[4].

The GDPR standardizes data protection rules across the EU with guidelines for the collection and processing of personal data. More precisely, it allowed for the establishment of new rights and strengthening of already existing ones in the digital environment, offering more effective

[1] Translated in "Digital Sovereignty"

[2] "'personal data' means 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". G.D.P. Regulation 2016/679, p. 33, Art. 4 (1).

[3] Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

[4] G.D.P. Regulation (GDPR) (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 L 119, p. 1-88).

control of individuals over their own data. One example of an existing right that required clarification is the *right to be forgotten*: the right of individuals to obtain from a data controller the erasure of their personal data without undue delay. Under the GDPR, this right was expanded and explicitly adapted to address the challenges of digital environments. In contrast, the *right to data portability* represents a newly established right: it allows individuals to receive their personal data from an organisation in a commonly used form, enabling them to easily transfer it to another service provider.

This global regulation on data privacy was therefore a requirement to allow people to share their data trustfully and in turn, to make the market for personal data efficient.

Our objective is to explore how the concept of digital sovereignty can be meaningfully applied at a narrower level: the individual one. We aim to understand how individuals' agency over the control of their data can be evaluated. Making an analogy with the above-mentioned principles relating to the concept of digital sovereignty at a nation's level, digital sovereignty for citizens would be a citizen's authority over the data they generate, which includes their ability to employ secure technologies to process their data, supported by a reliable data environment. It also involves their awareness and education about the risks present in the cyber-environment.

Therefore, digital sovereignty for individuals would be citizens' right and ability to have control over their personal data, grounded in the economic notion that data, like any other goods, belongs to the individual, who thus holds the right to use it and benefit from its value.

While they are linked to each other, the notions of digital privacy and digital sovereignty are different, as the former refers to the right to prevent any other entity from accessing personal data without the individual's consent. Digital privacy entails the existence of data protection instruments, from technical instruments such as an antivirus software to legal and regulatory instruments such as the GDPR. In turn, these regulatory instruments enable a data market to exist, giving space for the concept of digital sovereignty to be adapted at the citizen's level. Figure 1 summarizes the links between the two concepts of data privacy and digital sovereignty according to our vision.

To our knowledge, no other study in the current literature has drawn such parallel between digital sovereignty and the individual level. Works attempting to give an economic value to personal data have only focused on measuring digital privacy or data privacy, with those terms used interchangeably. Goldfarb & Que (2023) studied the topic from an economic perspective. They defined digital privacy as a term that "denote(s) a restriction on digital data flows" (p. 268), encompassing the dimensions of costs and benefits of restricting data sharing. More precisely, the authors explained how digital privacy has both an intrinsic and an instrumental value, which in other words means that digital privacy can be seen respectively as a final and an intermediate good. Indeed, sharing data is in itself an action that brings different levels of utility to people (what is considered "disclosable information" differs across individuals) and data holders, but it can also be seen as a mean to protect or hamper other's autonomy. It can do so directly, for instance in cases of sharing a list of contacts, or also indirectly, through a data-generating process (choosing to withhold data already gives market information) or probabilistic information (information about one person can reveal information about others). Thus, data flows present features of public good as they appear to be nonrival (the consumption of the good by one individual does not reduce its availability for others) and difficult to exclude (it is complicated or impossible to prevent others from accessing or using the good): in fact, shared personal information can often be duplicated and accessed by others. These first specific features characterizing digital privacy raise questions about how to adequately assess digital sovereignty from an economic viewpoint. In the following parts of this chapter, the analysis of digital sovereignty at the citizens' level will include a review of the literature that intends to quantify 'personal digital privacy' (or 'personal data privacy') as both notions are used when examining the data market from the individuals' perspective.

In their work on Economics of Privacy, Acquisti, Taylor & Wagman (2016) detailed more precisely the characteristics of privacy under the economic lens. Primarily, digital privacy generates information asymmetry, within an intertemporal scheme. In a first stage, before any disclosing of their personal data, individuals hold more information than service providers, such

as their consumption preferences, creating a first imbalance in the market. In a second stage, upon disclosing personal information, some immediate benefits appear for data subjects, such as for instance gaining a discount in exchange of sharing information. At a third stage, once data holders acquire individuals' information, they might be able to use it in ways not anticipated by data subjects, creating ambiguous and potentially long-term costs for the individuals. This can lead to price discrimination: through the analysis of consumers' purchase or location history, or also browsing behaviours, sharing personal information can become a tool for companies to segment customers, by extracting consumer surplus (the difference between what consumers would be willing to pay for a good and the actual price they pay), and targeting them with different prices.

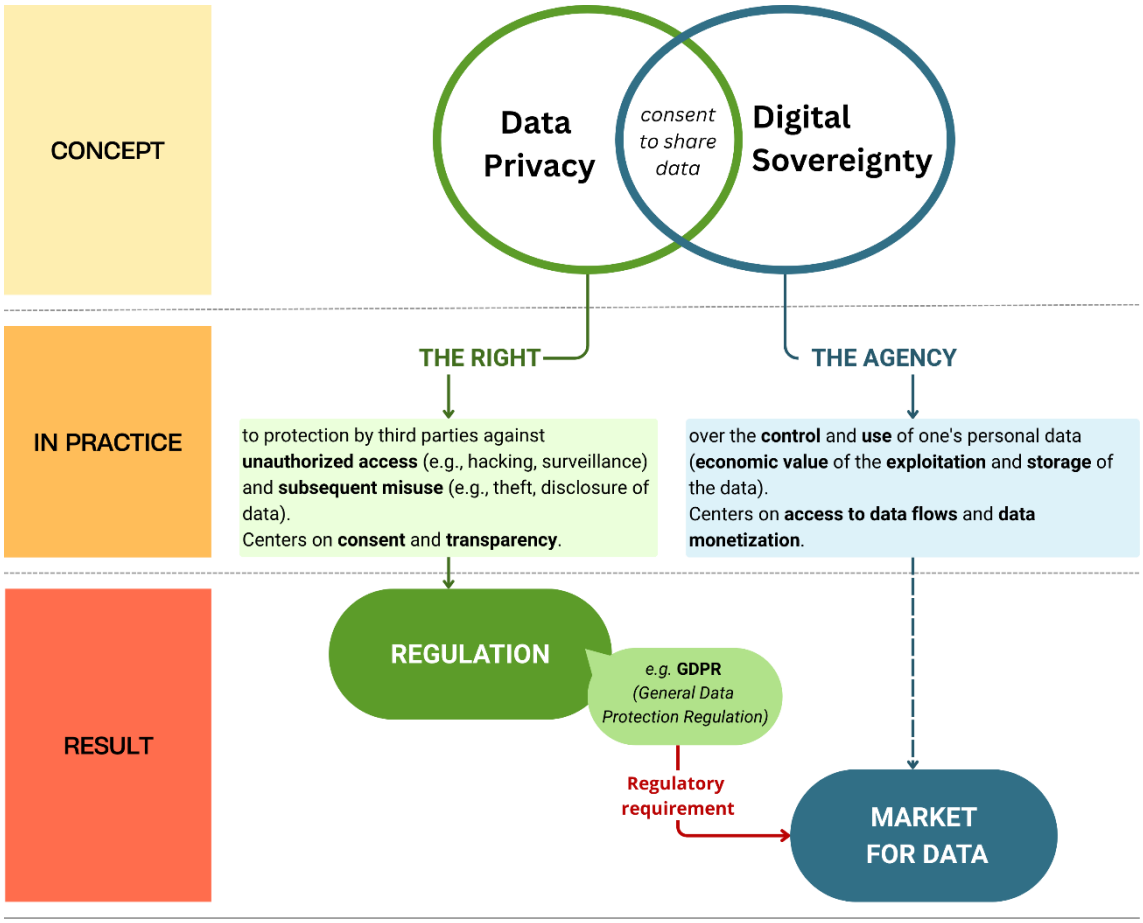
We mentioned the ideas of information asymmetry and intertemporality in disclosing personal data, but another feature described by Acquisti et al. (2016) is the tangibility of privacy trade-offs. The example of getting a discount after disclosing personal information is indeed tangible, but the emotions associated with sharing personal data, or potentially having them exposed, are intangible and add complexity to assessing the value of sharing data.

Furthermore, the authors pointed out a dual dimension behind the multiple definitions of data privacy in the literature: there is the notion of privacy as "control over usage" but also as "protection against access" (Acquisti et al., 2016, p. 449). This has important consequences for valuation, policy implication and regulation design. While control over personal information can protect individuals from the economic leverage that firms may gain by acquiring their data, it can also allow individuals to strategically withhold information to negotiate better prices or discounts. In our attempt to define digital sovereignty for individuals, we thus see this duality behind the notion of data privacy as the difference between data privacy and digital sovereignty, with the *control over usage* of personal data being the concept behind digital sovereignty and *protection against access* being the data protection right, stemming from the notion of data privacy. In this chapter, digital privacy is defined in terms of the disclosure of personal data, therefore studies that explore the consequences of such disclosure are examined. Finally, having defined the characteristics of privacy, Acquisti et al. (2016) demonstrated how trade-offs associated with digital privacy have direct and indirect costs and benefits. As mentioned above, by sharing personal information, data subjects can directly obtain discounts or personalized services. Another kind of benefit lies in the saved opportunity cost: by divulging personal data, people can reduce their search costs and receive more accurate information. Reading the situation from an economic perspective, these benefits become opportunity costs in the case of someone choosing not to disclose its data. This cost-benefit approach enables us to perceive how it may be possible to value digital sovereignty.

To fully analyse digital sovereignty, another important aspect, that of cybersecurity, needs to be considered. Cybersecurity is a tool used to reach digital sovereignty: it enables control over data through the protection against cyber breaches of systems and networks at global level and, in turn, of personal data at narrower levels. Kianpour, Kowalski & Øverby (2021) explained that "cybersecurity deals with the different procedures that create a secure environment by protecting the assets" (p. 3).

In this first descriptive section, we have exposed the complexity behind the economic lecture of digital sovereignty and defined the main concepts bounded to it. In our view, digital sovereignty for individuals refers to the *right and ability of citizens to control and benefit from the use of their personal data*, supported by secure technologies and a trustworthy data environment. It is grounded in the idea that personal data, like any economic good, belongs to the individual. In contrast, digital privacy concerns the *right to prevent unauthorized access* to personal data. While related, the two concepts differ with privacy protecting access and sovereignty empowering usage. Legal and technical data protection instruments such as the GDPR make this distinction effective in practice by enabling individuals to exercise both protection and control.

Figure 1. Conceptual framework of the concepts of Data Privacy and Digital Sovereignty



1.2 Context dependency, cognitive biases and heuristics in privacy decision-making

Building on the definition and characteristics of digital sovereignty, this section explores how individuals' decisions regarding digital privacy are shaped by behavioural biases and contextual factors. While sharing personal data involves complicated trade-offs due to the complex nature of privacy as a good, people's valuation of these trade-offs is often influenced by cognitive biases and specific settings. Understanding these biases, along with the contextual specificity of privacy choices, provides deeper insight into how individuals miscalculate risks related to data privacy and, consequently, possibly incorrectly estimate how much they care about the sharing of their personal data.

An important aspect repeatedly underlined by the literature on the value of digital privacy, is that it is highly context dependent. In a report already published in 2013 entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value", the OECD highlighted the sensitivity of privacy and data valuation to contextual factors, emphasizing that estimations of the monetary value of personal data can differ across scenarios.

To illustrate context-dependency, one can take the common example of individuals who might be willing to share location data for navigation purposes, but would likely withstand disclosing the same information for targeted advertising – not necessarily due to the advertising itself, but due to the discomfort or even anxiety coming from a lack of transparency in how personal data are used to deliver personalized content. This example might be trivial as there are rational reasons explaining it, while other cases might appear more problematic because they are driven by less rational behaviours, such as individuals who may refuse to share the location of their mobile device with their relatives, even though doing so would facilitate finding it when misplaced for instance, while simultaneously consenting to location tracking by online platforms. Behind this

example lies the idea that individuals might fear sharing personal information to people that they know while unknown-online persons might appear to be less threatening.

These examples illustrate how the perceived value of privacy trade-offs is shaped by the purpose of data collection, the identity of the data collector, and the expected use of the data, making privacy valuation variable across different settings.

Bansal, Zahedi & Gefen (2016) empirically tackled the question of context dependency in privacy with a multidisciplinary study. Through an experiment using contextualization of Theory of Reasoned Action ("TRA-privacy") and Prospect Theory, they tested, among others, three hypotheses regarding trust, privacy concern and context sensitivity on disclosing private information. The use of TRA-privacy enabled to study context-related antecedents (personality and experience) of survey-takers and context-specific disclosure of private information, while Prospect Theory provided insights on the utility (or disutility) of individuals to disclose private information, and whether it varies across contexts. More precisely, they compared three contexts in their experiment, using finance, ecommerce and health websites to respectively encompass high monetary context sensitivity, low monetary context sensitivity and sensitive social-based context sensitivity. Their results showed that trust was positively associated with intention to disclose information, with a more significant role in a sensitive social-based context (health) compared to monetary ones (finance and ecommerce). On the contrary, they demonstrated that the relationship between privacy concern and intention to disclose information was significantly negative. Finally, their experiment revealed that privacy concern influenced trust only in sensitive monetary contexts, as the negative relationship between privacy concern and trust was indeed significant in the finance context but not in the ecommerce and health ones. Overall, these findings support the links between trust, privacy concerns and context sensitivity, reinforcing the argument that digital privacy behaviours are highly context-dependent, and therefore difficult to appraise. For what concerns experience, the authors found that previous experience with privacy invasion had an impact on both intentions to disclose and privacy concern. More precisely, they assessed that privacy concern, regardless of context, increased with prior negative experiences of privacy breach. Subsequently, they showed that prior positive experience with a website, especially in ecommerce contexts, had a positive association with intention to disclose data.

Chen, Gu, Wei & Lv (2023) studied the relation between privacy invasion experiences and protection intentions in social media contexts. They validated the hypothesis that prior privacy invasion experiences positively impacted privacy protection intentions. However, they advanced that this relationship was mediated by response costs (any costs such as monetary, time and effort of resulting protective actions) and the phenomenon of privacy fatigue, which they defined as "the complexity of the measures required to protect personal information aggravates user's sense of futility, leading to exhaustion among online users." (p. 2).

In an earlier work, Acquisti, Brandimarte & Loewenstein (2015) published a review entitled "Privacy and human behaviour in the age of information" in which they dug into key themes regarding privacy-related behaviours. Two of these themes are especially relevant for the understanding of context specificity. First, they specified that privacy norms are dictated by culture, time, situation and motivation. To justify this statement, the authors cited studies that looked at individuals' behaviours in diverse contexts, for instance where personal information was either revealed to friends or to strangers (Stutzman, Gross & Acquisti, 2013) or, where individuals were confronted with diverse websites interfaces (John, Acquisti & Loewenstein, 2011), or lastly where individuals were given information about others' behaviours regarding the same survey they had to take (Acquisti, John & Loewenstein, 2012). Results always showed that the group or situation individuals were assigned to was driving their disclosure of information in significative ways, thus underlining the context-dependence of privacy concern. Secondly, Acquisti et al. (2015) raised the topic of uncertainty, regarding both individuals' own privacy preferences and their awareness of what information they are sharing, with whom, and how it might be used. The authors argued that not only when there was information asymmetry, but also when people were aware of the consequences of privacy decisions, individuals were unclear about their privacy concerns and preferences. They detailed that not only social norms, emotions, heuristics, but also the desire for interaction, disclosure and recognition were motives behind

privacy preference uncertainty. By leading people to be undecisive, uncertainty can amplify context-dependence: individuals not being able to clearly identify their privacy preferences would try to detect signals in their environment that would provide them with guidance for privacy choices, making context-dependency even more prevalent.

We now delve into these cognitive, psychological and behavioural biases that distort in multiple ways individuals' uncertainty regarding sharing sensitive information, since other factors than purely contextual ones might worsen the assessment of digital privacy. Indeed, context dependency was mentioned by the authors cited in the previous section, but Goldfarb & Que (2023) also pointed out that not only privacy concerns are dependent on context, but they increase over time, "driven by an expansion of the types of data that consumers consider to be private" (p.270) while Acquisti et al. (2016) underlined that privacy concerns are also inherently diverse, as they take roots in individuals' traits and attributes.

