# Iberian Blackout: Communication Meltdown

## with serious human and economic consequences

Author
**Maryse Rebillot**

**September, 2025**
www.ozngo.com

# Table of Content

# Forword

The blackout that affected Spain on April 28th 2025 revealed, once again, the fragility of our interconnected infrastructures.

Beyond the technical incident, it was **crisis communication—or the lack thereof—that left a lasting impression and undermined confidence**.

It's astonishing that such a long-anticipated, high-impact scenario still caught key energy providers unprepared from a communication standpoint.

During the same period, communication tools have become more sophisticated and cyberattacks have skyrocketed, factors that make it essential to strengthen crisis preparedness, particularly in terms of communication with internal and external stakeholders, and especially in critical infrastructure such as energy suppliers.

This document provides a structured overview of the facts, the mistakes made, and the consequences for the various public and private stakeholders.

Above all, it highlights the measures that companies can implement today to strengthen their resilience in the event of a major outage.

## About the Author

Maryse Rebillot is Strategic Cyber Communication & Leadership Advisor, and Oz'n'gO founder.

Her conviction: cyber threats put people back at the heart of management strategies and decisions.

With over 20 years of experience in marketing and communications in high-tech and cybersecurity, she combines expertise in crisis management with a solid international network of experts in various fields (cybersecurity, AI, data governance, media, legal, etc.).

With an International Executive Marketing Master's degree (INSEAD), she helps organizations build resilient cultures to boost engagement and cohesion within the business ecosystem.

## Timeline of Events

- 12:33 CEST: 15 GW 2 subsequent grid failings, suddenly brought down the European grid — 60% of Spain's energy demand.
- Massive outages begin across Spain, Portugal, and southern France.
- Parts of Greenland lose all communication capabilities.
- Internet services in Morocco are disrupted.
- round 4:00 pm CEST: Red Eléctrica de España - REE announces power restoration may take 6 to 10 hours.
- Half past midnight: Greenland's telecommunications provider, Tusass, issues a statement informing the public that contact has been lost at their connection in Maspalomas, Spain.

In the meanwhile, big cities, hospitals, streets, people were panicking. What happens? Why? For how long?

## First Statements about the blackout

- REE issues at 4:00 pm a message on Twitter, saying the cause is under investigation.
- Iberdrola's CEO Ignacio Sánchez Galán speaks later, blaming REE and affirming Iberdrola's readiness.
- REN, Portugal's grid operator, refers vaguely to a "rare atmospheric phenomenon."

## Porte-paroles identifiés

- **Beatriz Corredor**, REE's president, appears days later to defend the company's crisis response.
- **Ignacio Sánchez Galán** (Iberdrola) calls on REE to explain the incident, rejecting all responsibility.
- **Bruno Silva** (REN) clarifies to AFP that REN never referred to the incident as atmospheric and distances the company from that claim.
- **João Faria Conceição**, board member at REN, provides some technical insight into the event.
- Spanish Prime Minister **Pedro Sánchez** criticizes the lack of transparency from operators.
- The Environment Minister warns against blaming renewable energy sources.
- No early-stage press briefings or spokespersons from **REE** in the crucial first hours.

## Serious consequences of communication failures

At least **eight deaths** in Spain and Portugal, **+6 million people affected** in public transport, elevators, parking lots, shops, etc. According to a study by Caixabank Research and the Spanish Ministry of Economy, the **direct economic impact is estimated at €400 million**, but the Spanish Business Confederation (CEOE) has estimated that **the outage could cost ~€1.6 billion** (or ~0.1% of Spanish GDP). Reuters

# 4 MAJOR COMMUNICATION FAILURES

- **Lack of Anticipation**
- **Missing Prioritization & fragmented communication**
- **Non-Compliance with Blackout Regulation**
- **Public Confusion and Mistrust**

## 1 - Lack of Anticipation

- **Late communication** with a first public message 4 hours after the blackout began.
- **No coordinated communication between the major players** (REE, REN, and Iberdrola), but rather accusatory communication towards each other. The only coordination was technical, to ensure the stability of the Iberian electricity grid.
- **No pre-approved adapted message for affected countries or stakeholders.**
- **Few, if any, redundant communication tools** prepared for large-scale outages (e.g. SMS, emergency radio, low-bandwidth apps, satellite phones) to inform the various strategic or critical contacts (public transport, for example). The result: an intense, time-consuming communication blur.
- **No dedicated multilingual platform** to centralize updates for affected populations. We found NONE. This would have made it possible to provide blackout victims with information on the analysis of the current situation, but even more so with a list of contacts according to requests, possible compensation measures, etc. etc.
- **No counter-messaging strategy to anticipate misinformation or rumors** (cyberattack? nuclear shortfall? renewables failure?), otherwise prior messages would have been sent to reassure and show control of the situation, not denials.

