CNR IRCrES

Who is willing to pay for resilience? An evaluation of households' appreciation of the security of electricity system in Italian regions

Elena Ragazzi (p), Ugo Finardi and Jeanne Vallette d'Osia

Special session S62 - A Changing World: Balancing Economic Growth with Sustainable Energy Transitions

Contents

Why should cybersecurity be interesting for this session?

- Electricity systems (ES) are a key element for energy transition. Most technologies for the green transition rely on electricity, at least in the short and medium term.
- ES reliability and resilience are a requirement for the economic and social sustainability of energy transition.
- Since ES are complex and fully interconnected systems (physical layers), managed remotely through IT systems (digital layers), cybersecurity is one element contributing to ES reliability.
- There has always been debate on the opportunity of imposing a regulation on the cybersecurity for ES, and how to decide the right level of investment to be required by operators.
- Our work wants to contribute to this debate by providing information on the value assigned by private users to the cybersecurity of the ES.

Electricity and cybersecurity

Nowadays cybersecurity (CS) is relevant in all economic sectors, but some features of the ES explain why here we should pay special attention:

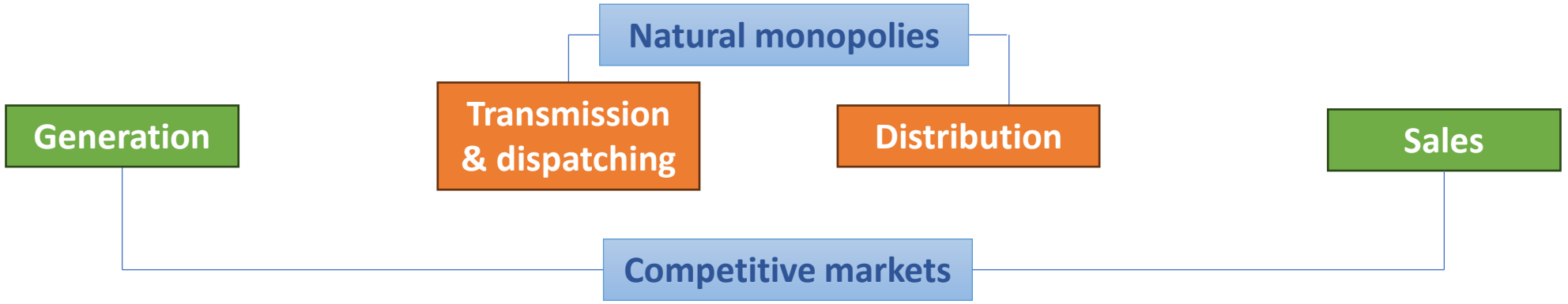
- **Critical infrastructures**. Some technical facilities (High voltage grids, control hubs, huge nuclear plants) are so important that their default can cause huge regional, national or even European (Energy community) blackouts.
- **Interconnected system**. The total level of vulnerability is given by its weakest point (so also private structure may become critical).
- **Data protection**. Energy providers hold personal data of citizens which should be protected to avoid malicious use.

Arguments for a regulation for CS in electricity systems

The discussion on the regulation of CS in ES is rather recent. What has changed?

1. When ES are managed by vertically integrated public utilities the level and type of CS investment is directly bargained between the government and the utility.

In competitive ES, on the other hand:



Regulation might ensure good protection in all the parts of the system.

2. The enlargement of the system. The European Energy Community includes all EU countries plus 9 neighbouring countries. Regulation might ensure that this enlargement will not carry new vulnerabilities into the networked system (lower willingness to pay high bills, higher geopolitical threats, less mature systems…), and might provide a roadmap to follow.

Difficulties in regulating CS

So, why not imposing a EU regulation for CS?

1. Evolving threats require evolving countermeasures. Compliance based systems risk to be out of date by the time they are implemented.
2. Compliance based regulation systems are costly (for the regulator) to implement (huge cost for compliance controls)
3. Performance based regulations lack easy and reliable performance metrics
4. It is difficult to understand the right level of investment, due to the lack of information on the costs and benefits of CS investments.
5. Defence (including cyber-defence) is exclusive competence of member states.

Our research work wants to fill the lack of information of 4, thanks to a data derived from an ad-hoc survey administered to a representative sample of Italian citizens.

Main results – value of cybersecurity

1. The only relevant **individual characteristic** affecting the value assigned to CS is **age**: older respondents are less prone to risk.
2. The **energy-dependence** does not seem to affect the value assigned to CS, unless several vulnerabilities co-exist. The presence of someone not self-sufficient at home (var. “assistance”), as well as not being married or cohabiting (var. “single”), drive positively the acceptance of the scenarios, but their interaction drives it negatively.
3. We do not observe **regional differences** (result robust to different specifications)
4. **Regional differences** in quality of service has no effect on the value assigned to CS
5. The value assigned to **data protection** is higher than the one assigned to protection from blackouts.
6. **Awareness** of potential impacts of blackouts is still low. Having experienced a long blackout (>30’) recently has no effect on the value assigned to protection (variable not significant). However there is low correlation between the answer and official data on black-outs: people do not remember well the black-out occurrence.
7. On the other hand, respondents who recently experienced a data theft tend to assign a lower value to protection. In the case of data breaches, people seem **more afraid of what they do not know.**

Main results - approach

1. The survey-based approach (discrete choice experiment) works, provided it is very well designed.
2. Most answers show good rationalities, very few missing data or inacceptable answers
3. The value given to the protection from cyber-induced blackouts increases with the length of the hypothetical blackout
4. Respondents acknowledged high interest for the topic.