One self-explanatory bias lies in the complexity and overload of data privacy information, also described as bounded rationality (van Ooijen & Vrabec, 2019; Acquisti et al., 2015). In fact, one can easily picture how fragmented and dense is the information about privacy policies, and terms and conditions of the number of websites we visit, mobile applications we download and online services we use in our daily life. To illustrate this, van Ooijen & Vrabec (2019) mentioned a Norwegian campaign-group who exposed that only reading terms and conditions of 33 typical smartphone apps would take nearly 32 hours (Palazzo, 2016). Evaluating what consenting to those terms actually entails would take even more time, creating an additional burden. The same authors, along with Acquisti et al. (2015), quoted another study to illustrate this phenomenon: after analysing 64 online privacy policies of US companies, Jensen & Potts (2004) found that almost half of them were not sufficiently accessible for most Internet users.

Bearing this in mind, another cognitive bias intervenes when accepting terms and conditions or privacy settings. It has been shown in the literature that default settings of websites, apps and other internet services are often interpreted by individuals as implicit recommendations, leading them to accept privacy settings more advantageous for the firm than for themselves (van Ooijen & Vrabec, 2019; Acquisti et al., 2015; Acquisti, Brandimarte & Loewenstein, 2020).

Moreover, Kianpour et al. (2021) mentioned three biases leading to incorrect beliefs about data privacy, namely the "law of small numbers", the "projection bias" and "overconfidence" or "illusory control" (on the topic see Acquisti et al., 2020). The law of small numbers skews perception by making individuals draw broad conclusions from limited experiences, for example, overestimating/underestimating privacy risks due to a lack of personal (or from peers) negative incidents, or overestimating/underestimating the efficacy of certain cybersecurity practices based on anecdotal success stories. Similarly, overconfidence can lead individuals to overestimate their capacity to detect or respond to cyber threats, creating a false sense of control and encouraging riskier behaviour when disclosing personal data. Finally, projection bias causes individuals to assume that their current attitudes and behaviours toward privacy will remain stable over time and are shared by others. Such assumptions can lead to the oversharing of personal data – or to the non-adoption of necessary protections – and to the expectations that others will act similarly, creating a feeling of trust that could be misplaced.

In a more extensive study about consumer privacy decision-making, Acquisti et al. (2020) described additional psychological factors affecting individuals' choices. Among them, the "present bias", the "adaptation bias" and the "drive to share" complexify the ability to align behaviour with long-term privacy interests. Indeed, the present bias leads individuals to prioritize immediate rewards over long-term consequences. As a result, people may willingly share personal data to receive small, short-term benefits, such as online discounts or quicker access to services, while underestimating the lasting and less visible costs, such as intrusive profiling or unexpected targeted advertising based on data profiling. Furthermore, even when the underlying risks of surveillance or data breaches persist or worsen, individuals may become less responsive, perceiving the problem as either unsolvable at their level or no longer urgent, creating an adaptation bias. Lastly, the drive to share reflects the powerful motivational forces behind self-disclosure, particularly in social media contexts. Individuals often disclose personal or even sensitive information online (such as location data) not because they undervalue privacy, but

because competing incentives driven by social connection are perceived as more immediate or emotionally rewarding.

This section detailed how human decision-making regarding personal data disclosure is shaped by psychological, behavioural and contextual factors. With very intertwined and sometimes reciprocal links - uncertainty about which personal data can be safely shared can lead to inaccurate assessments of cyber risks, while, conversely, a lack of clear understanding of those risks can create ambiguity in individuals' digital privacy preferences -, these factors impede the correct appraisal of individuals' data privacy. These factors are therefore the core reason behind what the literature defines as the "privacy paradox", the discrepancy between individuals' stated privacy expectations and data market behaviours, which we will investigate in the following sections. Indeed, we will now review some empirical studies that intend to evaluate data privacy at the individual level, to then examine the privacy paradox that some of them reveal.

2 Economic valuation of Digital Sovereignty: measures of costs and incentives of sharing personal data

This section tackles studies that seek to quantify individuals' perceptions of risk and preferences regarding their personal data. The review will show that valuing (or monetizing) individuals' digital privacy, often operationalized through the act of data sharing, relies mostly on empirical approaches which fall under the umbrella of stated-preference methods in recent literature. Besides, the economic assessment of digital privacy brings up a discrepancy between the desired and realized online privacy decisions, known in the literature as the privacy paradox. We address the discussion surrounding this concept in the last subsection of this chapter.

2.1 Valuation techniques and estimations of data privacy

The definition of privacy valuation we align with in this review is the one stated by Goad, Collins & Gal (2021), which involves the idea of privacy -preference, -concern and -calculus: "Privacy Valuation is the monetary value, which an individual assigns to a Privacy Preference and is essentially one form of quantification of that preference." (p.4), with "Privacy Preference [being] the choice between alternatives as they relate to decisions about controlling information about oneself." (p. 4). As digital sovereignty entails that individuals benefit from the value of their personal data, the idea that there should be a consecutive reward to the consent of sharing personal data must be kept in mind in addition to that of simple protection entailed by digital privacy.

To ensure the relevance and manageability of the reviewed literature, the search was limited to studies employing individuals' valuation methods applied to online privacy, from 2020 onwards. This choice of timeframe has both practical and substantive reasons. Indeed, the literature on the topic appeared in the late 1990's (see for instance Ackerman, Cranor and Reagle, 1999) and grew rapidly along with the importance of online services, leading to a substantial number of publications, impractical to include given spatial and temporal constraints. Moreover, as discussed in the previous section, the valuation of data privacy is highly context-dependent and sensitive to evolving digital environments, norms, and regulatory frameworks. Focusing on recent contributions allows for a more accurate reflection of current user attitudes and market conditions.

This analysis prioritizes individuals' valuation methods over market-based approaches (categories outlined by the OECD, 2013) because this study focuses on consumers' own perceptions of privacy value. Rather than examining the market value of data from a business-model perspective, the aim is to understand how individuals subjectively assess the value of their personal information. Moreover, market valuation methods often fail to account for externalities (Malgieri & Clusters, 2017), a dimension we explicitly aim to capture in this study.

Hence, the following studies all intend to disentangle individuals' awareness, concerns and preferences and in turn attempt to value the protection of privacy online. Among other features, they differ in the online themes and services they observe.

For instance, studies by Blythe, Johnson & Manning (2020) and Goad et al. (2021) were anchored in the concept of the Internet of Things (IoT), focusing on individuals' behaviours towards internet-connected devices, while Jung, Shin & Kim (2025) along with Yamaguchi, Oshima, Saso & Aoki (2020) explored the handling of personal information on social media.

The study by Blythe et al. (2020) focused on the UK and was based on a contingent valuation method (CVM) to measure the willingness to pay (WTP) for improved security in specific connected products (i.e. smart watch, smart thermostat, WI-FI router, smart TV and security camera). Unsurprisingly, the authors observed that consumers would pay more for more secure devices, even though this varies across the type of product under consideration (e.g. respondents cared more about their Wi-Fi Router and Security Camera being secure than their smart TV). More specifically, they found that presenting security-related information prior to asking about people's WTP did encourage consumers to pay more for secure devices, indicating that security information influences purchasing behaviours. However, they assessed whether the WTP was influenced by the relative improvement in security, which turned out to not be the case after testing for both a 50% and a 90% improvement in security afforded: enhancing security itself, regardless of its magnitude, affects individuals' purchasing behaviours.

Controlling for more attributes that affect privacy preferences, Goad et al. (2021), employed a discrete choice experiment (DCE) to their US sample to compute both individuals' WTP for beneficial features that improve privacy and willingness to accept (WTA) infringements on their privacy for a specific connected device: a fitness tracker. In exploring contexts, information type and personal characteristics through the choice tasks they submitted to participants, the authors found that some personal characteristics, namely age and gender, impact privacy preferences and argue for a "right amount of privacy" (p. 14) with a strong variation in WTA according to the type of private information. These findings underline how essential it is to assess the type of information, the context, the individual in question, but also the level of process, procedures and technology operated by organizations prior to deploying privacy solutions.

Though applied to online services in South Korea, the CVM study by Jung et al. (2025) supports similar arguments: sociodemographic features impact the monetary value of people's SNS (social networking services) privacy: "[…] highly educated young adults in their 20s or 30s, on average, put the highest monetary value on SNS privacy" (p. 1106), and SNS users who use platforms for personal purposes such as "friendship" and "self" tend to value their privacy more than those who use them mainly for information sharing. Overall, they estimated the monetary value of SNS privacy at $27.83 (how much participants are willing to accept to disclose their personal information on SNS by accepting a friend request from a marketing firm, which corresponds to how much compensation respondents would accept for the loss of SNS privacy in the paper).

Among other online services categories (such as messaging apps, online news, and search engines), Yamaguchi et al. (2020) also explored data utilization within social media. They used a CVM to uncover the amounts of WTP for data to be utilized or not utilized for the specific service in question, in Japan. Unlike Jung et al. (2025), the authors found that the WTP for social media services was positively associated with data utilization, as well as their internet literacy index. This finding suggests that greater familiarity with the Internet and social media allows individuals to better recognize the benefits of data use, such as the convenience of personalized services and targeted advertisements.

Other studies take a more service-specific approach, embedding privacy trade-offs within clearly defined usage contexts. For instance, Wein (2022) studied German users' preferences toward the artificial intelligence (language translator) DeepL in a controlled online experiment. The author employed control and treatment groups. The control group encompassed participants that could either use DeepL by accepting cookies (thus lowering their privacy) or opt out entirely and not use the service, while the two treatment groups reflected other privacy preferences, as, in addition, they could:

Group 1: choose a privacy-respecting version of DeepL by stating how much they were willing to pay for it (a self-reported WTP greater than zero).

Group 2: vote on whether they would pay a fixed, realistic fee (10€ annually) for a privacy-friendly campus version of DeepL. This group introduced a real market price to better reflect actual privacy preferences.

The author showed that introducing a monetary option for privacy significantly reduced participants' acceptance of cookies, thus giving up their data. In the control group, 79.31% accepted cookies, possibly due to cookie fatigue (dismissing cookie consent pop-ups without fully understanding the implications, potentially compromising privacy and data control), while 20.69% refused to use DeepL out of privacy concerns. In the treatment group with a self-reported WTP option, cookie acceptance dropped to 30.43%, and only 4.35% refused the service entirely. Finally, in the treatment group with a fixed fee for a privacy-friendly version, cookie acceptance further dropped to 27.91%, and just 2.33% refused DeepL altogether. Therefore, introducing a paid alternative for privacy reduced reliance on cookies and encouraged privacy-respecting choices, showing that people are more likely to protect their data when realistic options are available. Another insight was that 35% of the respondents in the self-reported WTP treatment group indicated a WTP less than 10€, suggesting that either their true WTP was indeed lower than 10€ or that they lacked a price reference, supporting the idea that market prices help clarify and reveal privacy preferences.

Similarly grounded in a specific online service, Paliński (2022) examined a ride-hailing service in Poland to estimate individuals' WTA personal data sharing in exchange for fare discounts. Using a DCE estimated with a mixed logit model, and a treatment and control groups as well, being respectively a group with the GDPR notice and one without, the author not only assessed users' readiness to share data for a discount on the final trip cost, but also investigated how awareness of digital rights under the GDPR influenced privacy preferences (for more empirical literature on the specific topic of GDPR's effects, see Goldfarb & Que, 2023 and Zamparini, 2024). The author found that reminding their GDPR rights to participants significantly increased the value they assigned to personal data protection, suggesting that legal awareness, rather than satisfying privacy concerns by giving a sense of control over privacy, seems to amplify them.

Another recent study aimed to measure individuals' WTA data sharing in exchange for a discount, this time using CVM through a five-point Likert-type willingness scale. D'Annunzio and Menichelli (2022) investigated both the willingness to share data for a discount (WSD), with the question "Which of the following types of personal data would you be willing to share to receive a price discount?" (p.578) and the WTP to protect data (WPP), with the question "For which of the following types of personal data would you be willing to pay a monetary price to keep private?" (p.578) in digital markets in Norway. This investigation illustrates how privacy preferences are not uniform but depend on how individuals weigh financial incentives against data sensitivity. Indeed, the study found that WSD (scale-reversed to be compared to WPP) was consistently higher than WPP across all types of personal data. However, the size of the gap between WSD and WPP was larger for highly sensitive data (e.g., credit card numbers, phone call and SMS content, pictures), in comparison with general, less sensitive, data (e.g., age, gender, name), indicating a stronger reluctance to share sensitive data, even for a discount.

Following the same goal to identify differences privacy preferences between data types, Skatova, McDonald, Ma & Maple (2023) examined whether participants in the UK were willing to pay to avoid sharing various types of data across different data sharing environments. They did so through five different evaluation techniques: two different WTP conditions and 3 additional conditions to elicit individuals' preferences to protect different types of data. This method allowed them to uncover whether stated preferences for keeping personal data private are stable within individuals and whether they systematically vary between data sharing environments. The study found that individuals' privacy preferences were stable and coherent across the different elicitation techniques, confirming the existence of well-defined privacy attitudes. However, the authors elicited three tiers of data, with the most valuable one encompassing banking transactions and medical records, while their second (browsing history, mobile phone GPS and social media) and third (electricity use, loyalty cards and physical activity data) tiers remained distinctively below in their ranking scores, which also illustrates the relative importance of protecting different

types of personal data. Goad et al. (2021) elucidated the same finding. In their case, personal health was also considered the most sensitive data type, along with physical location. These results emphasize a practical implication: there is no "one solution fits all" model for privacy concerns.

Cloos & Mohr (2022) also used a scenario-based approach to investigate how people value privacy in different environments. They presented respondents in their experiment with monetary benefits, either personal (treatment group 1) or environmental (treatment group 2), in exchange for data sharing. The environments in which the scenarios were taking place were the following: supermarket, in which data sharing could provide benefits on a loyalty card app; a health insurance company with potential benefits on a tracking bracelet app; the federal ministry of health with a nutrition app; a technology start-up company through a mobility tracking app; and finally, the energy provider with a smart meter app. The results indicated no treatment effects between the groups, but higher acceptance values for data sharing in the applications relatively more familiar to respondents, and among people with stronger green consumption values, higher risk propensity, or younger age show a higher acceptance of data sharing. Therefore, the study shows that acceptance depends more on the recipient of the data and the type of information shared than on the nature of the benefit.

Finally, another interesting characteristic was tackled by Prince & Wallsten (2022), namely a cross-country comparison, revealing significant cultural and contextual differences. Using discrete choice surveys conducted in the United States, Germany, and several Latin American countries (Mexico, Brazil, Colombia, Argentina), the authors estimated the WTA data sharing across various types of personal information (financial, biometric, location, browsing, etc.). They found that Germans valued privacy more than respondents in the U.S. and Latin America, with financial and biometric data being the most highly valued. International differences were even stronger regarding ads: in some Latin American countries, individuals were even willing to pay to receive targeted ads. This cross-national perspective shows that privacy policies should be tailored to national and cultural specificities.

All these empirical studies differed among them in their objectives and implementations, as some used treatment and control groups to test diverse framing effects or incentives, while others embedded privacy trade-offs in varied application environments (e.g., health, mobility, finance). After reviewing them one can validate the theoretical argument we exposed in the first section: *context and individual characteristics have significant roles in shaping privacy preferences and valuations*. Evidence that privacy calculus and valuation are influenced by the type of data, the recipient, and the context of data use was recurrently demonstrated. Moreover, these studies confirm that privacy preferences are neither fixed nor uniform across individuals or situations, rather, they reflect trade-offs between perceived costs and benefits.

Even though all the studies are based on similar measures in order to elucidate individuals' privacy preferences, mainly WTP for privacy or WTA data disclosure, it is important to note that a debate on their validity exists in literature. Winegar & Sustein (2019) intended to elucidate the disparities between WTP to maintain privacy and WTA to allow access to personal data, and they argued that "because of a lack of information and behavioural biases, both […] measures are unlikely to be reliable guides to the welfare effects of retaining or giving up data privacy." (p. 18). However, one limitation of their study is that it relied on directly asking participants to assign monetary value to their privacy, which is a task that can be difficult without prior experience. Eliciting economic value through responses to specific scenarios (thanks to DCE for instance) may yield more reliable results.

In addition, another theoretical aspect is worth underlining here. As explained by Prince & Wallsten (2020), measures of benefits of privacy protections cannot be interpreted as the net value of privacy. They take a practical example to illustrate this idea: they estimated consumers' value for keeping location data on a smartphone at $1.20, with the assumption that keeping location data private lowers accurate driving directions and concluded that "the net benefits of requiring smartphones to keep location data private would, therefore, be $1.20 minus however much people value high-quality directions on their phones." (p. 32).

Finally, one last theme repeatedly emerged in the above literature: the apparent gap between individuals' stated privacy concerns and their actual behaviour (Yamaguchi et al., 2020; Blythe et al., 2020; Goad et al., 2021). This discrepancy, known as the privacy paradox, will be the focus of the next section.