### Note

The major DSOs, including Iberdrola, have asked to take part in the crisis committee set up by the Spanish government to investigate the blackout. They have also requested full access to the data held by REE to understand the causes of the incident… without success (Iderdrola press release dated Apr. 29).

REE's CEO and her management team normally have Iridium or Inmarsat satellite phones, independent of the GSM network, which enable voice communications, encrypted SMS or secure messaging without a local power grid.

## 2 - Missing Prioritisation & fragmented communication

FAILED

No clear strategy has been deployed on information priorities according to audience, either by :

- Country (Portugal, France, Greenland, Morocco)
- Audience type & criticality (Government, critical partners, companies, citizens)
- Technical level (general public vs. technical stakeholder)

### Prioritisation by country

When serving several countries, it's crucial to prioritize them according to their criticality. Here, Portugal was the top priority. France came second, closely followed by Greenland, and finally Morocco.

REE maintains operational relations with RTE (France), REN (Portugal) and the Office National de l'Électricité et de l'Eau Potable (ONEE) in Morocco. As for Greenland, operations are managed directly from Maspalomas in the Canary Islands. However, there was no coordination on the type of messages to be sent to specific audiences, in their own language, at each phase of the crisis. This lack of communications coordination contributed to delays, inconsistencies and total confusion in international communications during the crisis.

#### Communication with Portugal

At the technical level, operational inter-connections were deactivated to protect the national grids, which operated autonomously in the days following the blackout.
Electricity was gradually restored thanks to the Portuguese capacities, notably the Castelo do Bode hydroelectric plant and the Tapada do Outeiro natural gas plant.
Public communication was widely criticized for its lack of responsiveness, clarity and coordination about what was going on. The Portuguese government has requested additional information from power system operators to clarify the causes of the blackout.

#### Communication with France

France experienced brief but significant power cuts that affected the French Basque Country for around 20 minutes. RTE quickly restored power thanks to safety measures. Again, the six interconnection lines with Spain were cut. Once the situation had stabilised locally, France progressively re-supplied Spain, reaching up to 2,000 MW of exports.
Public communications, too, have been criticised for their lack of responsiveness and consistency, and while the Spanish Prime Minister acknowledged France's assistance, REE has not issued a public statement specifically thanking French support.

### Communication with Greeland

Several isolated communities such as Qaanaaq, Ittoqqortoormiit and Tasiila lost access to the telephone network, internet, television and radio between 6:30pm and 12:36am (local time). Telecommunications services were restored on the night of April 28-29, after the connection with satellite equipment was restored. Although the satellite ground station in Maspalomas remained operational, the data cables connecting it ran through mainland Spain and were affected by the power outage, leading to the service disruption in Greenland.

No public record of direct communication or coordination between Red Eléctrica de España (REE) and Tusass regarding this incident.

### Communication with Morocco

The country escaped the domino effect of the blackout thanks to the automated defenses of its power system. At the time of the blackout, Morocco was importing around 778 MW of electricity from Spain. The disconnection maintained the stability of the national power system. However, despite the stability of the power grid, disruptions were reported to digital services (internet access) and air transport with the cancellation of some forty flights and disruptions to baggage delivery. After securing its own grid, Morocco provided assistance to Spain by exporting up to 519 MW of electricity, i.e. around 11.5% of its available capacity, which was crucial for the gradual restoration of the Spanish power grid.

Pedro Sánchez reaffirming Morocco's key role in restoring electricity to Spain.
Morocco World News, May 7th 2025

Note

- No press release from ONEE has been issued
- No coordination in communication with REE.
- Up to now, only Spanish Prime Minister, Pedro Sánchez, thanked Morocco.

FAILED FAILED
FAILED
FAILED FAILED

## Prioritisation by Type & Criticality

- Authorities
- Critical service providers and partners
- Companies
- Citizens

## Authorities

### REE & Spanish Goverment

REE, like all strategic critical infrastructure operators, is connected to an emergency telephone network with the Prime Minister's office (the Moncloa for Spain).

Despite these protocols, President Pedro Sánchez expressed his dissatisfaction with REE's lack of transparency. He called an emergency meeting with the heads of REE and other electricity companies to demand explanations and immediate cooperation. With the Ministries of Transport, Health, and Infrastructure, communication channels have been established between REE and the relevant ministries to coordinate actions in the event of a crisis.

### REE & the EU

REE naturally activated the planned protocol, but never coordinated with the European Union. The EU's involvement came after the fact, with a debate scheduled in the European Parliament on April 30.

## Critical Service Providers & Partners

Critical service providers: hospitals, public transportation, banks and finance, telephone operators, internet service providers, fire departments, police, prisons, wastewater treatment plants (the last four cases are not studied here, but we know that the repercussions were very tense).

Critical partners: large companies, critical SMEs, employer federations, charities, NGOs, etc.

Communication with these parties was generally slow, vague and inadequate, with disastrous consequences.

