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