The database may be used to estimate the benefits of CS investment, by calculating the value given to citizens to blackouts of a given duration in selected areas on Italy, or of different types of data breaches.

From where we start

Some research questions are based on evidences obtained by past projects:

“ESSENCE” - cost benefit analysis of the adoption of CS standards: in the two case studies (Italy, generation; Poland transmission), even though benefiths are much higher than costs, **consumer** benefits are MUCH GREATER than those for electric system **companies**.

Cybersecurity costs are afforded by electricity companies, but **returns** on investment for cybersecurity for the companies are **insufficient.** In competitive markets these externalities may cause sub-optimal level of investment.

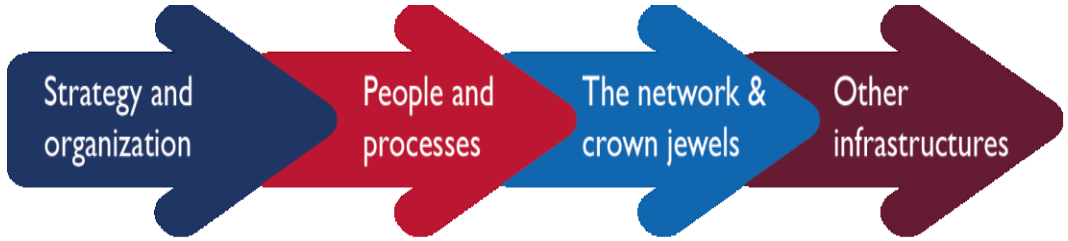
ITALIAN CASE STUDY

BENEFIT		COST	Delta	No protection
Electricity not sold	2	Investment	20-40	28-53
Non-households	35-46	Maintaining	3.5-6	6.5-12.9
Households*	36-52.5-64			
TOTAL	73-112			

POLISH CASE STUDY

BENEFIT		COST	Delta	No protection
Electricity operators	0.7	Investment	7.5	26
Non households	25-35	Maintaining	2.5	5
Households*	30-52-61			
TOTAL	55.7-96.7			

Source: Trial evaluation: conclusive lessons from Essence case studies
Fernando García Gutiérrez, Elena Ragazzi



Source: EVALUATING THE PRUDENCY OF CYBERSECURITY INVESTMENTS: Guidelines for Energy Regulators , USAID Bureau for Europe and Eurasia, E.Ragazzi (ed.)

“Guidelines for Energy Regulators”:

Guidelines developed for the regulators of the Black Sea Area countries (Georgia, Armenia, Moldova, Ucraine). They provided **approaches** for energy regulators to set up cybersecurity regulation according to **sound** and **economically feasible principles**.

They underline the need for benchmarking values for the fine tuning of regulation.

Insights from the literature: Economics of CS, theoretical & multidisciplinary studies

Numerous approaches to cybersecurity **cost estimation** and **investment optimization**:

- Franco et al. (2024): **Real Cyber Value at Risk** (RCVaR) approach based on real-world information from public CS reports combined with methods to predict the costs and associated deviation of cyberattacks on companies.
- Dash et al. (2024): **Game-theoretic model in** a **two-stage supply chain**, to study investment decisions when **multiple firms are interconnected**. The optimal level of investment differ according to the **type of attack** (opportunistic vs. targeted).
- Lee (2021): **Cyber risk management framework** to target macro-level CS issues and quantitative risk assessment methods, organized in 4 layers: cyber ecosystem – cyber infrastructure – cyber risk assessment and cyber performance.
- Massacci et al. (2016): **CS public policy model** that captures the hybrid nature of the regulations oscillating between **risk- and rules-based systems** for critical infrastructure operators.

Considering critical infrastructures:

- Rulleau (2023) assessed the preferences of residents (WTP) with regard to the **resilience of a drinking water distribution network** subject to a cyber-attack, through a **Discrete Choice Experiment survey**. She highlights the importance of knowledge and the influence of risk-perception on choices.

Insights from the literature: Economics of CS: data protection

However, proposed models for CS investment mainly have limitations (**limited scenarios, inconsideration of constraints, type of organizations and adversaries' strategies etc**.). There is a need for accuracy and simplicity for CS economics to create a resilient cyber environment. (Kianpour et al., 2021)

What about the analysis of **personal data breaches**?

- Yamaguchi et al. (2020) test three hypotheses regarding the data utilization of online services, through a **Contingent Valuation Methods (CVM)**. They elucidate a **privacy paradox**: though concerned about the use of data, people continue to use online services due to their convenience. It illustrates the importance of the role of **digital literacy** and the role of **service providers to offer different options of data utilization**.

- Blythe et al. (2020) study **digital sovereignty for individuals** by estimating consumer's (willingness to pay **for the security of different Internet connected products (Internet of Things),** also through a **CVM**. Their findings corroborated earlier studies which found that customers are **willing to pay more for secure products and services.**

An extensive literature review will appear in September in the "Quaderni IRCrES" series.

Insights from the literature: The economic nature of CS

Public goods are those goods presenting social and economic **utility,** but which are not tradeable and thus **priceable** because they are non rivalrous and excludable.

Defense (= security from external attacks) is the clearest **example** of a public good.
This does not hold properly for CS, which can be excluded in some cases.

Nevertheless, in the case of ES market failures emerge affecting the good allocation of resources and making it impossible to rely on prices as signals of value.