FAILED

| SERVICE PROVIDER | IMPACT | COMMUNICATION CHAIN | REMARKS |
|---|---|---|---|
| **Hospital** | Power outage lasting **+8 hours** forcing Hospitals have activated their **emergency generators** to ensure continuity of care. However, these systems **have their limitations**.<br>**Only critical services** (emergencies, life-saving care) **maintained**.<br>**Electronic records were inaccessible**.<br>**Temperature-sensitive medications** (vaccines, insulin, etc.) **at risk** due to cold cuts.<br>**Seven deaths in Spain and one in Portugal** due to the shutdown of respiratory assistance equipment, a fire caused by the use of candles, and carbon monoxide poisoning from an electric generator inside a house. | Public hospitals and large private hospitals have redundant internal communication networks (radio, landline telephony, secure local messaging).<br>However, they do not have any direct satellite connection to REE.<br>All information communication is carried out via:<br>- regional emergency centres (Protección Civil / CCAA).<br>- priority lines in the event of activation of the Plan Nacional de Emergencias<br>- the Ministry of Health communicates with REE to prioritise power supply, which is probably why no disasters have been reported. | The coordination with ambulances and firefighters has been severely compromised.<br>Conclusion: The resilience of healthcare systems must be considered a dimension of national security with a need for:<br>• decentralized energy solutions, digital redundancy, and integrated command between healthcare, civil protection, and defense.<br>• planning, audits, tested scenarios, etc.<br>source: PMC |
| **Banks & Finance** | ATM: Most cash machines broke down as soon as their backup batteries ran out, making it difficult for many users to access cash. As a result, withdrawals fell by 45% compared to unaffected regions such as the Balearic Islands, the Canary Islands, Ceuta and Melilla.<br>E-payments: Payment terminals (dataphones) stopped working, forcing retailers to accept only cash payments. 54% drop in e-commerce.<br>Online banking services: Although online banking remained operational, its use was limited due to power cuts and telecommunications network outages. | Large banks (BBVA, Santander, etc.) have autonomous IT continuity systems (servers, data centres). Some have their own emergency satellite connectivity, but this is directed towards their data centres and regulatory authorities (BdE, ECB), not directly towards REE.<br>Communication with REE or network operators is carried out via the National Securities Market Commission (CNMV) or cross-sector business continuity protocols. | No direct communication between REE and banks and financial institutions. Some have activated their business continuity plans, notably by mobilizing emergency teams and strengthening communication channels with customers.<br>Regulators closely monitored the situation to ensure the stability of the financial system and considered measures to strengthen the resilience of critical infrastructure.<br>ZERO PUBLIC COMMUNICATION from banks to inform their customers. This lack of communication contributed to panic among the public, who rushed to ATMs. |

FAILED

| SERVICE PROVIDER | IMPACT | COMMUNICATION CHAIN | REMARKS |
|---|---|---|---|
| **Public Transports** | Public transport in Spain and Portugal was severely disrupted, highlighting flaws in emergency communication between critical infrastructure operators and transport authorities.<br>Spain: All trains were stopped, affecting approximately 35,000 passengers. Metro lines had to be evacuated, and traffic lights stopped working, causing traffic jams and accidents.<br>Portugal: The Lisbon metro, trains and traffic lights were paralysed. Mobile networks also suffered severe limitations, hampering communication. | Operators such as Renfe (trains), Metro Madrid and EMT (buses) have autonomous control centres and sometimes independent radio lines, but no satellite telephone connection to REE.<br>In theory, during such a crisis, communication should follow this chain:<br>1 - REE informs the Ministry of Transport via a secure line.<br>2 - The Ministry activates the CECOR (Operational Coordination Centre) or the CNPIC (National Centre for the Protection of Critical Infrastructure).<br>3 - These centres coordinate with public transport operators to disseminate information and manage the crisis. | Despite this structure, communication was slow and ineffective:<br>- Passengers were informed late, often via the media or social networks, due to the failure of transport information systems.<br>- Transport operators did not receive clear instructions in a timely manner, exacerbating the confusion. |
| **TelCo & Internet** | 📉**Drastic drop in Internet traffic**.<br>In Spain, an immediate decrease of approximately 60% was observed, reaching an 80% drop within five hours of the outage beginning.<br>In Portugal, traffic fell by half immediately after the outage, reaching a 90% drop within five hours.<br>(The Cloudflare)<br>📞 **Mobile phone service disruptions**<br>In Spain, mobile phone services were interrupted, making communication difficult.<br>In Portugal, severe limitations to mobile networks were reported, particularly for voice calls. | Operators (Movistar, Vodafone and MasOrange) use relay antennas installed on sites belonging to specialised companies (called 'torreras') such as Cellnex, American Tower, Vantage and Totem. These sites generally have backup batteries that provide 2 to 3 hours of autonomy in the event of a power cut.<br>However, during the blackout, the sudden increase in telephone and Internet traffic reduced this autonomy, leading to an almost total breakdown of the mobile network at around 5 p.m. (El País). | Communication with telephone operators and internet service providers was limited, both technically and publicly. Operators had to manage the situation independently, without clear guidelines from REE.<br>Their communications were criticised by the public for their lack of clarity and responsiveness.<br>Messages were often technical and inaccessible to the general public, which contributed to confusion and the spread of rumours. |

## Companies

All Spanish companies, beyond the energy sector, have widely criticised REE for its inadequacy and lack of coordination. This coordination, beyond understanding the causes of the failure, enables joint development of solutions to prevent similar incidents in the future.