2.2 The discussion around the Privacy Paradox

The review of the literature on data privacy and its economic valuation reveals the ongoing debate about the so-called privacy paradox. Some authors argue for an irrational inconsistency in the privacy behaviours in comparison with people's stated preference (Yamaguchi et al., 2020), which concretely translates in "individuals [who] would indicate a higher preference for privacy than they would reveal in their everyday actions." (p. 4-5, Goad et al., 2021). Others argue that this discrepancy is better explained by bounded rationality and context-dependent cost-benefit reasoning, framing it as a "trade-off" rather than as a paradox (Wottrich, Van Reijmersdal & Smit, 2018). Finally, some scholars reject the notion entirely, claiming that the paradox is a myth as privacy attitudes and behaviours are incomparable (Acquisti et al., 2015; Solove, 2021). We delve into this discussion and analyse the studies that have been tackling this debate.

Multiple works have aimed to review the literature in order to disentangle the different explanations behind the privacy paradox, all taking roots on the one carried by Kokolakis (2017) (Bart & de Jong, 2017; Gerber, 2018; and Zamparini, 2024). The strategy of the initial study by Kokolakis (2017) was to review literature that supports or challenges the existence of a dichotomy between attitudes and behaviours, thus screening the debate around the privacy paradox. The author identifies three major limitations that undermine the privacy paradox as a fully robust theoretical construct: (1) contextual variability across studies, (2) inconsistent conceptual definitions, and (3) methodological disparities in research design.

We already elucidated in the previous section that the valuation of digital privacy is highly dependent on the context it is embedded in, which often leads to inconsistencies in stated preferences and realized intentions in privacy online. Kokolakis (2017) presented the example of a study that took place in a classroom, which can be classified as a familiar environment that probably led respondents to underestimate the risks of sharing personal information. In addition, the author emphasized that studies often examine different categories of personal information (e.g., demographic data, online behaviour, sensitive beliefs), which may not be directly comparable. They similarly highlighted how privacy concerns vary across three types, organizational threats (e.g., data misuse by companies), social risks (e.g., stalking), and unauthorized access by employers or the public, and therefore influence attitudes and behaviours to differing degrees.

For what concerns the theoretical background regarding research on the privacy paradox, Kokolakis (2017) provided a comprehensive review by listing five research themes: a) privacy calculus theory; b) social theory; c) cognitive biases and heuristics in decision making; d) decision making under bounded rationality and information asymmetry; and e) quantum theory homomorphism. In doing so, the author demonstrated that findings must always be interpreted in light of the researcher's underlying assumptions, which are shaped by their disciplinary lens (i.e., social theory, behavioural economics, psychology…). For instance, studying the privacy paradox as a trade-off, as argued under the privacy calculus theory, might lead to different conclusions than if it was studied under the scope of cognitive biases and heuristics, as the latter refutes the assumption of the former that individuals make privacy decisions as rational agents (see Section 1.2).

In a similar way, Bart & de Jong (2017) carried out a systematic review on the topic as well, with a focus on mobile computing, and considered online user's decision making under different lenses: (a) rational risk-benefit-calculation, (b) biased risk-benefit calculation and (c) no or only negligible risk consideration. These categories explain issues of information privacy and, in turn, the privacy paradox as, again, either rationality or influenced behaviour biases are reflected in the

results. The authors argued for mobile applications with mixed approach and design solutions adapted to different cognitive styles.

Methodological choices also matter in testing the presence of a privacy paradox. Kokolakis (2017), after observing that the most common approaches are surveys and experiments, concluded that experimental approaches used to address the validity issues did not recreate realistic contexts (e.g., studies were usually based on online questionnaires or convenience samples that were less robust than studies with factual data collected from a representative samples).

Gerber, Gerber & Volkmaer (2018) also agreed on methodological considerations explaining the privacy paradox. Their literature review, which identified the significant factors that predict privacy aspects, also assessed the theoretical privacy paradox explanations. About the methodological challenges, they underlined a strong limitation to many studies as behaviour was often assessed as a dichotomous answer while attitudes were measured on metric scales. They also dedicated a section of their paper to the assessment of predictors for different privacy aspects. In the first place, they showed that attitude towards privacy was studied through different variables, such as privacy attitude, privacy concerns or perceived privacy risk while intention and willingness to disclose data were used to assess privacy intentions, and privacy related behaviours were elucidated through disclosure of information, the actual usage of data sharing applications, the management of privacy settings and the performance of privacy protection behaviour. The multiplicity of predictor variables reflects the challenges in interpretability when debating the privacy paradox. Secondly, they observed that 'the privacy calculus' was the best approach, with 'gained benefits from disclosing data' being the best predictor for privacy behaviour (both for disclosing intention as well as actual disclosure) and the best predictor for privacy attitudes being internal variables like trust towards the websites, privacy concerns or computer anxiety.

However, two other works (Skatova et al., 2023; Glasgow, Butler & Iyengar, 2021) took into consideration these methodological challenges, trying to justify a potential privacy paradox, without finding significant results.

As mentioned in the previous section, Skatova et al. (2023) employed five different elicitation techniques, including WTP and various ranking methods, to examine whether individuals' preferences for protecting data were consistent across contexts and methods. In their cases, findings showed that rankings of data sensitivity were consistent across elicitation methods for most participants, particularly for highly sensitive data like banking or medical records. These results challenged the notion of a privacy paradox by demonstrating that people do have stable and structured privacy preferences. In addition, they supported the use of stated preference evaluation techniques as an appropriate methodological approach for uncovering people's underlying privacy preferences.

Glasgow et al. (2021) investigated whether survey methodology could explain the privacy paradox by comparing between-subject and within-subject designs in a discrete choice experiment based on hypothetical ride-hailing services. Contrary to their expectation, the results showed no statistically significant difference in privacy valuations between the designs. Notably, the within-subjects approach, which explicitly presented location sharing as an attribute in each choice scenario, failed to produce the hypothesized response bias that could have revealed a privacy paradox. The comparable outcomes across both designs suggest that methodological biases in survey design did not fully explain the discrepancy between stated privacy preferences and actual behaviour.

Drawing on the studies of Kokolakis (2017) and Gerber (2018), Zamparini (2024) reviewed theoretical and empirical studies regarding digital privacy, highlighting that privacy as a concept is strongly contextual, evolving over time, and that measuring digital privacy is subject to strong methodological challenges. For instance, the discrepancy between WTP to protect data and WTA compensation to share them reveals that privacy valuations vary significantly depending on the type of data, individual characteristics, and cultural context. He agreed with Gerber et al. (2018) and Kokolakis (2017), by stating that "the digital privacy paradox may be the result of the specific methodology that is used to test this hypothesis" (p. 154). The paper also situated the privacy paradox within the main public regulations on data privacy, such as the GDPR and its economic

effects, which stresses the need to interpret privacy preferences as highly contextual and shaped by institutional and informational environments.

Building on these studies and reviewing the literature on the privacy paradox and its applicable theoretical approaches, we now turn to the privacy calculus framework, identified by Gerber et al. (2018) as the most comprehensive explanatory model. Skatova et al. (2023) and Wottrich et al. (2018) illustrated well this theoretical approach. Indeed, both suggested that inconsistencies in behaviour, such as respondents sharing data despite stating they had a high concern for privacy, reflected trade-offs rather than irrationality. Wottrich et al. (2018) investigated privacy decision-making in the context of mobile app downloads through two online experiments. They framed the discrepancy between stated privacy preferences and actual behaviours as an economic trade-off where individuals weigh the perceived benefits of app use, defined as 'app value' against privacy costs, based on the concepts of "app intrusiveness" and "concerns". Their findings demonstrated that the benefits of using a mobile app significantly increased the likelihood of users' willingness to share data, to a greater extent than app intrusiveness and privacy concerns decreased it, even among users with high privacy concerns.

This highlights the context-dependent nature of privacy choices and illustrates bounded rationality, which refers to users' limited capacity to fully understand and evaluate all relevant information, even when that information is available, potentially leading to suboptimal or inconsistent decisions (Gerber et al., 2018). This study provides evidence that immediate benefits often outweigh privacy concerns, emphasizing that users do not disregard privacy irrationally, but make situational trade-offs.

The fact that Wottrich et al. (2018) argued for bounded rationality and context-dependency, is another common point shared with Skatova et al. (2023). In fact, the latter observed stability and structure in well-defined privacy preferences among their respondents, which suggests that there is not such a thing as a paradox. The thesis of stability of privacy expectations is also supported by Martin (2021) who used factorial vignette surveys to assess the extent and comparative significance of violating consumer privacy norms. First, she investigated the privacy paradox by testing its strong assumption (i.e., individuals give up privacy expectations after disclosure) and weak assumption (i.e., privacy is traded for benefits like better services or discounts). Contrary to these assumptions, her findings revealed that consumers do maintain privacy expectations post-disclosure and weigh how their data is used more critically than often assumed. To test privacy as a core value, the author compared privacy violations (e.g., third-party data sharing) with security breaches (e.g., hacking) and found that consumers perceived both as equally damaging to trust. The study challenges the privacy paradox by showing that users view online tracking and secondary data use as serious trust violations, undermining the notion that they willingly sacrifice privacy for convenience.

Finally, some authors argue that the privacy paradox is a misconception. Since privacy preferences are defined broadly while behaviours are analysed in very specific contexts, conclusions about people's valuation of privacy are impossible to compare to their privacy decisions. Acquisti et al. (2015) argued that privacy attitudes and behaviours should not be expected to be closely related, which Solove (2021) supported by concluding its article entitled "The Myth of the Privacy Paradox" that "[…] the gap between privacy behaviour and attitudes is not an anomaly that should be rectified; the gap exists because the behaviour and attitudes are about different things. The effort to try to align them falters because they cannot be fully aligned." (p. 51).

All in all, the literature on the privacy paradox shows that discussions around it are still ongoing. While some scholars frame it through privacy calculus theory as context-sensitive trade-offs under bounded rationality, others demonstrate stable and structured preferences that challenge the paradox's very existence. Some authors go further in the debate and argue that the paradox is a conceptual misunderstanding stemming from the misalignment between general attitudes and specific behaviours. Overall, the research community faces significant hurdles in drawing conclusions, as authors frequently refer to different constructs (e.g., varying definitions of privacy concerns, disclosure behaviours, and risk perceptions) without a comprehensive explanation. Three critical limitations emerge: (1) methodological inconsistencies, (2) the

heterogeneity of studied data types (from demographic to behavioural data), and (3) the lack of a shared definition of core concepts. Notably, while consumers do engage in privacy trade-offs, they often lack the tools for well-considered, self-regulated decisions, suggesting that design solutions should adapt to diverse cognitive styles. Ultimately, the paradox appears more as conceptual, behavioural and methodological biases, underscoring the need for unified frameworks that capture how individuals actually value and protect privacy across digital contexts.

3 CONCLUSIONS

The examination of literature on data privacy through an economic lens reveals the challenges of valuating individuals' preferences and actual behaviours. Our analysis first establishes the background and context of the literature review by defining the terms and characteristics bounded to digital sovereignty, which has not been yet analysed at the individual level. In a second step, we demonstrated the role of contextual specificities, as well as of behavioural biases. These are for instance the high burden put on cognitive abilities that represents websites' and apps' terms and conditions, or psychological factors like the present bias that overemphasize immediate costs and benefits. These biases distort risk assessments in data privacy decisions, leading to frequent misalignment between stated preferences and actual behaviours, referred to as the privacy paradox. Our review of valuation techniques highlighted the predominance of studies based on the elicitation of willingness to pay (or willingness to accept compensation) for data disclosure, and therefore mainly relying on Discrete Choice Experiments or Contingent Valuation methods. Still, methodological gaps in measuring and modelling privacy aspects remain, with for instance the long-lasting debate on the choice between opting for WTP or WTA. Ultimately, the privacy paradox discussion stemming from the discrepancy between individuals' attitudes or concerns and intentions or behaviours exposes ongoing debates about the frameworks and conceptual definitions to adopt. Yet, seeing the privacy paradox as an economic trade-off seems to be more realistic, making therefore the theoretical approaches based on privacy-calculus best suited to the topic. Together, these findings suggest that current approaches to digital sovereignty must address three dimensions: (1) developing behavioural frameworks that account for cognitive limitations, (2) creating context-sensitive valuation methodologies, and (3) establishing reliable models to resolve validity issues. Digital sovereignty is not merely a technical or legal issue; it necessitates interdisciplinary solutions that connect human decision-making with systemic governance needs.

4 BIBLIOGRAPHY

Ackerman, M.S., Cranor, L.F., & Reagle, J. (1999). Privacy in e-commerce: examining user scenarios and privacy preferences. In *Proceedings of the 1st ACM Conference on Electronic Commerce*, pp. 1-8. https://doi.org/10.1145/336992.336995

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), pp. 509-514. https://doi.org/10.1126/science.aaa1465

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age. *Journal of Consumer Psychology*, *30*(4), pp. 736-758. https://doi.org/10.1002/jcpy.1191

Acquisti, A., John, L. K., & Loewenstein, G. (2012). The impact of relative standards on the propensity to disclose. *Journal of Marketing Research*, 49(2), pp. 160-174. https://doi.org/10.1509/jmr.09.0215

Acquisti, A., Taylor, C., & Wagman, L. (2016). The Economics of Privacy. *Journal of Economic Literature*, *54*(2), pp. 442-492. https://doi.org/10.1257/jel.54.2.442

Baldoni, R. (2025). *Sovranità Digitale: Cos'è e quali sono le Principali Minacce del Cyberspazio Nazionale*. Il Mulino. ISBN: 978-88-15-39238-1

Bansal, G., Zahedi, F.M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management*, *53*(1), pp. 1-21. https://doi.org/10.1016/j.im.2015.08.001

Barth, S., & de Jong, M.D.T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), pp. 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013

Blythe, J.M., Johnson, S.D., & Manning, M. (2020). What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. *Crime Science*, *9*(1), pp. 1-9. https://doi.org/10.1186/s40163-019-0110-3

Chen, S., Gu, C., Wei, J., & Lv, M. (2023). Research on the influence mechanism of privacy invasion experiences with privacy protection intentions in social media contexts: Regulatory focus as the moderator. *Frontiers in Psychology*, *13*(1031592). https://doi.org/10.3389/fpsyg.2022.1031592

Cloos, J., & Mohr, S. (2022). Acceptance of data sharing in smartphone apps from key industries of the digital transformation: A representative population survey for Germany. *Technological Forecasting and Social Change*, *176*(121459). https://doi.org/10.1016/j.techfore.2021.121459

D'Annunzio, A., & Menichelli, E. (2022). A market for digital privacy: Consumers' willingness to trade personal data and money. *Economia e Politica Industriale: Journal of Industrial and Business Economics*, *49*(3), pp. 571-598. https://doi.org/10.1007/s40812-022-00221-5

European Commission. (2010). *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union* (COM/2010/0609 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52010DC0609

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, 77, pp. 226-261. https://doi.org/10.1016/j.cose.2018.04.002

Glasgow, G., Butler, S., & Iyengar, S. (2021). Survey response bias and the 'privacy paradox': Evidence from a discrete choice experiment. *Applied Economics Letters*, *28*(8), pp. 625-629. https://doi.org/10.1080/13504851.2020.1770183

Goad, D., Collins, A.T., & Gal, U. (2021). Privacy and the Internet of Things – An experiment in discrete choice. *Information & Management*, 58(2). https://doi.org/10.1016/j.im.2020.103292

Goldfarb, A., & Que, V.F. (2023). The economics of digital privacy. *Annual Review of Economics*, *15*(1), pp. 267-286. https://doi.org/10.1146/annurev-economics-082322-014346

Jensen, C., & Potts, C. (2004). Privacy policies as decision-making tools: an evaluation of online privacy notices. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, pp. 471-478. https://doi.org/10.1145/985692.985752

John, L.K., Acquisti, A., & Loewenstein, G. (2011). Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of consumer research*, *37*(5), pp. 858-873. https://doi.org/10.1086/656423

Jung, W.-J., Shin, W., & Kim, H.-W. (2025). Estimating the monetary value of personal information on social networking sites. *Electronic Commerce Research*, *25*(2), pp. 1089-1114. https://doi.org/10.1007/s10660-023-09715-3

Kianpour, M., Kowalski, S. J., & Øverby, H. (2021). Systematically Understanding Cybersecurity Economics: A Survey. *Sustainability*, *13*(13677). https://doi.org/10.3390/su132413677

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, pp. 122-134. https://doi.org/10.1016/j.cose.2015.07.002

Madiega, T. (2020). *Digital Sovereignty for Europe* (PE 651.992). European Parliamentary Research Service (EPRS). https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