The value of CS has to be estimated, relying on the **methods of cost-benefit analysis.**

	Excludable	Non-excludable
Rivalrous	**Private good** *Clothes, toothbrush*	**Common goods** *Fish, timber*
Non-rivalrous	**Club goods** *Private parks, cable TV*	**Public good** *Clean air, defense*

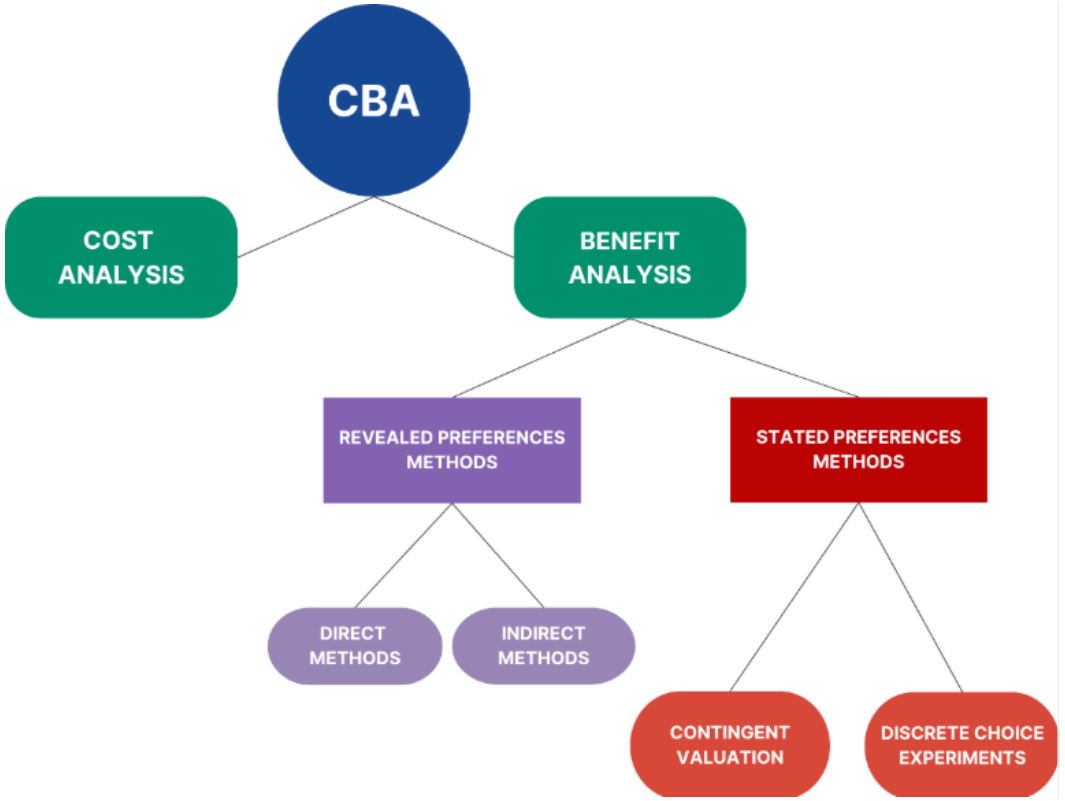
Approaches in the estimation of the value of CS

We opted to:

- Rely on **discrete choice experiments** rather CV, who are better in the case of goods for which the respondent has little personal experience.

- Rely on the concept of **willingness to accept** (a compensation for a damage) rather than willingness to pay (for the protection), because literature indicates that this is better when the respondent is in the position to suffer a loss from the event in the scenario.

In DCE respondents immerse themselves in hypothetical scenarios. They 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.



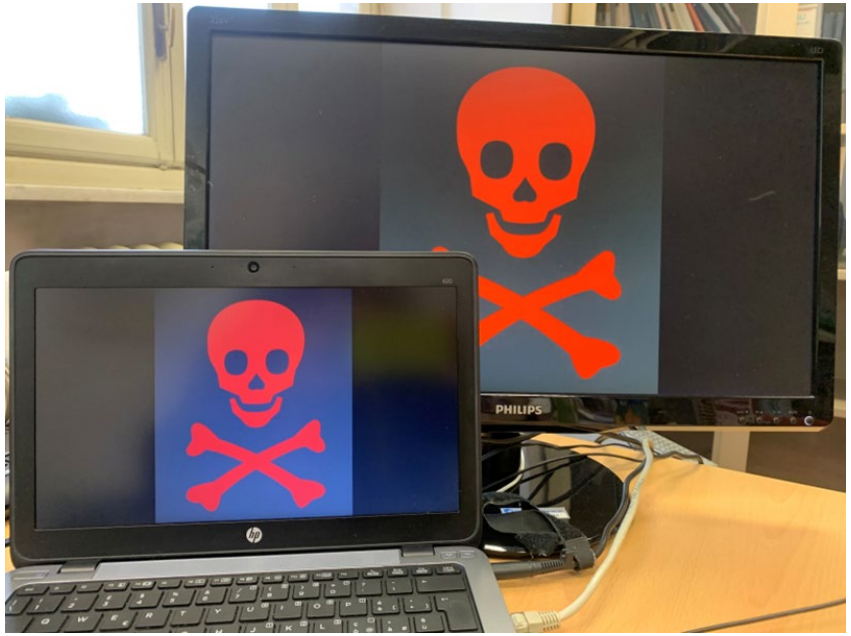
Our step forward

We succeeded to build a completely new database able to study the value of the most relevant aspects of CS for the electricity system: **protection of the controls of critical infrastructures** and personal **data protection**. This was possible thanks to two projects .

Scenarios include blackouts of different duration and different types of data theft.

We designed a survey on a large sample of Italian citizens (N= 750, sample quotas as in Italian population by gender, age and macroregion).

This will allow to estimate several “benefit scenarios” based on the real characteristics of the population potentially affected by the cyberattack.