Operational disruptions: Companies were unable to anticipate or respond quickly to the effects of the blackout, resulting in service interruptions and economic losses.

Loss of confidence: The lack of transparency eroded companies' confidence in REE and the authorities, complicating crisis management.

Coordination difficulties: Without clear information, businesses struggled to coordinate their actions with those of the authorities and other players in the sector..

Bloomberg reports that in Spain, the **blackout may have "wiped out" nearly €400 million** from the economy, according to an estimate by Caixabank, but the Spanish Business Confederation (CEOE) estimated that **the outage could cost ~€1.6 billion** (or ~0.1% of Spanish GDP). Reuters

| Secteur / type d'entreprise | Impacts / pertes signalées |
|---|---|
| Agroalimentaire / viande / produits frais | **Pertes estimées jusqu'à 190 millions €** dans l'industrie de la viande (réfrigération perdue, denrées abîmées) |
| Repsol / secteurs pétrochimiques et raffinage | Repsol dit avoir subi **~175 millions € de pertes** dues au blackout et autres interruptions d'alimentation électrique. |
| Refineries / huile / énergie secondaire | L'entreprise "Moeve" (anciennement Cepsa) a déclaré une **chute de bénéfice (~19 %)** pour le premier semestre 2025, en lien avec l'impact de la panne sur ses raffineries. |
| Assurance / interruption d'activité | Morningstar DBRS a estimé les **pertes assurées entre 100 et 300 millions €** pour l'Espagne, et un montant légèrement plus faible au Portugal. |
| Commerce de détail / magasins | Fermetures temporaires, terminaux de paiement inopérants, clients incapables de payer par carte, pertes de ventes immédiates. |
| Chaîne d'approvisionnement / supply chain | Rupture d'activités, retard dans les livraisons, perturbation des flux logistiques à cause de production à l'arrêt. |

Sources : Reuters, ReinsuranceNews, slimstock.com

FAILED FAILED FAILED FAILED FAILED

## Citizens, Grand Public

**The blackout disrupted the daily lives of millions.**

In major cities, metro and train services came to a halt, flights were delayed, and roads quickly became congested as traffic lights went dark.

Hundreds of people were trapped in elevators, requiring large-scale interventions by firefighters, while entire neighborhoods were left in darkness, heightening the sense of insecurity.

Essential services collapsed: payment terminals, ATMs, and e-commerce platforms went offline, forcing shops and restaurants to close.

The most vulnerable groups—elderly citizens, chronically ill patients, and people with disabilities—were hit hardest by the interruption of telecare services and the postponement of medical treatments. Local associations played a crucial role in providing food, shelter, and reassurance during the crisis.

Tourists, meanwhile, were caught completely off guard: stranded in train stations or airports, sometimes in hotels without electricity, and unable to pay or book services due to inoperative systems. Their direct experience of this fragility amplified perceptions of disorganization and dealt a blow to the image of Iberian and Mediterranean destinations.

REE **waited four hours to communicate** with this panicking population, issuing messages that were deemed too technical and incomprehensible. In other words, the communication was completely inadequate, which had several repercussions:

- **Public mistrust:** The lack of clear information fuelled mistrust of the authorities and network operators.
- **Spread of rumours:** The lack of accessible communication encouraged the spread of unverified theories about the causes of the outage.
- **Political pressure:** Criticism led to calls for better coordination and transparency in the management of energy crises.

FAILED

## Prioritization by Technical Level

In its poor public communication, REE failed to differentiate between technical communication, intended for energy stakeholders, and simplified communication, intended for non-technical audiences (governments, businesses, hospitals, banks, citizens, etc.).

A total lack of popularisation, which could only lead to widespread confusion and the spread of false information and even rumours.

### A glimpse of messages sent by REE 👇

> Sudden loss of 15 gigawatts of electricity production in a matter of seconds.

> Disconnection of the interconnection with France to prevent the outage from spreading.

> Frequency oscillations and imbalances in the electricity grid

FAILED FAILED FAILED FAILED FAILED

## 3 - Non-Compliance with Blackout Regulation

European directives require grid operators to maintain crisis protocols, including communication strategies:

- **Directive (EU) 2019/944 requires** EU states to ensure TSOs and DSOs have **emergency communication measures in place**.
- **Directive (EU) 2024/1711 mandates** detailed **crisis plans and clear communication protocols** for all major disruptions.