Malgieri, G., & Custers, B. (2017). Pricing Privacy – The Right to Know the Value of Your Personal Data. *Computer Law & Security Review*, 34, pp. 289-303. https://doi.org/10.1016/j.clsr.2017.08.006

OECD. (2013). *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value* [OECD Digital Economy Papers, No. 220]. https://doi.org/10.1787/5k486qtxldmq-en

Palazzo, C. (2016, 26 may). Consumer campaigners read terms and conditions of their mobile phone apps… all 250,00 words. *The Telegraph*. https://www.telegraph.co.uk/technology/2016/05/26/consumer-campaigners-read-terms-and-conditions-of-their-mobile-p/

Paliński, M. (2022). Paying with your data. Privacy tradeoffs in ride-hailing services. *Applied Economics Letters*, *29*(18), pp. 1719-1725. https://doi.org/10.1080/13504851.2021.1959891

Prince, J. T., & Wallsten, S. (2022). How much is privacy worth around the world and across platforms?. *Journal of Economics & Management Strategy*, *31*(4), pp. 841-861. https://doi.org/10.2139/ssrn.3528386

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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). *Official Journal of the European Union*, L 119, pp. 1–88. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

Skatova, A., McDonald, R., Ma, S., & Maple, C. (2023). Unpacking privacy: Valuation of personal data protection. *PLoS ONE*, 18(5). https://doi.org/10.1371/journal.pone.0284581

Solove, D. J. (2021). The myth of the privacy paradox. *Geo. Wash. L. Rev.*, 89. https://doi.org/10.2139/ssrn.3536265

Stutzman, F.D., Gross, R., & Acquisti, A. (2013). Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of privacy and confidentiality*, 4(2), pp. 7-41. https://doi.org/10.29012/jpc.v4i2.620

van Ooijen, I., & Vrabec, H.U. (2019). Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. *Journal of Consumer Policy*, *42*(1), pp. 91-107. https://doi.org/10.1007/s10603-018-9399-7

Wein, T. (2022). Data Protection, Cookie Consent, and Prices. *Economies*, 10(12).https://doi.org/10.3390/economies10120307

Winegar, A.G., & Sunstein, C.R. (2019). How Much Is Data Privacy Worth? A Preliminary Investigation. *Journal of Consumer Policy*, *42*(3), pp. 425-440. https://doi.org/10.1007/s10603-019-09419-y

Wottrich, V.M., Van Reijmersdal, E.A., & Smit, E.G. (2018). The privacy trade-off for mobile app downloads : The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems*, 106, pp. 44-52. https://doi.org/10.1016/j.dss.2017.12.003

Yamaguchi, S., Oshima, H., Saso, H., & Aoki, S. (2020). How Do People Value Data Utilization?: An Empirical Analysis Using Contingent Valuation Method in Japan. *Technology in Society*, *62*(101285). https://doi.org/10.1016/j.techsoc.2020.101285

Zamparini, L. (2024). Data, digital markets, and the economic value of privacy. *Eastern Journal of European Studies*, *15*(2), pp. 147-164. https://doi.org/10.47743/ejes-2024-0208

Chapter 3
The ESSENCE project: a re-examination guided by emerging academic contributions

CLEMENTINA BRUNO, FABRIZIO ERBETTA

Università del Piemonte Orientale, Dipartimento di Studi per l'Economia e l'Impresa, Via Perrone, 18, 28100 Novara, Italia.

Corresponding author(s): clementina.bruno@uniupo.it

ABSTRACT
Improving power network security against cyber-attacks is paramount. The ESSENCE project evaluated the costs and benefits of implementing security standards, focusing in particular on the benefits of enhanced security, specifically in the form of avoidance of blackouts, intended as a non-market good. Drawing on a comprehensive literature review, we defined a mixed-method approach adopted for two distinct case studies: Italy (generation phase) and Poland (transmission network). For household users, we emphasize the rationale behind a stated preference method utilizing a Willingness-to-Accept (WTA) choice experiment. Conversely, for non-household users (industrial sectors), the utility of a production function approach is highlighted for calculating the Value of Lost Load (VOLL) based on macroeconomic data. Re-examining the ESSENCE project in light of recent literature underscores the vital importance of evaluating diverse and comprehensive outage costs in the assessment of power network security.

KEYWORDS: Blackout damage, production function approach, willingness-to-accept, ESSENCE project.

DOI: 10.23760/2499-6661.2025.24_03
ISBN: 978-88-98193-39-4
ISSN (online): 2499-6661

HOW TO CITE
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

1 ESSENCE OBJECTIVES AND THE VALUE OF SUPPLY SECURITY

The ESSENCE (Emerging Security Standards to the EU power Network controls and other Critical Equipment) project was aimed at evaluating the costs and benefits of the implementation of particular security standards to the electric system. The evaluation was based on two case studies describing hypothetical system failures that, under very particular conditions, can arise as consequences of malicious cyber-attacks. One case study involved the generation phase and focused on Italy, while the other one involved the transmission network and was focused on Poland. (Ragazzi and Stefanini, 2019; Abrate et al., 2016; Bruno et al., 2015; CERIS – CNR RT. 47, 48, 51, 52, 53, 55, 56, 57).

In particular, our team was involved in the benefit evaluation, i.e. facing the complex task of evaluating improved security. As previously discussed in this work, there are some situations, such as the one considered in ESSENCE, in which security shows some features common to other public goods, since it is non-rival, non-excludible and not traded on the market, therefore it cannot be valued on the basis of market prices

Therefore, it required an approach for evaluating non-market goods, which could be suitable for being applied to the electricity sector. A deep analysis of the literature led us in the field of evaluation of the damage deriving from blackouts (the negative consequence of security failure considered in the two case studies), an issue that at that time had been addressed by relying on a variety of methods.

1.1 Which methods in literature fitted our case studies?

A crucial starting point for the choice of a methodology has been represented by the taxonomy proposed by De Nooij et al. (2007). The authors consider approaches deriving from different scientific backgrounds, not necessarily rooted in statistics or econometrics. We considered the advantages and disadvantages of all the discussed methodological categories.

- The revealed preference methods are based on the observation of real users' behavior with respect to power outages. Examples of observable behaviors include investments in back-up facilities or the acceptance to adhere to interruptible contracts, representing choices allowing the researcher to infer information about the value assigned to supply continuity. Unfortunately, such behaviors are observable for very limited consumers' segments.
- The case studies usually consist of listing and quantifying damages or developing a survey immediately after a real blackout. The reference to an actual (not hypothetical) fact improves the reliability of the results, which, however, are difficult to use for evaluating other events of the same nature.
- Stated preference methods rely on micro-data collected through surveys and aim at asking for or eliciting the value of supply continuity (or of failures with the features desired by the researcher) in terms of Willingness-to-Pay or Willingness-to-Accept (WTP or WTA). The main advantage is related to preference information directly collected from the respondents, but we must be aware that responses can be affected by different types of biases of cognitive origin. Particular attention should be given to the framing of the questions.
- Another option is represented by the production function approach. The basic idea relies on the assumption that no productive activity is possible in absence of electricity, therefore the total damage is proportional to the amount of energy non-supplied during the blackout, assuming a constant ratio between GDP or Value-Added measures and the corresponding amount of energy consumed in a given area in a time unit. This approach can be refined by considering non-complete dependence of some activities on electricity, different Value-Added / Electricity ratios in different sectors or input-output matrices for considering interdependencies among sectors. Some authors adapt the approach to individual

consumers or families, by measuring the damage in terms of lost leisure time, for which a value must be determined (usually starting from the salary level in the area). This approach is often classified as a "proxy method", since the computed damage represents, in any case, an approximation, since "non-linearities" are difficult to be included (e.g. long restarting time or damages to equipment).

For examples of applications of the different methods in the literature, see RT n. 52, 55, 56 (2014) CERIS-CNR and Abrate et al. (2016).
In the literature, we can find examples of mixed approaches, such as that provided by Reichl et al. (2013a, b), who rely on a production function approach for the productive sectors (improved by firm surveys) and on a stated preference methodology for households.
A mixed approach, as we will illustrate later on, has been judged to be the best option also for ESSENCE. The reasons leading to this choice relate to the nature of the project, that required to evaluate hypothetical blackouts, and to cover the largest possible set of user categories. The production function approach was judged as sufficient to account for the damage suffered by the productive sector, which is mainly of economic and productive nature, with the advantage of relying on secondary (macroeconomic) data, thus avoiding the issue of direct data collection from firms, a segment likely to show relatively low response rates to surveys. The stated preference method, instead, has been found to be suitable for household users, since in this case a relevant source of damage (probably, the main one) is not monetary, but is of social or psychological nature.

Table 1. Advantages and disadvantages of the considered methods

Methodology	Advantages	Disadvantages
Revealed preferences	Based on observable market behavior.	The relevant market choices involve very narrow consumers' segments.
Case study	Damage quantified after observing a real event.	It is very difficult to rely on the results for evaluating other blackouts.
Stated preferences	Damage value directly inferred from the preferences declared by consumers. Can be adapted to hypothetical events.	Potential bias of cognitive origin. The framing of the questions is relevant.
Production function	Relatively easy to apply (also for hypothetical events), once secondary macro-level data are available.	The estimated damage represents a proxy of the total one.

Source: our elaboration from De Nooij et al. (2007) and RT. 52, 55, 56 (2014) Ceris-CNR.

1.2 Outage costs: ideas from a subsequent study.

An interesting contribution by Ericson and Lisell (2020) identifies some dimensions that determine outage costs (p. 97).

- Magnitude, in terms of lost load (which is considered by the largest part of the contributions on this theme).
- Perspective, identifying the subject (individual or entity) that is involved in the blackout;
- Timing of the outage.

- Duration of the outage.
- Advanced warning (or not).

Interestingly, the authors develop an approach aimed at including all the possible damage sources, and identify three cost components:

- Fixed costs, not depending on the outage duration (e.g. data losses or damages to equipment).
- Flow costs, depending on the lack of energy, which can increase, decrease or remain stable over time depending on the ability of users to cope with the outage (e.g. by moving workers to non-energy-dependent activities).
- Stock costs, depending on spoilage of materials, expiration of obligations or even vandalism.

The authors include in the cost categories also damages to households or particular sectors such as health care.

2 CONCEPTUAL FOUNDATIONS OF THE METHOD FOR THE ASSESSMENT OF THE COST OF THE BLACKOUT FOR HOUSEHOLD USERS

As regards household users, the assessment has been thought about as based on the impact on the daily living activities. In this respect a stated preference method has been identified as the most suitable. In this context, two approaches could be used: the measurement of the willingness to pay (WTP) to avoid a blackout and the measurement of the willingness to accept (WTA) a blackout. The two approaches are based on a different conceptual framework. The first implies the willingness of users to pay an amount of money to avoid the adverse situation, while the second implies the willingness to accept that the adverse event occurs in exchange for a compensation (in ESSENCE, a discount on the bill). While the first approach seems conceptually based on the behavioural assumption of non-industrial users that the departure from a status quo is always undesirable, the second is based on the more contingent logic that users pay to have the guarantee of a service and may not be a priori willing to pay an extra-amount to avoid a non-tolerated disservice. Rather, they may be more inclined to think in terms of discount when faced with the acceptance of a negative event.

Actually, such a decision is not trivial, since the literature demonstrates that the two approaches usually lead to different value quantifications, with WTA providing larger (in some cases, much larger) values than WTP, due to some anomalies characterizing consumers choices, such as the endowment effect, the status quo bias and, in general, the loss aversion issue (Kahneman et al., 1991).

A recent study by Koń and Jakubczyk (2019) suggests that, especially in the past, the disparity between WTP and WTA has been overestimated in the literature, for the presence of publication bias. In fact, it is the authors' opinion that in the past it was easier to get published for studies that suggested large differences between the two measures; on the contrary, studies finding similar WTA and WTP measures could be considered as less appealing and therefore less accepted, or even less submitted, for publication, thus being underrepresented in literature.

However, recent studies also confirm a disparity between WTP and WTA, such as Frondel et al. (2021), with a study based on supply security, although the authors find that the disparity reduces if the evaluation setting is perceived as more realistic. Koetse and Brouwer (2016), focusing on environmental goods, verify that a disparity between WTA and WTP does exist, increases with the distance from the reference point, and depends on the reference point itself. However, the authors conclude that "WTA values which are obtained from studies that assess a different range of possible changes, and that use a different reference value than is the case for the specific welfare analysis, may overestimate a welfare change" (p. 744). Furthermore, WTP could, instead, lead to underestimation issues. The authors suggest the need to rely on approaches specific to the considered case studies. In addition, Nguyen et al. (2021) sustain that "Many,

perhaps most, interventions [...] appear disproportionately to be more likely to be regarded as remedial and therefore as reductions of losses rather than gains and, consequently, to call for WTA measurements" (p.631).

Weighing the two approaches (WTP and WTA), although the first is closer to a behavioural vision based on risk aversion, the second appears close to a more contingent logic and seemed therefore more suitable for setting up a survey designed for a sample of household users asked to evaluate a single interruption, which is likely to be intended as a welfare loss with respect to a service that is assumed to be continuous.

The choice of relying on WTA, in ESSENCE, appears therefore supported also in the light of subsequent contributions. First, it is advisable to frame the choice set properly, and WTA appears the most suitable indicator for a welfare loss such as a blackout, since WTP could lead to underestimating the damage. Second, the difference between the two measures could be less dramatic than expected. Third, our choice experiment evaluated exactly scenarios corresponding to the blackouts considered for the case studies, thus limiting the risk of overestimating the damage.

3 THE METHOD FOR THE ASSESSMENT OF THE COST OF THE BLACKOUT FOR NON-HOUSEHOLD USERS

As regards the second category of users, the "production function" approach was used. This approach, using data available at the macro level (for example, by industrial sector), is based on the measurement of the value added per unit of energy at industry level and, therefore, of the amount of the value of the load lost (VOLL) in the event of no energy supply due to the blackout. By multiplying the VOLL by the amount of energy lost, it is possible to provide an estimate of the industrial damage for the sector in question and for the economic system as a whole.

It's worth noting that estimations of blackout costs at the industrial level are prudential (or conservative) as they are based on the assumption of a linear relationship between energy consumption and production (simulations accounting for non-complete energy dependence are also provided). In reality, however, other sources of damage can affect the productive sector. Indeed, costs deriving from damage are of a diverse nature, and—besides loss of consumption goods—might include costs due to breakage of machinery or internal electrical lines, or costs for reactivation of lines, up to serious damages that make production lines unusable beyond repair.

4 DATA, RESULTS AND CONCLUSIONS

As regards the evaluation of the blackout cost for household users, our chosen methodology was implemented via a choice experiment. Within this framework, participants were presented with choice questions designed to elicit their willingness to accept (WTA) blackouts of predetermined durations, contingent upon a compensation from their electricity supplier in the form of a bill discount.

Recognizing the infrequent occurrence of such scenarios in typical residential settings, the questionnaire was meticulously structured to progressively familiarize respondents with the problem. This gradual introduction aimed to induce comprehensive reflection on the potential ramifications of an electricity interruption on household life. Regarding the core choice experiment component, respondents were directly queried on their acceptance or rejection of a specified blackout duration, provided a corresponding bill discount. Consequently, the choice sets were deliberately simplistic, comprising only two alternatives: 'Acceptance of the blackout given a certain discount' and 'No interruption and no discount'. Thus, each blackout scenario was characterized by two salient attributes: its duration and the proposed discount level.

A total of 28 distinct scenarios (representing combinations of duration and discount) were formulated, based on the following parameters:

- Four duration levels: 1 minute, 2, 4, and 6 hours.
- Seven discount levels: 1, 7, 13, 19, 25, 31, and 37 euros.

The presentation of all 28 choices was deemed potentially burdensome, posing a risk to data quality and respondent engagement. To mitigate this, scenarios were randomly partitioned into 7 blocks of 4. Each respondent was subsequently exposed to only one randomly selected scenario from each block, resulting in a total of 7 scenarios per respondent.

Other variables of interest are: the age category, the gender, the income level, the education level, the zone type (if urban or non-urban) and the average monthly electricity bill.

Our analysis assumes that the probability of a respondent choosing a particular blackout scenario, and thus the associated utility, is a function of several key factors: the blackout characteristics themselves, the respondent and household characteristics.

For non-industrial users, the average cost of a 15-minute blackout is estimated at €2.86 for Italy. This figure varies, ranging from a minimum of €1.79 to a maximum of €3.34, depending on other user-specific attributes. As expected, the average cost increases significantly for longer outages; a 6-hour blackout results in an average cost of €43.04 for Italy (€62.65 for Poland), with a range between €32.43 (€35.31) and €54.57 (€73.46).