Experimental approach: the questionnaire

General information on the respondent:

Gender, age, standard of living, marital status, dimensions of the town, qualification, job	→	**CONTROL VARIABLES**
Location (region, province, municipality, ZIP)	→	**TO ASSESS THE EFFECT OF CONTEXTUAL VARIABLES**

Variables on the use of electricity and of digital technologies:

Number of persons in the household, cost of the electric bill, use of electric appliances, presence of children/non-self-sufficient elderly or disabled persons	→	**TO ASSESS THE EFFECT OF INCREASED DEPENDENCY ON ELECTRICITY OR DIGITAL TECHNOLOGIES**
Questions on the use of internet and digital technologies		

Questions on the use of digital technologies and Internet are taken from the Istat "Indagine multiscopo sulle famiglie", which will allow to use data referred to the Italian population (or also to EU countries from Eurostat) as benchmarking values

Questions on the awareness of the specific problem of electric blackouts and digital sovereignty	→	**AWARENESS MAY DIRECTLY AFFECT THE WTA**

Experimental approach: the choice sets

In the DCE part of the questionnaire, respondents face some **scenarios** (cyberattacks to electric system and data storage); each scenario considers a monetary **compensation** for the occurred **inconvenient** (blackout or data breach) which can be accepted or not.

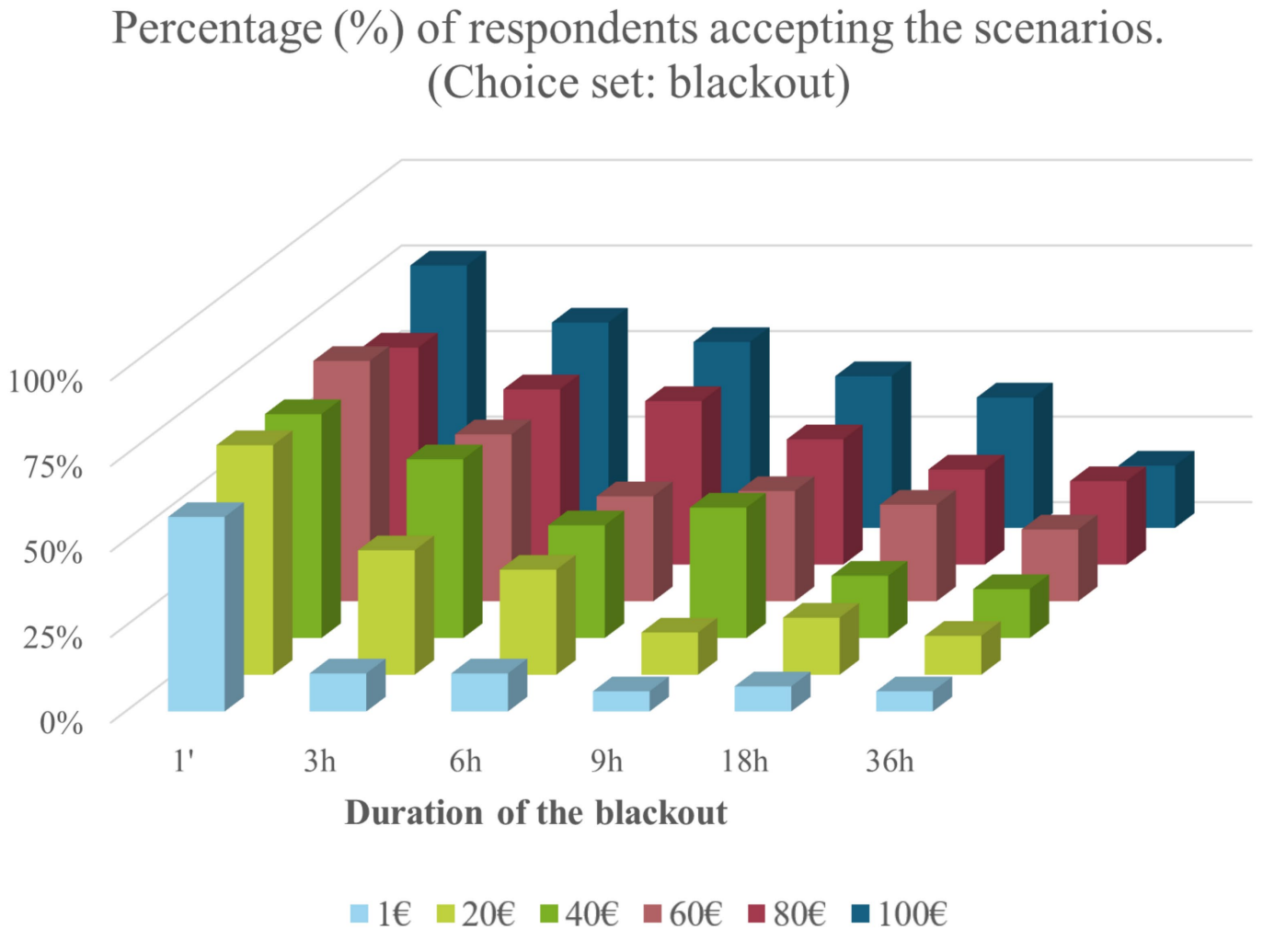
The two sections (on electricity and data protection) and the scenarios are allocated **randomly**.

- 4 **blackout** scenarios for each respondent; each scenario presents:
  - 6 different durations (from 1 minute to 36 hours).
  - 6 different levels of compensation (from 1 Euro to 100 Euros).
- 3 **data breach** scenarios, entailing:
  - The theft of 4 different types of data (going from personal contact data to credit card or bank account).
  - 6 different levels of compensation (again from 1 Euro to 100 Euros).