It's no surprise that the Spanish and Portuguese governments have publicly turned to REE for explanations, and that the EU is showing interest in the event.

## 4 - Public Confusion and Mistrust

An unbelievable chaotic, confusing, and sometimes contradictory flow of messages with with confused or invisible spokespersons gave an impression of amateurism and internal discord.

- Public finger-pointing between operators. No responsibility taken.
- Spokespeople either absent or underprepared.
- Overly technical communication.
- Inconsistent messaging: "rare atmospheric phenomenon", "unknown causes", "not renewables-related", "no cyberattack".
- No public thank-you from REE to other countries (e.g., France, which provided 2,000 MW to support the grid).

# Most Likely Consequences for the Operators

## Short, Middle & Long-term

RED ELÉCTRICA DE ESPAÑA

The operator most exposed to to criticism from all sides

### 🔥 Short term

- **Loss of technical credibility** with the Spanish government and the EU
- **Spanish and European parliamentary inquiry** into crisis management
- **Media pressure:** ‘REE knew but did not speak out’ / ‘shameful silence’
- Temporary **blockage of strategic files or funding**
- **Social and economic disruption** with mass withdrawals of funds from banks, disruption of the supply chain, increase in customer complaints, etc.
- **Crisis of confidence** in technical institutions among the population
- **Risks for exporting companies:** perception of vulnerability in foreign markets
- **Exploitation of rumours and reputation crisis** with conspiracy theories, false expert reports, designated scapegoats, fakes, etc. on social media, propagandists, foreign media, etc.

### Internally

🔥 Post-crisis emergency management: intense mobilisation of technical, communications, legal, compliance and public relations teams; fatigue, high stress, cognitive overload; silo effects between teams: IT vs communications, management vs field staff.

⚠️ Internal communication under pressure: informal rumours about responsibilities, errors or negligence, misalignment between external/public discourse and internal perception, confusion about the crisis exit strategy.

💬 Tense social relations: mistrust between unions and management, feelings of shame about being an employee of REE, expectation of clarification on recognition or compensation for exposed teams, etc.

## ⏳ Medium term

- **Political and institutional pressure** from the Spanish, Portuguese and French governments with demands for accountability, administrative investigations and a decline in bilateral trust.
- **Strengthening of external audits** imposed by Brussels (ACER, ENTSO-E)
- **Possible internal reshuffle** or resignation of the CEO to 'reset' trust
- **Initiation of administrative and legal proceedings** by states and complaints filed by affected economic actors (airlines, hospitals, distributors, telecom operators)
- **Risk of fines** from the CNMC or the European Commission, which could result in heavy financial penalties
- **Loss of confidence** among users and institutional customers, with energy-intensive companies reconsidering their relationships or demanding guarantees
- **Increase in demands for compensation** or transparency from consumer groups
- **Weakening of international image** with a review of its role as an interconnected operator in the European network and a decline in REE's credibility in international forums (ENTSO-E, OECD, GIE).

### Internally

👥 Human resources & management: turnover of technical or strategic talent who are tired or demoralised, loss of high-potential talent, fear of reorganisations or internal sanctions, difficulties in recruiting for certain key positions (loss of attractiveness).

🧠 Internal reputation and commitment: erosion of confidence in leadership if no clear vision is provided, resistance to change, especially if monitoring or reporting measures are strengthened without support, erosion of the sense of belonging if pride in belonging to REE is not restored.

📈 Organisation: pressure from internal and external audits (EU, CNMC, Parliamentary Commission), acceleration or improvisation of reforms (protocols, supervision, tools) that are not always well accepted, proliferation of meetings, committees, reports... leading to information overload.

RED
ELÉCTRICA
DE ESPAÑA

## 🧊 Long Term

- **Strategic review by governments** with the inclusion of enhanced resilience clauses in network operator obligations and possible legislative reforms on public crisis communication.
- **Enhanced EU oversight of REE governance and investments** with a direct supervisory agency (scenario type: ‘post-COVID response to national inaction’).
- **Lasting damage to the company's image** among the Spanish population.
- **Difficulties in achieving technical leadership** in Europe on smart grid projects.
- **Risk of competitive repositioning** with less room for manoeuvre and private players potentially using the failure as a marketing lever.
- **Risk of losing strategic opportunities** on interconnected projects (e.g. Morocco–France cables, Africa–EU projects).
- **Significant indirect financial impact** with downgrading by investors or rating agencies, reluctance to finance new projects without proof of profound transformation, and increased compliance, cybersecurity and communication costs (tight budgets)
- **Rise of territories or regions demanding energy autonomy** (decentralisation).