The results are similar in terms of order of magnitude but differ among the two countries. In addition, even in the same area, results are likely to change over time: Carlsson et al. (2021) find relevant WTP changes in two blackout evaluations of Swedish households carried on in 2004 and 2017 respectively (for instance, an unplanned outage of 1 hours showed a mean value 12.9 SEK in 2004 and 29.02 SEK in 2017; the same values are about 47 vs 107 SEK for 4 hours; the values are in constant 2017 prices).

As regards the determination of the VOLL for non-household users, the data used were the levels of value added at territorial level (from ISTAT source, up to 2008) and the data on distributed energy over the same period (from Terna, the Italian TSO). For Poland, the data on total gross value added were published by the Statistical Office in Warsaw, while data on total consumption were provided by the City of Warsaw, Infrastructure Department. The average VOLL calculated for the entire production system in Italy is 5.92 €/kWh (7.58 €/kWh for Poland). For comparison purposes, we can for example observe that these values are consistent with the results of Linares and Rey (2013) for Spain (5.56 €/kWh) or of De Nooij et al. (2007) for the Netherlands (7.59 €/kWh).

Notice that, for both case studies (Italian and Polish), the blackout characteristics were precisely defined in terms of lost load, time of the day, day of the week and duration. In addition, the blackout has been defined as unexpected. Both the methodologies adopted (stated preferences and production function approaches) are also able to differentiate the damage among user's types. We are therefore confident that all the relevant determinants later suggested by Ericson and Lisell (2020) have been accounted for, acknowledging that the estimation of damage at the industrial level is conservative as it does not account for non-linearities between energy consumption and production. With respect to the stated preference approach, the evaluation of damage is specifically referred to our case studies; however, as suggested by Frondel et al. (2021) and Carlsson et al. (2021), the results are often context-dependent (in temporal and geographical perspectives). Thus, for cost-benefit analysis purposes, we suggest relying on context-specific evaluations.

5 BIBLIOGRAPHY

Abrate, G., Bruno, C., Erbetta, F., Fraquelli, G., & Lorite-Espejo, A. (2016). A choice experiment on the willingness of households to accept power outages. *Utilities Policy*, 43, pp. 151-164.

Angeletti, V., Guidi, L., Pestonesi, D., Biancardi, M., Alessi, M., Abrate, G., Bruno, C., Erbetta, F., Fraquelli, G., & Lorite-Espejo, A. (2014) *Italian Case Study: socio-economic impact*

analysis of a cyber attack to a power plant in an Italian scenario. Cost and benefit estimation of CIPS standard adoptions. A reduced version. Ceris-CNR RT. 55. http://essence.ceris.cnr.it/images/documenti/RT_55.pdf

Bartoszewicz-Burczy, H., Bruno, C., García, F., & Włodarczyk, T. (2014). *Polish case study. Scenario based assessment of costs and benefits of adoption of comprehensive CIP standards*. Ceris-CNR RT. 56. http://essence.ceris.cnr.it/images/documenti/RT_56.pdf

Bruno, C., Abrate, G., Bartoszewicz-Burczy, H., Cortes, A., Diu A., Doheijo, E., Erbetta, F., Falavigna, G., Finardi, U., Fraquelli, G., Guidi, L., Lorite-Espejo, A, Moiso, V., Pestonesi D., Ragazzi, E., & Wlodarczyk, T. (2014). *Benefit analysis. Assessing the cost of blackouts in case of attack. Evaluation based on Italian and Polish case studies*. Ceris-CNR RT. 52. http://essence.ceris.cnr.it/images/documenti/RT_52.pdf

Bruno, C., Guidi, L., Lorite-Espejo, A., & Pestonesi, D. (2015). Assessing a potential cyberattack on the italian electric system. *IEEE Security & Privacy, 13*(5), pp. 42-51.

Calabrese G., Finardi U., & Ragazzi, E. (2014). *Cost analysis of standard implementation in the SCADA Systems of electric critical infrastructures*. Ceris-CNR RT. 53. http://essence.ceris.cnr.it/images/documenti/RT_53.pdf

Carlsson, F., Kataria, M., Lampi, E., & Martinsson, P. (2021). Past and present outage costs – A follow-up study of households' willingness to pay to avoid power outages. *Resource and Energy Economics*, 64, 101216.

De Nooij, M., Koopmans, C., & Bijvoet, C. (2007). The value of supply security. The cost of power interruptions: economic input for damage reduction and investment in networks. *Energy Economics*, 29, pp. 277-295.

Diu, A. (2014). *Terms of Reference for the trials*. Ceris-CNR RT. 51. http://essence.ceris.cnr.it/images/documenti/RT_51.pdf

Ericson, S., & Lisell, L. (2020). A flexible framework for modeling customer damage functions for power outages. *Energy systems*, *11*(1), pp. 95-111.

Finardi U., Ragazzi E., & Stefanini, A. (2013). *Considerations on the implementation of SCADA standards on critical infrastructures of power grids*. Ceris-CNR RT. 47. http://essence.ceris.cnr.it/images/documenti/RT_47.pdf

García F., Alessi M., Bartoszewicz-Burczy, H., Cortes A., Pestonesi D., & Włodarczyk, T. (2013). *Attack scenarios. Threats, vulnerabilities and attack scenarios along with their selection criteria*. Ceris-CNR RT. 48. http://essence.ceris.cnr.it/images/documenti/RT_48.pdf

García Gutiérrez, F., & Ragazzi, E. (2014) *Trial evaluation: conclusive lessons from Essence case studies*. Ceris-CNR RT. 57. http://essence.ceris.cnr.it/images/documenti/RT_57.pdf

Kahneman, D., Knetsch, J.L., & Thaler, R.H. (1991). Anomalies: The endowment effect, loss aversion and status quo bias. *The journal of economic perspectives*, *5*(1), pp. 193-206.

Koetse, M.J., & Brouwer, R. (2016). Reference dependence effects on WTA and WTP value functions and their disparity. *Environmental and Resource Economics*, 65, pp. 723-745.

Koń, B., & Jakubczyk, M. (2019). Is the literature on the WTP-WTA disparity biased?. *Journal of Behavioral and Experimental Economics*, 82, 101460.

Frondel, M., Sommer, S., & Tomberg, L. (2021). WTA-WTP disparity: the role of perceived realism of the valuation setting. *Land Economics*, *97*(1), pp. 196-206.

Linares, P., & Rey, L. (2013). The cost of electricity interruptions in Spain. Are we sending the right signals? *Energy Policy*, 61, pp.751-760.

Nguyen, K.T., Knetsch, J.L., & Mahasuweerachai, P. (2021). WTP or WTA: a means of determining the appropriate welfare measure of positive and negative changes when preferences are reference dependent. *Environmental and Resource Economics*, 78, pp. 615-633.

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. 206-226.

Reichl, J., Schmidthaler, M., & Schneider, F. (2013a). The value of supply security: the cost of Power outages to Austrian households, firms and the public sector. *Energy Economics*, 36, pp. 256-261.

Reichl, J., Schmidthaler, M., &Schneider, F. (2013b). Power outage cost evaluation: reasoning, methods and application. *Journal of scientific research & reports*, *2*(1), pp. 249-276.

Chapter 4
Methods to assess the economic value of cybersecurity

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

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
This chapter of the Quaderno IRCrES on *Cybersecurity and data protection in the electricity sector: state-of-the-art of the literature and evaluation methods* focuses on demonstrating the suitability of the Cost-Benefit Analysis (CBA) approach for assessing the value of cybersecurity in electrical infrastructures, from the perspective of citizens. Given the absence of market data for such non-market goods, we argue for the validity of Stated Preferences methods, particularly discrete choice experiments. We review the existing literature applying CBA methods to cybersecurity before narrowing our focus to works evaluating the economic valuation of electricity service continuity. This body of work is largely composed of case studies focused on specific countries or environments and discusses the relative merits of willingness to pay versus willingness to accept. Despite a growing interest in the economic implications of service interruptions, our review reveals a consequential gap: the absence of studies examining power outages caused by cyberattacks on critical electricity infrastructures. This highlights an urgent need for further research at the intersection of cybersecurity and energy system resilience.

KEYWORDS: Cybersecurity, electricity continuity, cost-benefit analysis, stated preferences methods, discrete choice experiments.

DOI: 10.23760/2499-6661.2025.24_04
ISBN: 978-88-98193-39-4
ISSN (online): 2499-6661

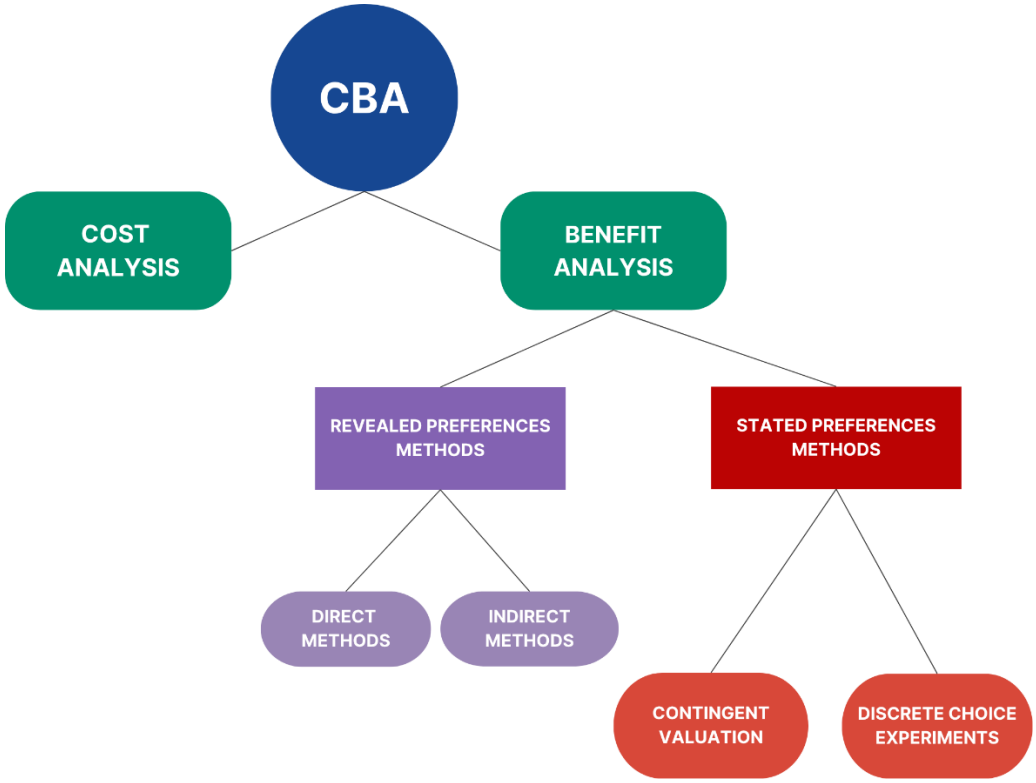
HOW TO CITE
Vallette d'Osia, J.C.M., Finardi, U., & Ragazzi, E. (2025). Methods to assess the economic value of cybersecurity. In Ragazzi, E., Finardi, U., & Vallette d'Osia, J.C.M. (eds.). *Cybersecurity and data protection. in the electricity sector. State-of-the-art of the literature and evaluation methods* (pp. 53-63). Quaderni IRCrES 24. CNR-IRCrES. http://dx.doi.org/10.23760/2499-6661.2025.24_04

1 INTRODUCTION

Cost-benefit analysis (CBA) methodologies aim to evaluate the economic value of non-market goods, such as security. Furthermore, these methods analytically compare the costs and benefits related to a project. To this end, CBA makes it easier to make and justify investment or regulatory decisions by providing an estimate of the economic impacts before implementation begins. Boardman, Greenberg, Vining & Weiner (2018) define CBA as a "policy assessment method that quantifies in monetary terms the value of all consequences of a policy to all members of society" with the purpose of "social decision making […] or, more technically, to improve allocative efficiency" (p. 2).

The analysis of the value of cybersecurity in electrical infrastructures for citizens falls within the scope of CBA because it allows for the estimation of the benefit of investing in measures to increase control over digital resources. In this framework, to better clarify the different methodologies, we have summarized in Figure 1 the methodological options available for evaluating benefits and costs, and how the different methods are related to each other.

Figure 1. Framework of the different methods for evaluating non-market goods under a Cost Benefit Analysis



Source: Own elaboration.

When the benefit of an investment is a market product or service, the prices set in the market can be used as a reference. However, when the benefit is a non-market product, as is the case with security, estimates based on non-market valuation methods are required. In some cases, the preferences of citizens or target users can be inferred from their behaviour regarding different products or services that may reveal preferences for the good in question (Revealed Preferences

methods). If this is not possible, the data to estimate the value must be derived from statements made by individuals (Stated Preferences (SP) methods).

The quality of the estimate depends largely on how these statements are obtained. With contingent valuation (CV), individuals are asked to directly state a value (e.g., "what is the maximum amount you would be willing to pay for..."). One may investigate either the willingness to pay (WTP) for a certain good or the willingness to accept (WTA) compensation if one were to be deprived of it. Contingent valuation is usually based on a detailed set of questions presenting different scenarios. The structure can be simple, with a single set of mutually exclusive questions, or it can include multiple layers of questions to better define different scenarios (e.g., one layer might be the duration of a blackout, another its timing, and so on).

It should be emphasized that it is very difficult to provide well-founded answers by expressing a monetary value for aspects/goods/services for which one has no direct experience. The choice experiment approach partially addresses this difficulty by asking respondents to imagine possible real-life situations described in precise scenarios, where a monetary value is usually presented as an attribute among those defining the scenarios. The economic value of the non-market good will be elicited, through econometric models, by combining responses on the acceptance or rejection of different scenarios.

Applications of the described methods can be found in the literature. For example, to understand the value of cybersecurity for consumers, Blythe, Johnson & Manning (2020) investigate the WTP for secure "Internet of Things" devices. The authors use CV to assess the extent to which consumers value the security of various internet-connected products. They confirmed previous findings (Nguyen, Rosoff & John, 2017; Rowe & Wood, 2013) that customers are willing to pay for safer products and services.

Moreover, over time, several studies have focused on analysing the costs and benefits related to personal data breaches, showing how CBA methodologies can be applied to the context of cybersecurity (Wottrich, Van Reijmersdal & Smit, 2018; Winegar & Sunstein, 2019; Yamaguchi, Oshima, Saso & Aoki, 2020; Paliński, 2022).

A further justification for using cost-benefit analysis to evaluate cybersecurity lies in its importance within regulatory frameworks. For example, Gordon, Loeb & Zhou (2020) argue that current regulatory frameworks, which aim to maximize cybersecurity investments in organizations, lack specificity and clear guidelines. This, in turn, leads to a loss of effectiveness in assessing cybersecurity risks within organizations. The authors therefore propose integrating the Gordon-Loeb model (Gordon & Loeb, 2002) into the NIST (National Institute for Standards and Technology) framework. They use the Gordon-Loeb model as a basis for deriving a cost-effective level of spending on cybersecurity activities. The Gordon-Loeb model has indeed been widely recognized in the literature as the leading model for cybersecurity investment (Haapamäki & Sihvonen, 2019). Consequently, following this evaluation, organizations would be able to select the most accurate level of security within the NIST framework, corresponding to the rigor and sophistication of their risk management process.

CBA has also been widely applied in the context of cybersecurity risk management. For example, Kayode, Arome, Tolulope & Ajoke (2016) discuss cybersecurity strategies through the application of mathematical models implemented in a cost-benefit analysis. To make their estimates, the authors first interviewed individuals from academia, financial institutions, and internet service providers, asking questions about the advantages, disadvantages, and effectiveness of their security strategies. The authors claim that their application of CBA can automatically compare the projected amount with the allocated amount of the cybersecurity strategy in question. In their study, Algarni, Thayananthan & Malaiya (2021) also use mathematical models to estimate the cost of a breach and the probability of a data breach within 12 months. By estimating these two components of cybersecurity risks, the authors aim to improve data security solutions. Furthermore, Lee (2021) developed a cybersecurity risk management framework. In this framework, organized into four levels, cost-benefit analysis plays a central role. In particular, CBA is necessary within the "cyber risk assessment level" because it requires three steps: risk identification, risk quantification, and cybersecurity investment analysis.

Finally, as mentioned in previous sections, cyberattacks can have enormous consequences for society as a whole. These consequences are often not taken into account when constructing regulatory frameworks and policies. However, CBA addresses this aspect by providing a model of rationality. Indeed, as explained in the OECD (2018) guideline on CBA applied to environmental issues, CBA "forces the decision-maker to look at who the beneficiaries and losers are in both the spatial and temporal dimensions" (p. 32). In this way, CBA applied to the context of cybersecurity can provide a comprehensive and extended estimate of the economic value of cybersecurity.