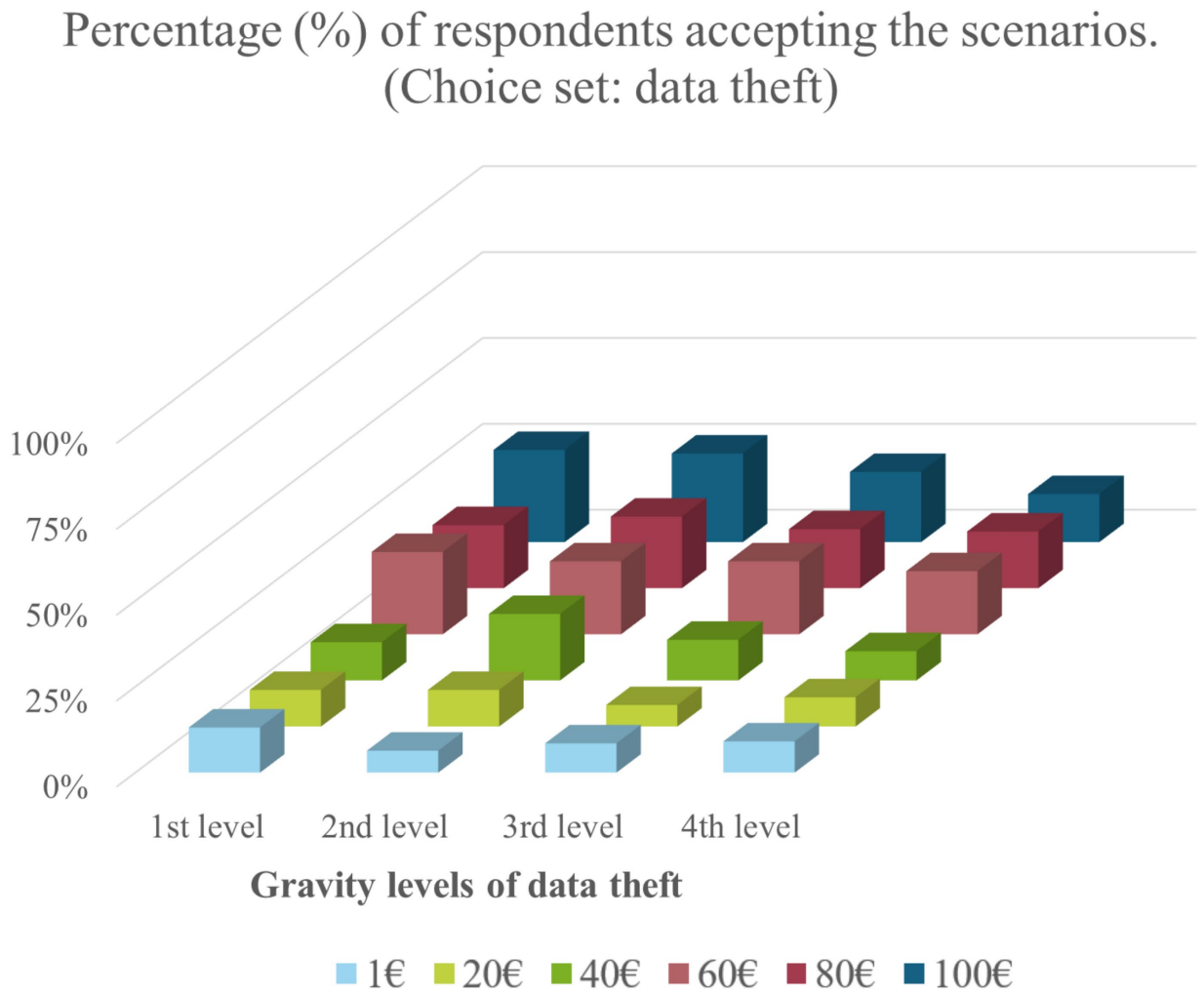
Some preliminary results: word cloud from respondents

The (optional) answers to the final open question asking for remarks acknowledge the interest of the population for the topic