### Internally

🛠️ Organisational transformation with the implementation of new crisis management procedures, sometimes rigid or bureaucratic, the creation of new steering entities (resilience, cybersecurity, critical communication) and governance reform (more control, independence, even political pressure).

💼 Strategic positioning with a temporary loss of credibility in international negotiations (interconnections, investments) and increased EU surveillance or pressure to integrate more restrictive common measures.

🧬 Internal culture & resilience with two possible scenarios: ❌ **Defensive culture**: mistrust, withdrawal, slowness, risk of future inaction or ✅ **Learning culture**: transparency, training, commitment, strengthened public service spirit.

## REN

A supportive but discreet player with virtually invisible communication.

### 🔥 Short term

- Less targeted than REE, but caught up in the same logic of shared responsibility.
- Portuguese government concerned about interconnected dependence.
- Image of a weak follower: 'REN said nothing, did nothing'.
- Mobilisation of civil society on energy sovereignty
- Internal crisis with fatigue, stress, demotivation

### ⏳ Medium term

- Political pressure to create a national crisis communication capacity
- Call for a strengthening of the role of the Portuguese energy authority (ERSE)
- Increased mistrust of technical cooperation with REE

## IBERDROLA

A private company with big influence, but silent at the wrong moment.

### 🔥 Short term

- Image of supplier absent, while customers were waiting for answers
- Potential bad buzz on social media: 'What about Iberdrola? Where were they?'
- Growing irritation among certain large B2B customers and local authorities

### ⏳ Medium term

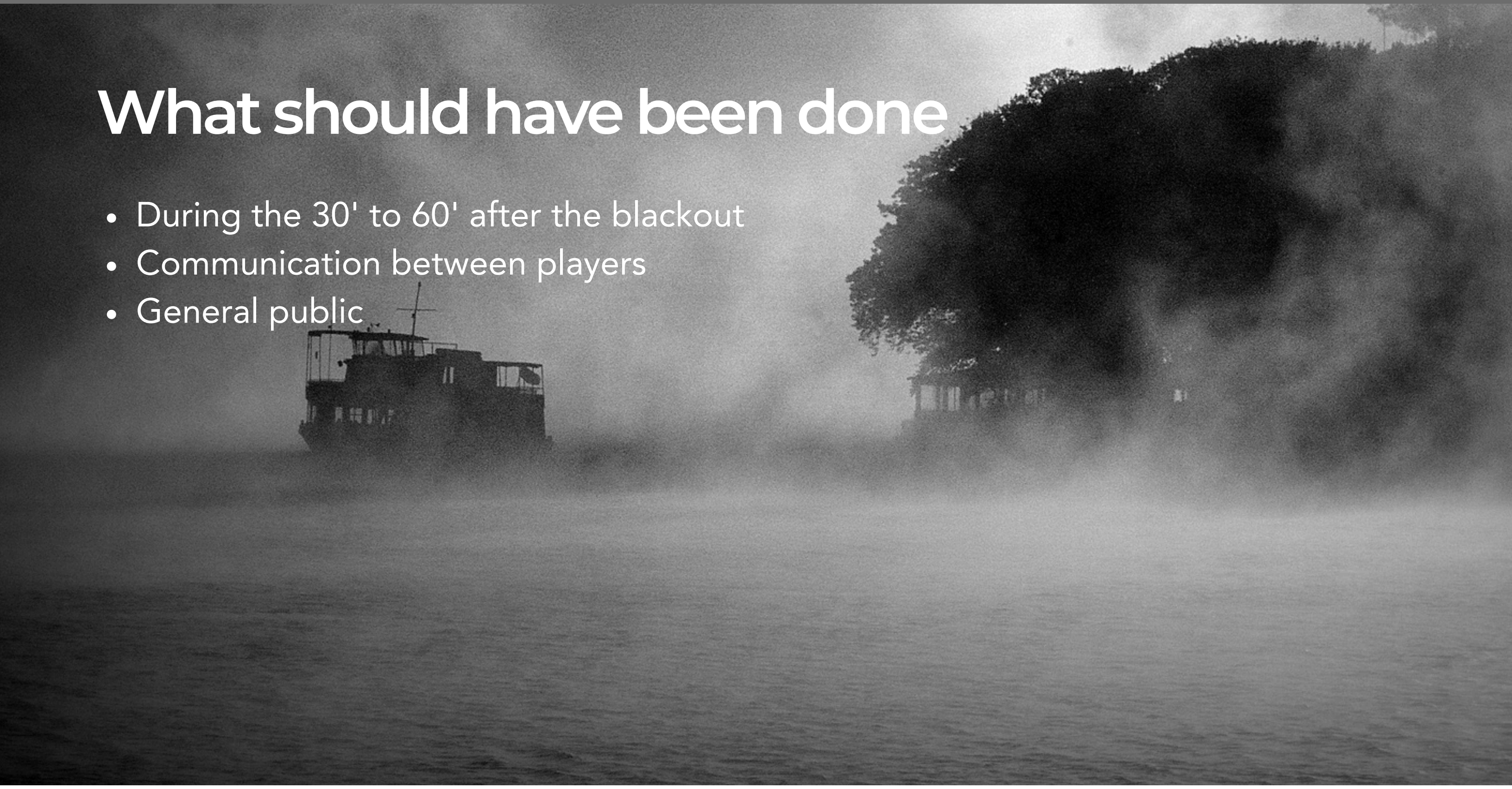
- Institutional clients more hesitant to sign long-term contracts
- Risk of individual or collective complaints for poor information management
- EU pressure on Iberdrola to implement a mandatory cyber resilience communication plan
- Turnover