To summarize, conducting studies on cybersecurity using a cost-benefit analysis methodology has proven effective and significant. More specifically, economic sciences argue that to assign an economic value to non-market goods through CBA, direct methods such as Stated Preferences can be used. These methodologies allow deriving the value of a non-directly monetizable good through studies conducted on a representative sample of a population. As described above, this also applies to cybersecurity analyses. To narrow the analysis and explain our methodological choices, the following section addresses a practical situation: a cyberattack leading to a blackout, to examine the economic value of cybersecurity attributed by energy consumers.

2 COST-BENEFIT ANALYSIS APPLIED TO THE CASE OF THE ELECTRIC SYSTEM

To demonstrate the value attributable to a good or service for which market information is unavailable, SP methodologies often use individuals' WTP for the good or service in question or their WTA compensation following a change in the provision of that good or service. Through the use of WTP or WTA, monetary values are derived from participants' responses to specific questions about real or hypothetical but realistic scenarios. In this way, SP methodologies contrast with revealed preference methodologies, which rely on actual purchasing behaviours. Specifically, WTP and WTA are tools evaluated through two types of survey methodologies. One is the CV method, which uses direct questions where participants must state their WTP or WTA for a non-market good. The second is the DCE method, which presents scenarios involving different characteristics of the good in question, where participants must choose between different options of acceptance or compensation.

The goal of this section is to narrow the literature analysis to themes closer to the specific research focus. Therefore, this section presents scientific articles that conduct cost-benefit analyses using stated preference methodologies related to the specific topic of security in the management of electrical systems. This literature overview shows that works on the topic are preferably represented by case studies specific to countries or environments.

Several studies relate to the economic evaluation of electricity service reliability in developing countries. The reason behind this high number of studies lies in the fact that these countries experience what can be characterized as a "double tragedy". In fact, these countries suffer from both low electricity access rates and frequent power outages, which are often persistent and severe. This situation, on the one hand, highlights how understanding the value of service continuity is fundamental in prioritizing the various types of infrastructure investments a country needs. On the other hand, it allows consulting panels of respondents who are fully aware of the impacts of service disruptions on their work and non-work activities. However, it should also be noted that in contexts where electricity supply is particularly unreliable, economic operators often equip themselves with emergency generators, the presence of which could reduce WTP but whose costs should be included in the overall CBA. Moreover, it should be emphasized that these results cannot be simply transferred to developed contexts. In fact, in markets with a high reliability of electricity provision, consumers show higher propension to buy electric devices with respect to other available technologies (e.g. for cooking or heating) and they depend more on continuity of supply.

A series of articles addresses the problem of power outages in Ethiopia. The most recent is by Entele & Ayalew (2024). The authors conduct a CE study aimed at estimating the economic cost

of power outages for manufacturing firms in Ethiopian cities. Consequently, they derive the WTP of small, medium, and large manufacturing firms using an econometric analysis performed through a mixed Logit model. In this way, they complement the work of other authors such as Carlsson, Demeke, Martinsson & Tesemma (2020) and Meles et al. (2021). Entele & Ayalew (2024), in fact, study the impact of power outages in areas outside the capital Addis Ababa, which has a specific energy supply situation. Their results show strong heterogeneity depending on the size of the firm and the industrial sector. However, both the costs of power outages and the WTP of firms to avoid outages are significant. Consequently, the authors argue for the importance of optimizing the diversification of electricity sources. For their part, Aweke & Navrud (2022) studied Ethiopian households in rural areas, who on average experienced 160 blackouts, lasting an average of four hours, per year. They found in their analysis that participants' WTP to avoid blackouts is worth about 32% of the annual electricity bill.

Some articles have focused on the impact of households' socioeconomic and demographic characteristics on WTP for improved energy services. Abdullah & Mariel (2010) and Osiolo (2017) conducted a choice experiment and a contingent valuation, respectively, based on the population of Kenya. The latter author examined WTP in the form of a "quality tax" on energy sources, namely firewood, charcoal, and electricity for households and businesses. The former author, on the other hand, studied WTP to avoid power outages for rural households. For their part, Taale & Kyeremeh (2016) studied WTP for reliable services using a CV method. These authors were able to clarify that households are willing to pay 44% more than the average monthly electricity bill for greater reliability. These three studies highlight two common socioeconomic characteristics that can influence WTP: household size and education level. Additionally, Abdullah & Mariel (2010) also emphasizes the effects of age, years of residence in the area, employment status, agricultural activities, and whether participants had a bank account. Taale & Kyeremeh (2016), on the other hand, found that notice period, business ownership, monthly income, and ownership of a separate meter (compared to households who share their meter) were significant.

Two papers focused on the impact of the timing of power outages on WTP. Nkosi & Dikgang (2018) and Alinsato (2015) use the same methodology for two studies based in South Africa and Benin, respectively, with results that are not very aligned (likely due to the different contexts of the two studies). This methodology involves a CV survey where WTP to avoid power outages is derived using a random parameter Tobit model. In the study by Nkosi & Dikgang (2018), WTP is higher when seeking to avoid power outages on weekdays and in winter, while in Alinsato (2015), the preference for service reliability is greater during the night and on weekends. However, both studies emphasize that WTP depends positively on the duration of the outage.

Other studies, conducted in Ghana (Amoah, Ferrini & Schaafsma, 2019), Nigeria (Oseni, 2017), Senegal (Deutschmann, Postepska & Sarr, 2021), Northern Cyprus (Ozbafli & Jenkins, 2015; 2016), and Nepal (Hashemi, 2021), use SP methods, assessing WTP for reliable electricity supply or WTP for quality improvement. All works show that households exhibit significant preferences for high-quality and reliable electricity service.

The economic evaluation of service reliability in the electricity sector has also been studied in developed nations. For example, Praktiknjo (2014) studied the monetary consequences of power outages for German households. To this end, he used both the estimation of outage costs using WTA and WTP methodologies and the derivation of VoLL (Value of Lost Load). In this way, the author found that residential consumers assign relatively high values to the security of supply, with the duration of the power outage having a significant impact on VoLL and the magnitude of outage costs.

Looking at other aspects of electricity reliability, Amador, González & Ramos-Real (2013) focused on WTP for three levels of service attributes: supply reliability, share of renewable energy, and availability of a complementary energy audit service. Their work is based on the residential market in the Canary Islands. Among other results, the article shows that respondents with a high level of education exhibit higher WTP for renewable energy, in line with their stated concern about greenhouse gas emissions.

Some studies have chosen to use WTA as a measure of preferences regarding the reliability and quality of electricity service. Xu, Yang, Deng & Wang (2024) examined compensation (WTA) for energy rationing during peak hours in China, while Abrate, Bruno, Erbetta, Fraquelli & Lorite-Espejo (2016) studied WTA compensation for power outages in Italy. Tocock, Hatton MacDonald & Rose (2024), on the other hand, focused on WTA regarding lower cost increases in Australia. The similarities between the three articles lie in their methodologies, as all use a DCEs. However, their results differ. Xu et al. (2024) observe that participants' preferences are for a higher level of compensation in summer and at night. As for Abrate et al. (2016), they note that VoLL is correlated with both the duration of the outage and various household characteristics. Finally, Tocock et al. (2024) conclude that households value electricity contracts that influence the pace of energy investments, making the compensation modelled for lower cost increases in cases where such features within a contract are reduced.

Woo et al. (2014) also employed WTA, but this time observing participants' acceptance preferences in cases where they could pay a lower electricity bill in response to reduced reliability. This experiment was conducted in Hong Kong, where electricity supply is considered nearly flawless. The authors establish that participants are unwilling to accept a reduction in reliability, even in exchange for financial compensation.

Regarding the use of WTP, various articles have measured it in cases where power outages must be avoided. This is the case for Hensher, Shore & Train (2014) in Australia, Carlsson, Kataria, Lampi & Martinsson (2021) in Sweden, Morrissey, Plater & Dean (2018) in England, and Gorman & Callaway (2024) in the United States. Although they use similar methods, these works investigate different aspects of the problem. Gorman & Callaway (2024) examined the impact of advance notice of power outages on household WTP. Morrissey et al. (2018), on the other hand, characterized power outages using five attributes: duration; peak/off-peak hours; day of the week; winter/summer; price. Hensher et al. (2014) differentiated their work by studying the frequency and duration of power outages. Finally, Carlsson et al. (2021) compared past studies from 2004 and 2017 to investigate changes in WTP. It can be seen here that the variety of topics and aspects studied can be broad and detailed, while the conclusion remains fairly homogeneous across studies: deriving monetary values of electricity reliability allows for demonstrating significant preferences for avoiding power outages.

Finally, various setups and case studies have been implemented in Switzerland (Motz, 2021), Finland (Küfeoğlu & Lehtonen, 2015), Norway (Vennemo, Rosnes & Skulstad, 2022), Pennsylvania, USA (Baik, Davis & Morgan, 2018), and South Korea (Kim, Nam & Cho, 2015). A detailed analysis of each of these works would be too space consuming, but it is worth noting their added value in the research area of electricity system security management through the lens of SP methodologies.

To summarize, works using SP methodologies, particularly through the use of WTP and WTA, on the specific topic of security in the management of electrical systems are characterized by their particular geographic contexts. The diversity of characteristics of electrical systems, as well as socioeconomic contexts, can lead to very different results regarding the effect of conditioning variables (respondent characteristics) or the appreciation of specific aspects of service continuity.

This review shows that, despite a certain richness and variety of works on service continuity, there is an almost total lack of studies addressing the challenges of cybersecurity in ensuring the security of electrical systems. Indeed, no work to our knowledge refers to the specific case of power outages due to cyberattacks on critical electricity grid infrastructures, highlighting the need for further research and investigations.

3 FROM THEORY TO PRACTICE: METHODOLOGICAL ASPECTS RELATED TO THE IMPLEMENTATION OF A DATABASE FOR ANALYSING THE ECONOMIC VALUE OF CYBERSECURITY

The goal of this "Quaderno IRCrES" is to provide a review as complete as possible of the state of the art of economic research related to the various existing methods related to cybersecurity and data protection, with a particular focus on the electricity sector. More specifically, this chapter focuses on the acceptance of monetary compensation in the form of discounts on electricity bills, using the WTA method as a valuation tool. To carry out this estimation, we deem as the best option the use of a Choice Experiment (CE) method, that we practically apply in our experimental activity presented in the next chapter (Vallette d'Osia, Finardi & Ragazzi, 2025).

DCEs, along with CV methods, as defined and illustrated above, are significant stated preference techniques for analysing individual preferences in the electrical industry.

In surveys conducted by the CV method, the structure is usually simple. In fact, a single set of mutually exclusive questions is used or, in order to further detail different scenarios, additional levels of questions (e.g., one level might be the duration of the blackout, another its time location, and so on).

In contrast, in DCE methods, respondents are offered a choice of several specific decision-making processes, where several alternative fixed options are displayed. A high number of scenarios are then assumed, combining attributes in different proportions. Since respondents can only accept or reject a scenario as a whole, the estimate of how each attribute impacts the economic value of the studied good or service is obtained by combining the responses from a large sample. Different types of cyber breaches are simulated in our scenarios, leading to outages of different durations. For this purpose, our research is inspired by the survey conducted in the ESSENCE (Emerging Security Standards to the EU power Network controls and other Critical Equipment) project, widely described in chapter 3[1] (Bruno & Erbetta, 2025); it adopts its approach while conducting a much larger experiment in terms of sample coverage and scenario attributes.

Supporting the use of a choice experiment method in our case stems from the idea that we believe it is difficult for individuals to attribute monetary values to their preferences in both cybersecurity and electric service interruptions. This problem is addressed by the DCEs because they allow respondents to immerse themselves in hypothetical scenarios without having to provide an exact value of what is difficult for them to monetize. In fact, DCEs are constructed so that respondents do not have to actively provide a monetary value to a nonmarket good or service. Instead, they must choose among discrete alternatives that are proposed to them.

As mentioned above, our research project employs the concept of WTA for the purpose of deriving acceptance of monetary compensation in the form of rebates on electricity bills in the event of a blackout caused by a cyberattack. The choice between WTA and WTP has been widely debated in the literature. Our position of using WTA also has to do with the difficulty of valuing a nonmarket good or service. We think it is more difficult for respondents to think about how much they would be willing to pay for reliable cybersecurity or uninterrupted electricity. In this we agree with what Abrate et al. (2016) say in their paper as they thoroughly explain the use of WTA in the context of a choice experiment to value power outages. We therefore find it simpler to evaluate disruption than the service that respondents benefit from on a daily basis.

To summarize, it seems more reliable to demand WTA compensation for a discontinuity or breach because respondents consider it fair and almost guaranteed to benefit from a cyber-secure electricity provider. Conversely, where electrical supply security or cyber security were not normally guaranteed, WTP would be an appropriate survey tool. The results of Grutters et al. (2008) support this idea. Indeed, their work makes it clear that the choice between WTP and WTA in a DCE must be made taking into account whether most respondents are potential beneficiaries or losers, depending on the cost attribute defined in the DCE (a payment or a discount). The paper also argues that the choice of a WTA experiment is in fact the best option in the case of potential

[1] See also https://essence.ceris.cnr.it/ (link visited July 2025).

losers, which is true in our case as respondents face scenarios in which they experience a cyberattack-induced blackout.

In addition, it is important in our case not only to look at the total change in blackout preferences caused by cyberattacks, which is usually done with CV surveys, but to retrieve the combinations of attribute levels that would be acceptable to respondents, justifying our choice for a DCE (OECD, 2018).

4 CONCLUSIONS

The present chapter goes deeper in adding specific topics to this Quaderno. After addressing the economic perspective of cybersecurity in the electricity sector, exploring the broader concept of digital sovereignty, and introducing relevant insights from the ESSENCE experience, this section turns to an analysis of the methodological approaches that can be used to disentangle the challenges involved in citizens' economic evaluation of these relevant topics. The concise but complete analysis, performed mostly by part of a literature review, of the methodologies that can shed light on these magnitudes, goes directly into the fifth chapter of this Quaderno (Vallette d'Osia et al. 2025), that is, a synthetic description of an experimental activity aimed at the direct evaluation of costs and benefits of cybersecurity.

5 BIBLIOGRAPHY

Abdullah, S., & Mariel, P. (2010). Choice experiment study on the willingness to pay to improve electricity services. *Energy Policy*, *38*(8), pp. 4570-4581. https://doi.org/10.1016/j.enpol.2010.04.012

Abrate, G., Bruno, C., Erbetta, F., Fraquelli, G., & Lorite-Espejo, A. (2016). A choice experiment on the willingness of households to accept power outages. *Utilities Policy*, 43, pp. 151-164. https://doi.org/10.1016/j.jup.2016.09.004

Algarni, A.M., Thayananthan, V., & Malaiya, Y.K. (2021). Quantitative Assessment of Cybersecurity Risks for Mitigating Data Breaches in Business Systems. *Applied Sciences*, *11*(8), 3678. https://doi.org/10.3390/app11083678

Alinsato, A.S. (2015). Economic valuation of electrical service reliability for Households' in developing country: a censored random coefficient model approach. *International Journal of Energy Economics and Policy*, *5*(1), pp. 352-359.