Results: descriptive analysis - BLACKOUT

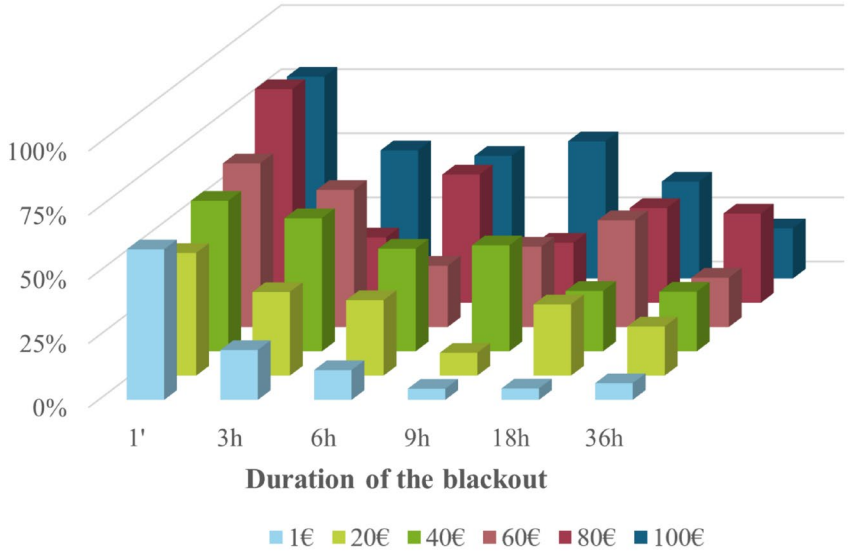


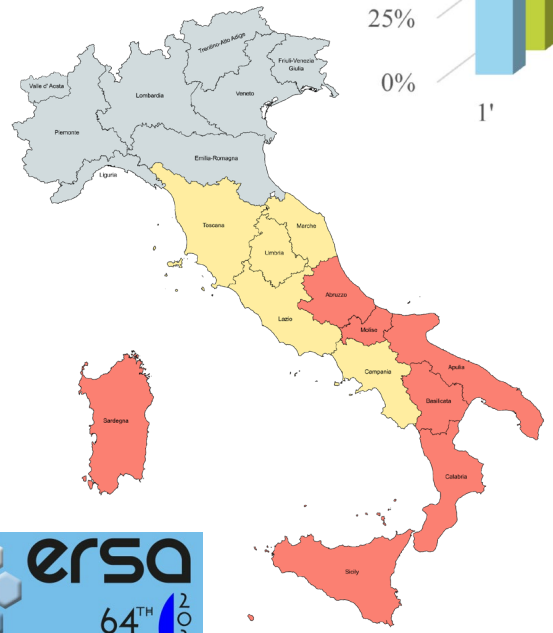
Results: descriptive analysis – DATA THEFT



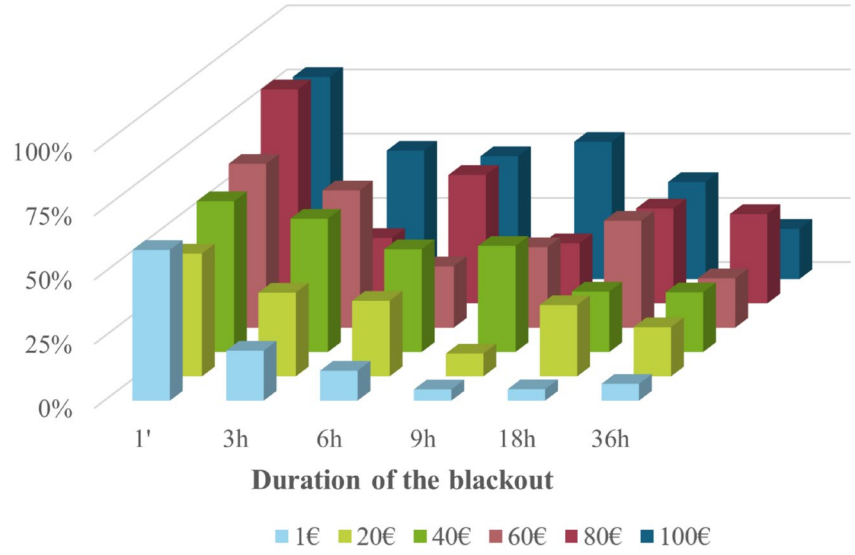
Results: descriptive analysis – REGIONAL PATTERNS

Percentage of respondents living in the **Center, South and Islands of Italy** accepting the scenarios (Choice set: blackout)





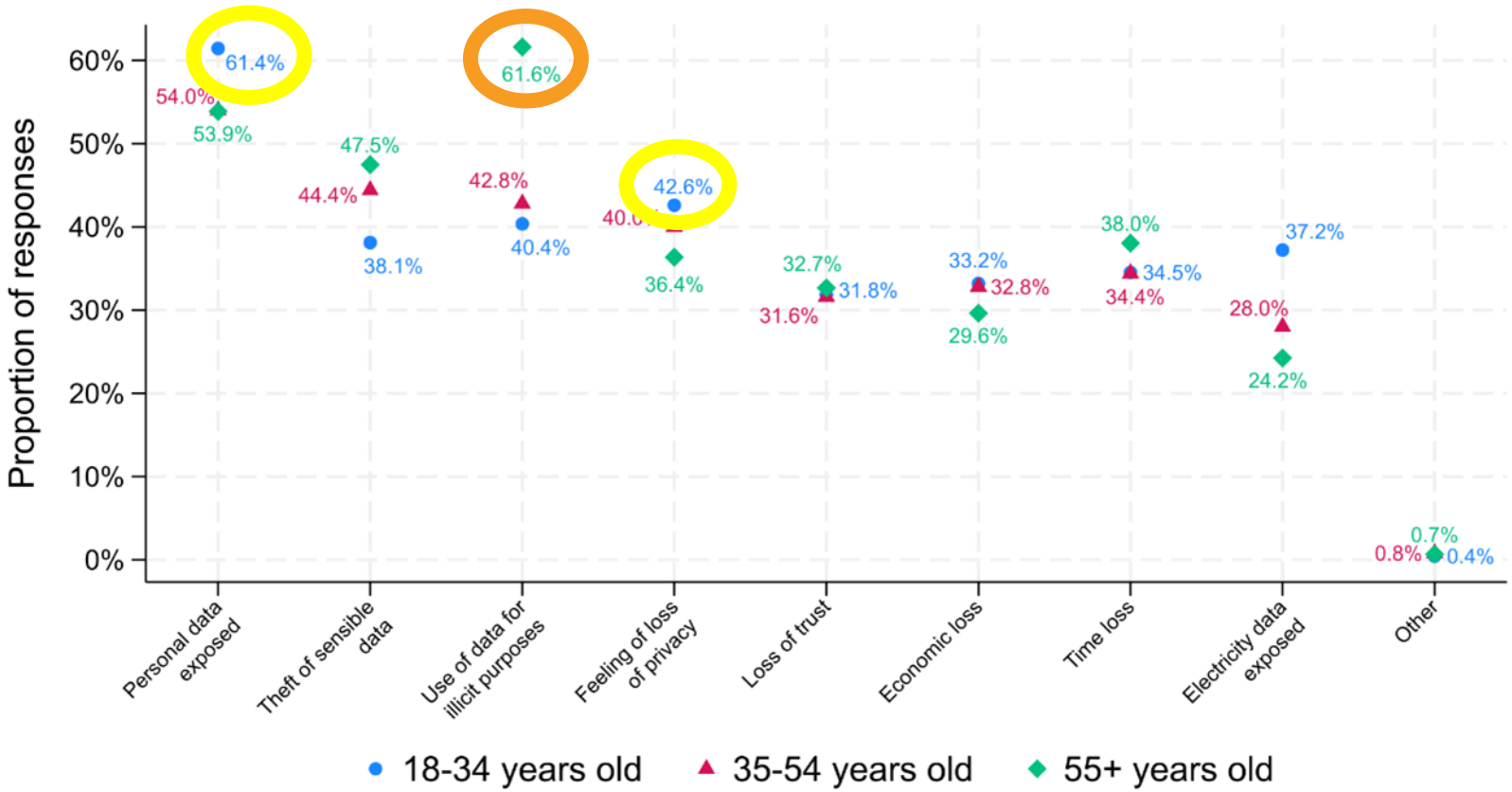
Percentage of respondents living in the **Center, South, and Islands of Italy** accepting the scenarios (Choice set: blackout)