### 🧊 Long Term

- Sustained reputational strain (such as EDF after Fessenheim or Enedis after the storm)
- Weakening of the 'responsible leader' narrative
- Need to rebuild trust through visible, rapid and sincere commitments

### 🧨 Probable trigger: the EU

- The EUis to launch an investigation into cross-border coordination.
- Risk of fines or partial supervision of crisis management plans.
- The EU could impose a centralised energy crisis communication platform, with a requirement to respond within one hour.



# What should have been done

- During the 30' to 60' after the blackout
- Communication between players
- General public

## Speak up asap

Do not allow others to speak.
Show that things are under control.
Simplify.
Avoid rumours.

## Adjust messages

## Prepare the crisis communication

A dedicated team
Regular simulations
Pre-written messages
Secure and tested communication channels

## 💣In 30' to 60' after the blackout

| Audience | Message | Channel | Objective |
|---|---|---|---|
| Gover-nment | *Blackout confirmed at 15:42 – instantaneous loss of 15 GW on the Iberian grid. Interconnections secure. No sabotage identified at this stage. REE–Moncloa coordination initiated. Technical note to be sent in 10 minutes. Confidential line open.* | Secured official channels<br>Secure landline telephone / Satellite | Inform at the highest level as soon as possible |
| Critical Partners & Service Providers | *Power loss confirmed in your area. You are part of the priority infrastructure. Immediate coordination with your technical contacts will be activated. Confirm your autonomy capabilities (generator, satellite relay). Activate your crisis unit to ensure communication with your various contacts. Next update in 30 minutes.* | Identified secured Channels<br>Satphone / Talkie / Radio | Ensure an immediate coordination |
| General public | *Nationwide outage confirmed. Our technical teams are working to restore service. The network is under control. Listen to public radio or follow local instructions. Avoid using your telephone to prevent network overload.* | AM/FM Radio<br>Vehicules equipped with loud-speakers<br>Paper display (townhall, shops, commercial centers)<br>Mobile App "112"/"Alerts"<br>SMS if batteries are actives still 2-3h | Provide information quickly and reassure people.<br>Issue a simplified alert message.<br>Fill the silence, avoid rumours, show that you are in control. |
| Companies | *Major power failure confirmed. Industrial zones X, Y, Z currently without power. Load reduction implemented to prevent spread. Estimated duration of interruption: 60 to 90 minutes. Please activate your continuity plans. A sector-specific technical data sheet is being sent via your federation.* | Direct calls for corporations.<br>Encrypted SMS messages to federations, associations, unions (as long as the network is maintained) | Anticipate needs and minimise impact |

This **requires having an up-to-date database of priority contacts** in the event of a blackout, as well as having **secure communication channels in place beforehand, tested** with the various audiences.

**apply this plan to each phase of the crisis until control is regained.**

## Coordinate communication between the players

SIX essential steps:

1. Activate a coordination protocole between the operators
2. Co-create a common language
3. Send common messages at the same time
4. Set up a “common information hub”
5. Share common media kits, to spread in the local language
6. Activate a joint monitoring team

**Objective**:
NO dissonance
NO ping-pong
NO ambiguity

### 1 Coordination protocole between operators

As soon as the incident is confirmed, REE should have initiated in emergency a coordination committee with:

1. REN (Portugal),
2. RTE (France),
3. ONEE (Morocco),
4. Iberdrola (integrated operator in Spain),
5. Tusass (Greenland via Maspalomas).

Recommended format: secured channel + express channel (e.g. : sat message system, liaison via Signal or dedicated hotline for crisis communication)

### 2 Co-creation of a common language

→ **Harmonisation of key terms** to be used publicly to avoid confusion:

- “breakdown” vs “major incident”
- “load reduction” vs “blackout”
- “active coordination” vs “inter-connection issue”

Objective: avoid REN say "Spanish breakdown", while RTE speaks of "regional instability".