Amador, F.J., González, R.M., & Ramos-Real, F.J. (2013). Supplier choice and WTP for electricity attributes in an emerging market: The role of perceived past experience, environmental concern and energy saving behavior. *Energy Economics*, 40, pp. 953-966. https://doi.org/10.1016/j.eneco.2013.06.007

Amoah, A., Ferrini, S., & Schaafsma, M. (2019). Electricity outages in Ghana: Are contingent valuation estimates valid? *Energy Policy*, 135, 110996. https://doi.org/10.1016/j.enpol.2019.110996

Aweke, A.T., & Navrud, S. (2022). Valuing energy poverty costs: Household welfare loss from electricity blackouts in developing countries. *Energy Economics*, 109, 105943. https://doi.org/10.1016/j.eneco.2022.105943

Baik, S., Davis, A. L., & Morgan, M. G. (2018). Assessing the Cost of Large-Scale Power Outages to Residential Customers. *Risk Analysis*, *38*(2), pp. 283-296. https://doi.org/10.1111/risa.12842

Blythe, J.M., Johnson, S.D., & Manning, M. (2020). What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. *Crime Science*, *9*(1). https://doi.org/10.1186/s40163-019-0110-3

Boardman, A.E., Greenberg, D.H., Vining, A.R., & Weimer, D.L. (2018). *Cost-Benefit Analysis: Concepts and Practice* (5th ed.). Cambridge University Press. https://doi.org/10.1017/9781108235594

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

Carlsson, F., Demeke, E., Martinsson, P., & Tesemma, T. (2020). Cost of power outages for manufacturing firms in Ethiopia: A stated preference study. *Energy Economics*, 88, 104753. https://doi.org/10.1016/j.eneco.2020.104753

Carlsson, F., Kataria, M., Lampi, E., & Martinsson, P. (2021). Past and present outage costs – A follow-up study of households' willingness to pay to avoid power outages. *Resource and Energy Economics*, 64, 101216. https://doi.org/10.1016/j.reseneeco.2021.101216

Deutschmann, J.W., Postepska, A., & Sarr, L. (2021). Measuring willingness to pay for reliable electricity: Evidence from Senegal. *World Development*, 138, 105209. https://doi.org/10.1016/j.worlddev.2020.105209

Entele, B.R., & Ayalew, S. (2024). The cost of electricity interruption for manufacturing firms in Ethiopia: Valuing outage by applying stated preference approach. *Journal of Applied Economics*, 27(1), 2394715. https://doi.org/10.1080/15140326.2024.2394715

Gordon, L.A., & Loeb, M.P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, *5*(4), pp. 438-457. https://doi.org/10.1145/581271.581274

Gordon, L.A., Loeb, M.P., & Zhou, L. (2020). Integrating cost-benefit analysis into the NIST Cybersecurity Framework via the Gordon-Loeb Model. *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/cybsec/tyaa005

Gorman, W., & Callaway, D. (2024). Do notifications affect households' willingness to pay to avoid power outages? Evidence from an experimental stated-preference survey in California. *The Electricity Journal*, 37, 107385. https://doi.org/10.1016/j.tej.2024.107385

Grutters, J.P.C., Kessels, A.G.H., Dirksen, C.D., Van Helvoort-Postulart, D., Anteunis, L.J.C., & Joore, M.A. (2008). Willingness to Accept versus Willingness to Pay in a Discrete Choice Experiment. *Value in Health*, *11*(7), pp. 1110-1119. https://doi.org/10.1111/j.1524-4733.2008.00340.x

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, *34*(7), pp. 808–834. https://doi.org/10.1108/MAJ-09-2018-2004

Hashemi, M. (2021). The economic value of unsupplied electricity: Evidence from Nepal. *Energy Economics*, 95, 105124. https://doi.org/10.1016/j.eneco.2021.105124

Hensher, D.A., Shore, N., & Train, K. (2014). Willingness to pay for residential electricity supply quality and reliability. *Applied Energy*, 115, pp. 280-292. https://doi.org/10.1016/j.apenergy.2013.11.007

Kayode, A.B., Arome, G.J., Tolulope, A., & Ajoke, A.O. (2016). Cost-Benefit Analysis of Cyber-Security Systems. In *Proceedings of the World Congress on Engineering and Computer Science*, 1.

Kim, K., Nam, H., & Cho, Y. (2015). Estimation of the inconvenience cost of a rolling blackout in the residential sector: The case of South Korea. *Energy Policy*, 76, pp. 76-86. https://doi.org/10.1016/j.enpol.2014.10.020

Küfeoğlu, S., & Lehtonen, M. (2015). Interruption costs of service sector electricity customers, a hybrid approach. *International Journal of Electrical Power & Energy Systems*, 64, pp. 588-595. https://doi.org/10.1016/j.ijepes.2014.07.046

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), pp. 659-671. https://doi.org/10.1016/j.bushor.2021.02.022

Meles, T.H., Mekonnen, A., Beyene, A.D., Hassen, S., Pattanayak, S.K., Sebsibie, S., Klug, T., & Jeuland, M. (2021). Households' valuation of power outages in major cities of Ethiopia: An

application of stated preference methods. *Energy Economics*, 102, 105527. https://doi.org/10.1016/j.eneco.2021.105527

Morrissey, K., Plater, A., & Dean, M. (2018). The cost of electric power outages in the residential sector: A willingness to pay approach. *Applied Energy*, 212, pp. 141-150. https://doi.org/10.1016/j.apenergy.2017.12.007

Motz, A. (2021). Security of supply and the energy transition: The households' perspective investigated through a discrete choice model with latent classes. *Energy Economics*, 97, 105179. https://doi.org/10.1016/j.eneco.2021.105179

Nguyen, K.D., Rosoff, H., & John, R.S. (2017). Valuing information security from a phishing attack. *Journal of Cybersecurity*, *3*(3), pp. 159-171. https://doi.org/10.1093/cybsec/tyx006

Nkosi, N.P., & Dikgang, J. (2018). Pricing electricity blackouts among South African households. *Journal of Commodity Markets*, 11, pp. 37-47. https://doi.org/10.1016/j.jcomm.2018.03.001

OECD. (2018). *Cost-Benefit Analysis and the Environment: Further Developments and Policy Use*. OECD Publishing. https://doi.org/10.1787/9789264085169-en

Oseni, M.O. (2017). Self-Generation and Households' Willingness to Pay for Reliable Electricity Service in Nigeria. *The Energy Journal*, *38*(4), pp. 165-194. https://doi.org/10.5547/01956574.38.4.mose

Osiolo, H.H. (2017). Willingness to pay for improved energy: Evidence from Kenya. *Renewable Energy*, 112, pp. 104-112. https://doi.org/10.1016/j.renene.2017.05.004

Ozbafli, A., & Jenkins, G.P. (2015). The willingness to pay by households for improved reliability of electricity service in North Cyprus. *Energy Policy*, 87, pp. 359-369. https://doi.org/10.1016/j.enpol.2015.09.014

Ozbafli, A., & Jenkins, G.P. (2016). Estimating the willingness to pay for reliable electricity supply: A choice experiment study. *Energy Economics*, 56, pp. 443-452. https://doi.org/10.1016/j.eneco.2016.03.025

Paliński, M. (2022). Paying with your data. Privacy tradeoffs in ride-hailing services. *Applied Economics Letters*, *29*(18), pp. 1719-1725. https://doi.org/10.1080/13504851.2021.1959891

Praktiknjo, A. J. (2014). Stated preferences based estimation of power interruption costs in private households: An example from Germany. *Energy*, 76, pp. 82-90. https://doi.org/10.1016/j.energy.2014.03.089

Rowe, B., & Wood, D. (2013). Are Home Internet Users Willing to Pay ISPs for Improvements in Cyber Security? In Schneier, B. (eds.). *Economics of Information Security and Privacy III* (pp. 193-212). Springer. https://doi.org/10.1007/978-1-4614-1981-5_9

Taale, F., & Kyeremeh, C. (2016). Households′ willingness to pay for reliable electricity services in Ghana. *Renewable and Sustainable Energy Reviews*, 62, pp. 280-288. https://doi.org/10.1016/j.rser.2016.04.046

Tocock, M., Hatton MacDonald, D., & Rose, J.M. (2024). Risk preferences, bill increases and the future reliability of electricity networks in Australia. *Energy Research & Social Science*, 118, 103763. https://doi.org/10.1016/j.erss.2024.103763

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. 63-68). Quaderni IRCrES 24. CNR-IRCrES. http://dx.doi.org/10.23760/2499-6661.2025.24_05

Vennemo, H., Rosnes, O., & Skulstad, A. (2022). The cost to households of a large electricity outage. *Energy Economics*, 116, 106394. https://doi.org/10.1016/j.eneco.2022.106394

Winegar, A.G., & Sunstein, C.R. (2019). How Much Is Data Privacy Worth? A Preliminary Investigation. *Journal of Consumer Policy*, *42*(3), pp. 425-440. https://doi.org/10.1007/s10603-019-09419-y

Woo, C.K., Ho, T., Shiu, A., Cheng, Y.S., Horowitz, I., & Wang, J. (2014). Residential outage cost estimation: Hong Kong. *Energy Policy*, 72, pp. 204-210. https://doi.org/10.1016/j.enpol.2014.05.002

Wottrich, V.M., Van Reijmersdal, E.A., & Smit, E.G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems*, 106, pp. 44-52. https://doi.org/10.1016/j.dss.2017.12.003

Xu, S., Yang, Z., Deng, N., & Wang, B. (2024). Residents' willingness to be compensated for power rationing during peak hours based on choice experiment. *Applied Energy*, 367, 123335. https://doi.org/10.1016/j.apenergy.2024.123335

Yamaguchi, S., Oshima, H., Saso, H., & Aoki, S. (2020). How Do People Value Data Utilization?: An Empirical Analysis Using Contingent Valuation Method in Japan. *Technology in Society*, 62, 101285. https://doi.org/10.1016/j.techsoc.2020.101285

Chapter 5
An empirical approach to assess the value assigned by individuals to cybersecurity and data protection

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

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
Anchoring the literature review carried in the prior chapters of the Quaderno IRCrES *Cybersecurity and data protection in the electricity sector: state-of-the-art of the literature and evaluation methods* to a practical application is a necessary exercise to grasp entirely the challenges previous studies encountered in estimating the value attributed by individuals to cybersecurity within the electric power sector. This chapter presents our experimental activity, which consists of a representative survey based on a discrete choice experiment designed to evaluate the monetary value the Italian population attributes to electricity blackouts and data theft incidents. Specifically, we examine individuals' willingness to accept compensation in exchange for experiencing an electricity outage or a data breach, with scenarios varying by duration of the blackout and severity of the data theft. Some questions addressing cybersecurity risks in the electricity sector were included intentionally to raise awareness of the public on the topic. The chapter details the development of the survey instrument, beginning with a synthesis on the methodological choices made to ensure its validity, followed by a description of the data collection process.

KEYWORDS: discrete choice experiment, willingness-to-accept, cybersecurity, electricity blackout, data theft.

DOI: 10.23760/2499-6661.2025.24_05
ISBN: 978-88-98193-39-4
ISSN (online): 2499-6661

HOW TO CITE
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

This chapter describes synthetically an experimental activity entailing a discrete choice experiment (DCE) performed with the aim of evaluating the value attached by the Italian population to a blackout and to a data theft. More specifically, also given the speculative nature of this Quaderno, we concentrate, rather than on the experimental results, on the methodological path that led to the survey, describing how and why we collected data. Thus, we describe in the sections below the survey instrument, with a specific focus on the administered scenarios, and the practical outcome of the survey.

1 JUSTIFICATION OF THE ANALYSIS DESIGN IN THE CONTEXT OF STUDYING CYBERSECURITY FOR THE ELECTRICITY SECTOR

In Chapter 4 (Vallette d'Osia, Finardi & Ragazzi, 2025) we reviewed the main reasons for preferring a DCE experiment over a Contingent Valuation method. First, we align with the literature that finds that respondents are not knowledgeable and experienced enough to directly put a price on the disruption of electrical continuity. Since the DCE method does not require respondents to be able to do so, the method better fits the purpose of our research. Second, since we aim to discover changes in the level of attributes of interest (i.e., we examine different durations of the outage and gravity levels of data theft), we need a method that takes this into account, which is precisely the case with DCEs.

The design of our DCE experiment was therefore developed taking into account the challenges that weaken the validity of the method. Boxebeld (2024) reviewed existing literature to highlight the role of ordering effects within DCEs. In our case, with two alternatives (i.e. Yes, I accept the economic compensation associated with the blackout or data theft/No, I prefer to remain without any blackout or data theft) and two attributes (i.e. blackout and discount for the blackout choice experiment, data theft and discount for the data theft Choice experiment), we do not have strong concerns about either the order of alternatives or the order of attributes effects. Similarly, the position bias, related to the "lexicographic behaviour" mechanism is unlikely to be significant in our case because of the low number of attributes and alternatives. Still, we chose to randomize the order of alternatives since it was not difficult to implement.

However, we do note the presence of choice set ordering effects. Indeed, the position of a scenario within the sequence presented to a respondent could have an impact on both the error variance and the probability of choosing the status quo. Three mechanisms are at play: learning effect, cognitive burden and anchoring effect. The *learning effect* occurs as participants become more familiar with the choice setting, leading to better-defined preferences and more consistent decisions over the course of the sequence. Conversely, *cognitive burden* can set in after the completion of multiple scenarios, causing fatigue, loss of focus, and thus an increase in random or irrational choices. Lastly, the *anchoring effect* suggests that respondents' later choices may be influenced by the attribute levels they encountered earlier, introducing a starting point bias.

To overcome these issues, we adopted some mitigating measures. First, we opted for advanced disclosure of the set-up to induce institutional learning and anchoring before the start of the experiment. To do so, we informed respondents about the number of scenarios and the random variation of attribute levels. Secondly, we gave a visual idea of the scenario that respondent would be seeing prior to the start of the choice experiment so that respondents would become familiar with the topic and environment, thus reducing anchoring effects. Thirdly, we randomized the attribute levels[1] and order of scenarios to prevent starting point bias. Finally, we maintained a low number of scenarios shown to respondents (4 to be completed for the blackout choice set, 3 for the data theft one) to reduce the cognitive burden.

To summarize, the validity of a DCE can be compromised by various ordering effects, highlighted in the literature on the topic; consequently, we implemented mitigation measures in

[1] The levels of attributes were randomized, still, we implemented two constraints: respondents could be asked twice about the same amount of discount, but never more than once the same length of blackout/or the same level of data theft.

our survey design to reduce as much as possible the various biases arising from respondents' learning, fatigue, anchoring, or lexicographic behaviours.

Attribute levels were randomized; however, we implemented two constraints: respondents could be asked twice about the same amount of discounting, but never more than once about the same duration of blackout and/or the same level of data theft.

2 THE DATA COLLECTION DESIGN TO ASSESS THE ECONOMIC VALUE OF CYBERSECURITY IN THE ELECTRICITY SECTOR FOR CITIZENS

This section goes details the approach used to collect the data, concretely explaining the survey instrument that was designed for the purpose and the administration method used to carry out the survey.

2.1 The survey instrument

The survey instrument used is a questionnaire containing a series of questions designed to elicit the respondents' "Willingness to accept" combined with a number of additional questions aimed at framing the respondents' characteristics in detail and raising their awareness on the topic. Specifically, the questionnaire contains four types of questions:

- Questions related to respondent characteristics.
- Questions related to household use of electricity.
- Questions related to knowledge and awareness of specific issues.
- The scenarios.

Table **1** at the end of the section presents the details of the questions included in the questionnaire.

The survey was entrusted to a specialized company, Qualtrics™, which ensured the use of a balanced panel and specific quality control methods. In fact, the panel is constituted as follows:

- Gender: males (48 %), females (52 %), natural spillover due to the presence of non-binary respondents.
- Age: 18-34 (30 %); 35-54 (32 %); over 55 (38 %).
- Geographical origin: North (41 %); Central (21 %); South and Islands (38 %).
- Income: < 50K€ (~35%); between 50K€ and 100K€ (~35%); >100 K€ (~30%).
- Education level: graduates (35%); non-graduates (65%).

In addition, the implementation of the questionnaire included a series of quality checks, which allowed for the identification of actions such as the introduction of illogical answers or random strings of characters, duplication of answers, the presence of bots, and the insertion of random answers (such as "Christmas tree" answers in Likert scales or the constant insertion of the same answer). In addition, a check was made on response times: answers that were too quick (the speeding check was measured as half the median time during the test phase) were automatically eliminated, as were questionnaires that were incomplete or had inconsistent combinations of answers (e.g., on location).

2.2 The scenarios

In the main section of the questionnaire, respondents were faced with two choice sets, including a series of scenarios describing:

- a cyberattack on the electrical system, resulting in a general blackout of different duration, referred to as the *blackout choice experiment*.
- a cyberattack on the electrical system, resulting in a data theft of different gravity levels, referred to as the *data theft choice experiment*.

In addition to randomly display scenarios within the choice sets, we randomized the order of the two experiments. In this way, respondents were equally likely to begin with either the data theft or blackout experiment, each with their own scenarios and related questions.

The scenarios were constructed after a careful review of relevant scientific literature to conform as closely as possible to the state of the art for conducting surveys of this type.

Before viewing the scenarios, the respondent was given a brief explanation in which he or she was asked to identify with the situation described in each question. In this way, the respondent had to assess the possible consequences for the household, with reference to domestic life, carefully evaluating the discomfort caused by the interruption and the proposed discount.

In proposing the scenarios, considerable attention was paid to their randomization, again following the dictates of the scientific literature on the subject. Accordingly, the scenarios were proposed completely randomly, so as to decrease cognitive bias on the part of the respondents (Boxebeld, 2024).