ersa 64TH CONGRESS 2025

RESULTS: descriptive analysis – AGE PATTERNS

Answers to the Q°: "In the event that a supplier or a platform you use becomes the victim of a data breach or theft, which of the following potential problems or inconveniences do you think would have the most serious consequences for you? *(You may select up to 5 options.)"*

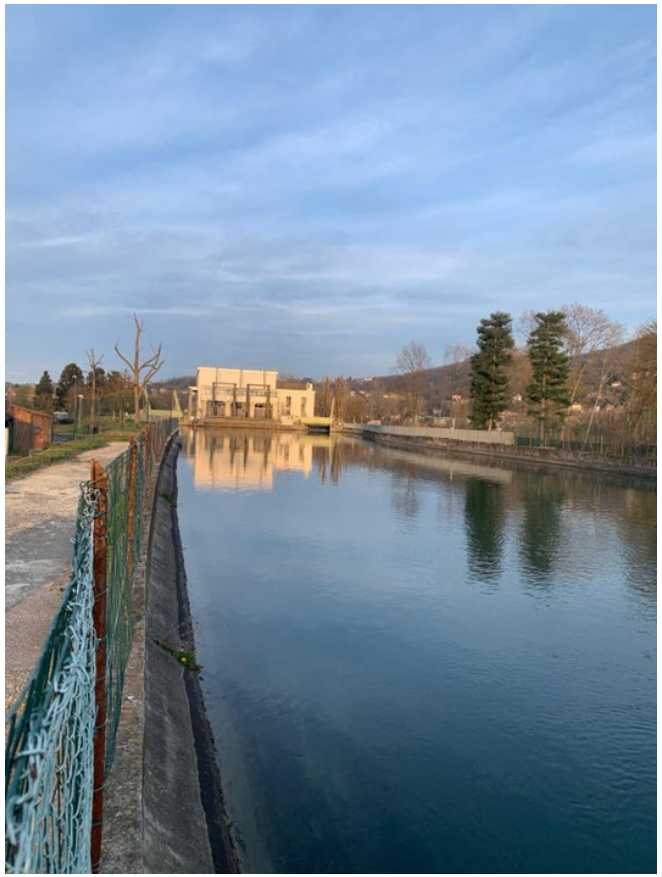


Results: Econometrics

Logit model (dependent var.: accept/not accept the proposed scenario/discount).

Independent variables:

- Variables on the individual:
  - About the age, gender, education level, marital status…
- Variables on the household.
  - On the territory of residence (macro-area, inner area, urban/rural gradient),
  - On the presence of persons requiring assistance at home (elderly, handicap or sick person non auto-sufficient, children below the age of 10 y.o.),
  - Whether water and/or heating system is powered with electricity at home.
- Variables on electricity features:
  - Of the household (size of the bill, occurrence of a blackout in the last year),
  - Of the territory (SAIDI-SAIFI).
- Variables on the use of internet:
  - Of the household (occurrence of a data theft, frequency of use of Internet).