The blackout choice experiment:

Other possible contextual elements affecting the value of the blackout (season of the year, time of the day, day of the week) were not considered to keep the scenario complexity low. The respondent was asked four questions, referring to a sudden power outage that occurred at 6 p.m. on a Wednesday evening in October. In each question the duration of the blackout was different; possible durations were 1 minute, 6 hours, 9 hours, 18 hours and 36 hours. For each outage, a discount was proposed in the bill by the power company. The discount was quantified in different amounts: €1, €20, €40, €60, €80, and €100. Discounts and durations were combined, identifying a list of 30 possible scenarios. No respondent could happen to have to evaluate scenarios with the same duration. Unlike duration, discounts could instead be repeated within the four scenarios proposed to each respondent.

Thus, the proposed scenarios were of the type:

The blackout lasts from 18:00 to XX:XX (duration of XX minutes/hours). The proposed discount is Y €.

For each scenario each respondent was then put in front of the option:

- I would accept this interruption, given the proposed discount.
- I would rather have no interruption and no discount.

The data theft choice experiment:

The respondent was asked three questions, referring to a data theft suffered by their electricity supplier. The type of data breach suffered was different in each question, with four different levels of severity. The levels are defined in a cumulative and hierarchical manner, with each subsequent level encompassing the characteristics of the preceding levels while adding an additional dimension.

- 1st level:
  - Personal contact data (personal data, such as telephone number, postal address and email).
- 2nd level:
  - Personal contact data,
  - Consumption profiles (time slots during which electricity is used at home).
- 3rd level:
  - Personal contact data,
  - Consumption profiles,
  - Login credentials (username and password to authenticate the account under which you manage the contract).
- 4th level:
  - Personal contact information,
  - Consumption profiles,

- Login credentials,
- Data related to payment instruments (credit card or checking account) that could be used for money theft.

As for the blackout choice experiment, each breach was associated with a hypothetical discount in the bill as compensation for the inconvenience suffered, which varied in the same amounts, between €1 and €100. Discounts and gravity levels were combined to generate a total of 24 possible scenarios. Each respondent was presented with three scenarios, each featuring a different gravity level, while discounts could be repeated at most two times across the three scenarios.

Thus, the proposed scenarios were of the type:

The data breach results in the theft of X (level of gravity X, with its description). The proposed discount is Y €.

For each scenario each respondent was then put in front of the option:

- I would accept this data infringement, given the proposed discount.
- I would rather have no data infringement and no discount.

In structuring the questionnaires, particular attention was paid to defining the geographic location of respondents. This was done to analyse potential influences from contextual characteristics on responses regarding the perceived value of cybersecurity. The geography of responses, in fact, allows for correlating the collected data with territorial values. These can relate to technical aspects of the electricity service, such as service quality and continuity, but also to broader contextual factors, such as institutional quality, the geography of dissatisfaction, and the level of legality. Special attention should also be given to analysing differences in response profiles between those living in urban, suburban, or rural areas.

Table 1. Reasoned structure of the questionnaire

SURVEY STRUCTURE	**PURPOSE OF THE SECTION**
GENERAL INFORMATION ABOUT RESPONDENTS	
Gender; age; standard of living; marital status; city size of residence; education level; employment.	Control variables to assess the effect of individual characteristics on WTA.
Place of residence: region, province, municipality, postal code.	Questions aimed at geolocating the respondent to evaluate the effect of contextual variables on WTA.
HOUSEHOLD ELECTRICITY USAGE	
Number of people in the household.	Questions aimed at understanding the household's dependence on electricity.
Cost and frequency of electricity bills.	
Use of various types of electrical appliances.	
Presence of children and/or elderly or non-self-sufficient disabled persons in the household.	
KNOWLEDGE AND AWARENESS OF THE ISSUE	
In the past year, have you experienced a power outage/data theft lasting at least one hour?	

Below are some possible inconveniences associated with a blackout/data theft. Indicate which ones you consider the most serious (you can choose up to 5 options).	Awareness of the likelihood and impact of a blackout/data theft can directly influence WTA.
How do you assess the damage caused by a blackout/data theft?	
QUESTIONS ON THE USE OF INFORMATION AND TELECOMMUNICATION TECHNOLOGIES	
A list of questions is provided to generate a composite indicator of digital literacy.	Digital literacy may influence awareness, which in turn affects WTA.

Source: Own elaboration.

2.3 The survey

The survey was administered via CAWI (Computer-Assisted Web Interviewing) between late November and late December 2024 through the system implemented by Qualtrics™. At the end of the data collection, the sample consisted of 770 respondents, each of whom answered four different scenarios.

All data were carefully classified and prepared for statistical processing. As mentioned in previous sections, appropriate measures were taken to ensure truthful and non-random responses. In addition to the response verification systems implemented by Qualtrics™, answers given excessively quickly were removed, as well as response sets that showed highly irrational behaviour in comparing different combinations of blackout duration and financial compensation.

3 CONCLUSIONS

This chapter outlines the methodological framework and implementation of the DCE survey built to estimate the economic value attributed by Italian citizens to cybersecurity events in the electricity sector, specifically blackouts and data theft. Justification for the use of DCE over alternative methods was provided, along with a detailed discussion of design choices intended to mitigate known biases such as ordering effects, cognitive burden, and anchoring. The survey instrument was rigorously developed, incorporating questions on individual and contextual characteristics, household electricity use, and digital literacy, to ensure a comprehensive understanding of factors influencing willingness to accept compensation for service disruptions. A structured and randomized presentation of scenarios was employed to enhance internal validity, while data collection through a representative sample and quality checks ensured the reliability and robustness of the dataset. Together, these methodological decisions support the credibility of the experiment and contribute to the literature on valuing cybersecurity-related disruptions in critical infrastructures and energy services.

4 BIBLIOGRAPHY

Boxebeld, S. (2024). Ordering effects in discrete choice experiments: A systematic literature review across domains. *Journal of Choice Modelling*, 51, 100489. https://doi.org/10.1016/j.jocm.2024.100489

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

Concluding remarks

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
Understanding how individuals perceive the value of their personal data in the electrical energy sector is a relevant topic for two main reasons. First, the question of valuing cybersecurity has, to our knowledge, never been tackled within the electricity sector, which is of great interest especially for assessing the correct value of investments in protecting infrastructures. Second, the new market for individual big data is still subject to uncertainty and imperfect allocation, making our practical study on valuing digital sovereignty for individuals relevant as it is rooted in current challenges. In this way, the last chapter of this Quaderno IRCrES *Cybersecurity and data protection in the electricity sector: state-of-the-art of the literature and evaluation methods* provides a summary of the findings deriving from our extensive literature review as well as past and present experimental activities. We emphasize the theoretical and practical relevance of our representative survey, especially given the strong interest respondents expressed in cybersecurity issues. At the same time, we acknowledge that certain challenges persist and need to be addressed, offering potential lines of research for future projects.

KEYWORDS: Cybersecurity economics, digital sovereignty, electricity sector.

DOI: 10.23760/2499-6661.2025.24_06
ISBN: 978-88-98193-39-4
ISSN (online): 2499-6661

HOW TO CITE
Ragazzi, E., Finardi, U., & Vallette d'Osia, J.C.M. (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

This "Quaderno IRCrES" justifies and describes an approach to gather evidence on the economic value assigned by citizens to cybersecurity in the electricity sector. Due to its technical and managerial characteristics, the electricity system relies on interconnected infrastructures, which can become critical in the event of well-designed cyberattacks. Although the electricity system is designed to be resilient, meaning it can return to a state of equilibrium after a shock, it can happen (and indeed has already happened) that cyberattacks designed to exploit moments of temporary vulnerability or to strike multiple digital control infrastructures in a coordinated manner can lead to a blackout.

The digital infrastructures of the electricity system must therefore be protected with specific countermeasures that involve investments and management expenses. It is thus legitimate to question, on the one hand, what the appropriate level of protection for these infrastructures should be, and on the other one, whether competitive electricity markets, as organized in the European Union, are capable of ensuring sufficient investments.

The extensive literature review included in the first chapters of this Quaderno leads to the conclusion that the provision of the "cybersecurity" good is affected – in general, not just in the electricity market – by market failures, primarily due to information asymmetries, network externalities, and misaligned incentives. The particular characteristics of the electricity sector make these issues even more pronounced, allowing us to conclude that in this sector, so strategic for the economy and society, regulatory intervention is desirable.

Regulating cybersecurity remains, nonetheless, very challenging, whether it involves indicating the path through a series of suggested or required countermeasures or providing economic incentives through cost coverage or the allocation of other types of benefits.

Among the various difficulties inherent in regulatory activity is the need to correctly prioritize protection objectives while avoiding overinvestment, which inevitably translates into higher energy costs. Acquiring information on the value citizens place on protection from cyberattacks on the electricity system contributes to this informational need. The approach described in this Quaderno, as well as the database created through its application, aim precisely to contribute to this need, which until now has not been systematically addressed. Indeed, while numerous studies examine the value of service continuity in the electricity sector, the same cannot be said for the specific case of blackouts caused by cyberattacks.

Assigning some value to a good (in our case, cybersecurity in the electricity sector) that does not have its own market and is not normally subject to exchange is already complicated in itself. It becomes even more so when people's experience with the subject of the investigation is extremely limited. It is therefore necessary to identify techniques that do not directly ask respondents to assign an economic value to the cybersecurity good, as this would be impossible for them, but rather elicit it from the preferences they express indirectly. The chosen technique is that of discrete choice experiments (DCEs), where the respondent is presented with a scenario, imaginary but realistic, and can decide whether to accept or reject the proposal.

In the specific case of evaluating the economic value of cybersecurity in the electricity sector for citizens, the choice scenarios vary in terms of the duration of the blackout and the amount of monetary compensation offered in exchange for the inconvenience suffered. The respondent can decide whether to accept the compensation and the interruption of electricity supply or reject the interruption and forgo the monetary compensation.

Similarly, some scenarios address the topic of digital sovereignty, to assess the value of protecting the personal data managed by electricity operators. Here the choice scenarios vary in terms of the severity of the data theft (additive levels were designed to ensure that the scenarios may be ordered by severity) and of monetary compensation. Considering the discussion of the privacy paradox included in chapter 2 (Vallette d'Osia, Finardi & Ragazzi, 2025), we must be aware that an estimate of the value of individual data protection based on stated preferences may be higher than one based on revealed preferences (hence there is a risk of overestimate). Nevertheless, in the specific situation concerning data on customers (contact data, energy profile data, financial data) managed by the electricity supplier, the respondent does not face any trade-off dilemma (need to accept undesired data sharing because of the high utility placed on the

connected services), neither cognitive limitations, so our estimate might be close to the unobservable real value assigned to data privacy.

The questionnaire, in addition to the core of the choice scenarios, also include questions about the respondent, their use of electricity, their awareness of the consequences of a blackout and cyber risks – variables that can influence their willingness to accept compensation.

The data collection effort resulting from the described approach has made it possible to create a comprehensive database, based on a sample of 770 respondents stratified according to the characteristics of the Italian population by gender, age, and macro-region. The questionnaires yielded a total of 3,080 usable scenarios for descriptive and econometric analyses.

The value attributed to defence against cyberattacks that could lead to a blackout can be indirectly derived from these responses through econometric models. The value will be conditional on individual sociodemographic characteristics, as well as the area of residence. The results obtained from the econometric models can then be used to estimate the social cost of cyberattacks in scenarios that differ in duration and location of the event. This is therefore a significant resource that can be leveraged by public decision-makers for a better understanding of the benefits associated with investments in cybersecurity in the electricity sector.

It should be noted that the low frequency of power outages experienced by Italian consumers might lead them to underestimate the impacts of prolonged blackouts, resulting in a greater propensity to accept economic compensation. Extending the sample to include respondents from other nations, characterized by different risk profiles and levels of electricity service quality, would further strengthen the conclusions drawn from these analyses. By reverse the introduction of GDPR, which affects every day lives of citizen in the European Union might have increased they awareness and above all their expectations in terms of data protection ensured by energy providers. These caveats echo the concept that is the most robust results in the literature review on digital sovereignty performed in chapter 2 (Vallette d'Osia, Finardi, Ragazzi, 2025): results are strongly context specific and may not be easily transferred to other geographical areas or economic sectors or services.

Finally, it is worth highlighting that the questionnaire was very well received by respondents, who generally answered accurately and expressed interest in the initiative. We deduce that the topic of cybersecurity is one that matters even to non-experts, and that they appreciate information and intervention initiatives in this field.

BIBLIOGRAPHY

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

ISSN: 2499-6661

Quaderni IRCrES
Temi e problemi di sostenibilità sociale, economica, ambientale

2025

- N. 23 Verso un invecchiamento attivo, in salute e sostenibile. Quaderni IRCrES 23. Donatella Bramanti, Luisa Errichiello, Greta Falavigna, Sara Nanetti. ISBN: 978-88-98193-38-7

2024

- N. 22 Persistenza dei Residual Earnings e valutazione dell'Equity. Quaderni IRCrES 22. Franco Varetto. ISBN: 978-88-98193-37-0
- N. 21 Cambiamento climatico e sostenibilità: una visione multidisciplinare. A cura di Ugo Finardi. ISBN: 978-88-98193-36-3
- N. 20 Gerolamo Cuneo. Scritti di biochimica 1891-1923. A cura di Grazia Biorci. ISBN: 978-88-98193-35-6

2023

- N. 19 Ambiente, salute e lavoro: analisi empiriche per uno sviluppo integrato. A cura di Franco Nosvelli. ISBN: 978-88-98193-34-9
- N. 18 Caratteristiche statistiche di alcune serie storiche contabili. Franco Varetto. ISBN: 978-88-98193-33-2
- N. 17 Torino creativa. Specializzazioni, impatti e profili di consumo. A cura di Giovanna Segre, Giampaolo Vitali. ISBN: 978-88-98193-32-5

2022

- N. 16 CNR case histories in the Blue Planet Economy. Edited by Giampaolo Vitali, Isabella Maria Zoppi. ISBN: 978-88-98193-29-515
- N. 15 Lo sviluppo locale: un approccio sistemico e generativo con la leadership orizzontale. Erica Rizziato. ISBN: 978-88-98193-28-8
- N. 14 Agile working in Public Research Organizations during the COVID-19 pandemic. Organizational factors and individual attitudes in knowledge production. Edited by Emanuela Reale. ISBN (online): 978-88-98193-26-4 // ISBN (print): 978-88-98193-27-1

2020

- (5)3 Macchingegno: lavoro, scienza, energia tra il XVI e il XIX secolo. Dispensa per gli animatori scientifici dell'Ecomuseo del Freidano. A cura di Grazia Biorci. ISBN: 978-88-98193-20-2
- (5)2 L'efficacia degli incentivi agli investimenti in sicurezza. A cura di Elena Ragazzi. ISBN. 978-88-98193-19-6
- (5)1 Studi miscellanei. Quaderni IRCrES

2019

- (4)2 Studi miscellanei. Quaderni IRCrES
- (4)1 Studi miscellanei. Quaderni IRCrES

2018

- (3)5 Studi miscellanei. Quaderni IRCrES
- (3)4 Studi miscellanei. Quaderni IRCrES
- (3)3 Narrazioni dal Secolo Breve. Ripensare il Mediterraneo. A cura di Antonella Emina. ISBN: 978-88-98193-13-4
- (3)2 Territori e Scenari. Ripensare il Mediterraneo. A cura di Antonella Emina. ISBN: 978-88-98193-12-7
- (3)1 Studi miscellanei. Quaderni IRCrES

2017

- (2)2 The relation between public manager compensation and members of parliament's salary across OECD countries: explorative analysis and possible determinants with public policy implications. Igor Benati, Mario Coccia. DOI: http://dx.doi.org/10.23760/2499-6661.2017.001
- (2)1
  What is the relation between public manager compensation and government effectiveness? An explorative analysis with public management implications. Mario Coccia, Igor Benati.
  DOI: http://dx.doi.org/10.23760/2499-6661.2017.002

ISSN: 2499-6661

2016

- (1)1 Ambiente, salute e lavoro: analisi empiriche per uno sviluppo integrato. Quaderni IRCrES 19. Clementina Bruno, Ugo Finardi, Azahara Lorite-Espejo, Elena Ragazzi.

Pubblicazioni edite dal CNR-IRCrES

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. The Quaderno IRCrES on *Cybersecurity and data protection in the electricity sector: state-of-the-art of the literature and evaluation methods* discusses the economic rationale of a study on the value of cybersecurity and reviews the methods to understand how citizens value cybersecurity when it comes to the essential good of electricity supply. Understanding how individuals perceive the value of their personal data and the continuity of electric supply is a relevant topic for two main reasons. First, the question of valuing cybersecurity has, to our knowledge, never been tackled within the electricity sector, which is of great interest especially for assessing the correct value of investments in protecting infrastructures. Second, the economic appraisal of cybersecurity is still subject to uncertainty and imperfect allocation, making our quantitative study on its evaluation relevant as it is rooted in current challenges.

ISBN 978-88-98193-39-4