RESULTS: Model

Dependent variable: accept the blackout and the proposed compensation

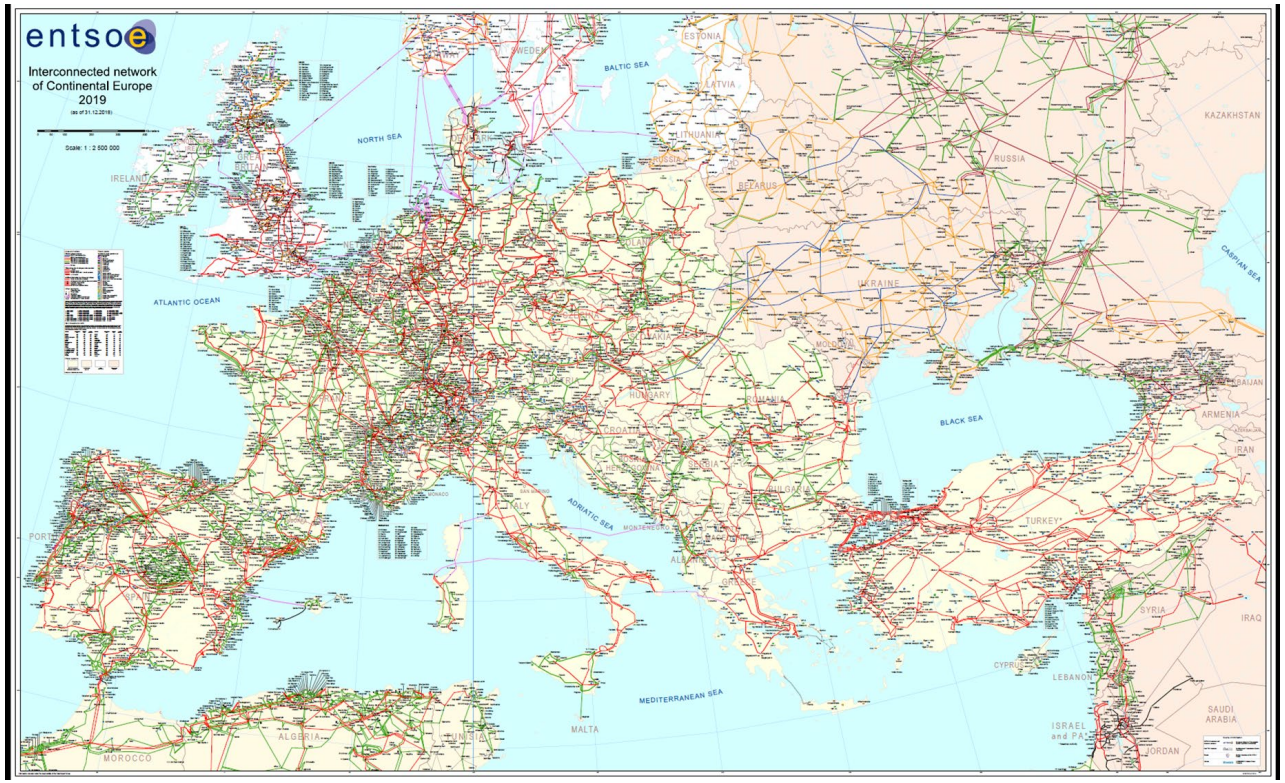
Standard errors in parentheses:

* p < 0.1,
** p < 0.05,
*** p < 0.01

Observations: 3012

discountBO	0.0314***	Middle level education	0.0917
	(0.00463)		(0.194)
discountBO²	-0.000152***	High level education	0.228
	(0.0000414)		(0.206)
timeBO=3	-1.080***	Single	0.361***
	(0.129)		(0.125)
timeBO=6	-1.500***	Assistance	0.428***
	(0.142)		(0.158)
timeBO=9	-1.788***	Interaction single#assistance	-0.714**
	(0.142)		(0.286)
timeBO=18	-2.109***	Water elec.	0.271**
	(0.149)		(0.117)
timeBO=36	-2.592***	Inner area	0.0895
	(0.172)		(0.156)
Woman	0.137	Saidi	0.00115
	(0.109)		(0.00356)
Age 55+	-0.426***	North Italy	-0.0370
	(0.124)		(0.119)
		Constant	-0.649**
			(0.298)

Future research



- Extend the survey to other countries to take into account differences in:
  - Consumption patterns,
  - Electricity costs and other economic variables,
  - ES features,
  - Society, values, geopolitical situation.

- Improve the model
  - Include new variables (territorial)

- Calculate some scenarios (eg. blackout of 6 hours affecting the Lombardy region or data theft concerning the customers of a large distributor/vendor)

- Suggestions?

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

Authors

Elena Ragazzi elena.ragazzi@ircres.cnr.it
Ugo Finardi ugo.finardi@ircres.cnr.it
Jeanne Vallette d'Osia jeanne.vallettedosia@ircres.cnr.it

Contributors

Graziano Abrate
Clementina Bruno
Fabrizio Erbetta

Funded by:

- the European Union - Next Generation EU and by the Ministry of University and Research (MUR), National Recovery and Resilience Plan (NRRP), Mission 4, Component 2, Investment 1.3, project "SEcurity and RIghts in the CyberSpace (SERICS)" (PE 0000014). All Authors are part of SERICS foundation.
- Progetto Ricerca di sistema nel settore elettrico - Piano Triennale 2022-2024 – 2.1 PROGETTO INTEGRATO CYBER SECURITY DEI SISTEMI ENERGETICI.

Thank you for your attention.

ersa 64TH CONGRESS 2025

CNR IRCrES Istituto di Ricerca sulla Crescita Economica Sostenibile

Special issue on impact evaluation

A special issue has been launched starting from the experience of this special session:

- ✓ **Title:** **The unexpected effects of policies on cities and regions**
- ✓ **Journal:** **The Annals of Regional Science (AoRS, I.F. 2.1)**
- ✓ **Call:** **https://link.springer.com/collections/jdeaafjjei**
- ✓ **Submission schedule:** **open until 15 November 2025**
- ✓ **Guest editors:** **Sébastien Bourdin, Elena Ragazzi, Lisa Sella**

We welcome contributions that analyze these often-underestimated side-effects to enhance our understanding of the interactions between policy decisions and local realities. The goal is to uncover how policies, even those not explicitly designed with territorial intentions, shape the spatial and socio-economic fabric of cities and regions, sometimes in unexpected ways. We encourage contributions that employ rigorous quantitative and theoretical approaches to explore these dynamics in different geographical and political contexts.