### 3 Coordinated joint Messages

Example of a co-signed REE + REN message:

*« REE and REN confirm that an electrical incident in Iberia is currently being investigated. Our teams are working together to secure the interconnections and ensure a gradual return to normal. No cyberattack has been confirmed at this stage. »*

Objective: show an active, coordinated and responsible cooperation active, before the media and experts would take the lead of the narrative

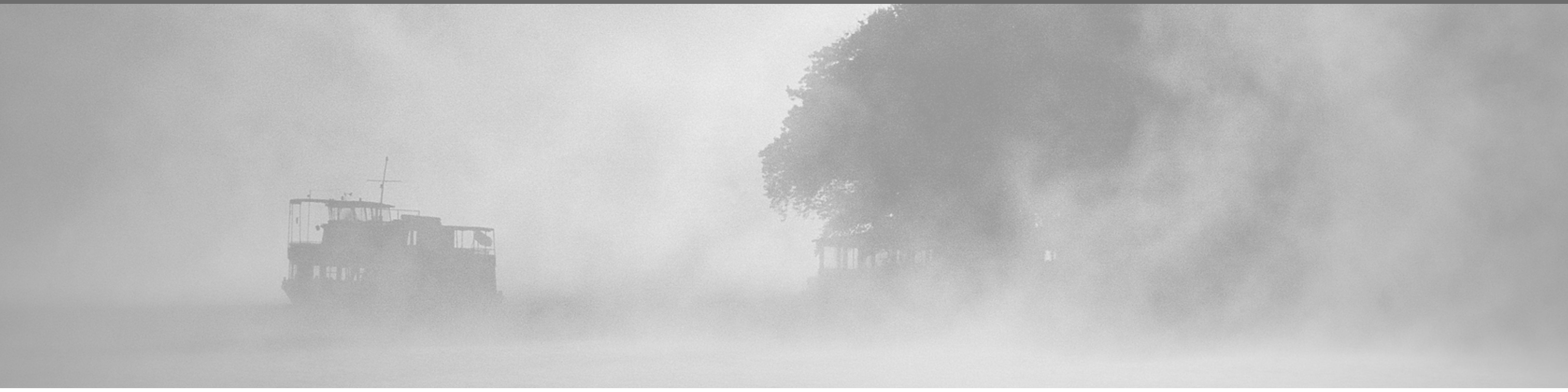
### 4 A common Information Hub

A regional webpage or platform with operators's logos (REE, REN, RTE, ONEE) updated in real time to provide:

- the status of interconnections,
- the areas affected by outages,
- the next steps (estimated time to restoration),
- a citizen FAQ.

Of course, a multilingual page - in the present case (Spanish, Portuguese, French, English, Inuit, Arab).

Objective: centralise the official speech and route the media and institutional traffic.



## 5 Share common Info Kits

The documents that should have been prepared jointly for:

- the media
- governments and local authorities
- critical partners
- employers' federations and associations
- corporations
- the generatl public

Of course, documents in several languages

Objective: to avoid contradictory or simplistic versions in each country concerned.

Typical contents of a kit

- Incident report
- Joint statement
- Joint FAQ
- Interconnection map
- List of dedicated contacts
- Recommendations
- QR code

## 6 A joint Monitoring cell

A transnational, inter-company task force should have been set up, bringing together:

- a smart grid specialist
- an OSINT analyst (press, social media, forums, etc.)
- a Threat Intelligence analyst (monitors the dark web, Telegram groups, hacker forums)
- Foreign langage specialists
- an analysis of the narrative (rumours, sabotage, abuses)
- a trend analyst (correlates noise peaks with current events)
- a strategic coordinator (summary note and recommendations)
- a cyber technical interface (translating alerts into actionable messages)
- and possibly an interface for each critical partner

Its role:

- Monitor public and underground information channels (social media, forums, dark web).
- Qualifying weak signals: shared technical vulnerabilities, accusations of sabotage, emerging narratives.
- Map ongoing reputational or narrative attacks.
- Correlate with technical or geopolitical threats reported by the SOC, CERT or INCIBE – Instituto Nacional de Ciberseguridad (National Cybersecurity Institute of Spain).
- Alert and advise the communications, security, legal and executive committees in real time.
- Working directly with institutions, technical partners, and Moncloa.

## Provide guidance for understanding to the general public

It is not just a matter of providing simplified technical explanations, but also providing a clear, accessible and reassuring framework for:

- Understanding what is happening
- Knowing what to expect
- Acting or waiting intelligently
- In other words: restoring meaning where uncertainty reigns.
- Explain in simple terms what a blackout is (chain of imbalances → power cuts)
- De-dramatise without minimising: 'a rare phenomenon, but under control'
- Give a realistic estimate of when things will return to normal (even if approximate)

Objective: create a 'mental framework' to avoid panic, fake news, over-interpretation and reduce dangerous behaviour.

### Examples of useful reference points to communicate

| | | |
|---|---|---|
| **Timing** | - The incident began at 3:42 p.m.<br>- We estimate a gradual return to normal within the next 90 minutes.<br>- Next update at 7 p.m. | Provides a timeframe, which structures expectations and prevents misinformation from taking over. |
| **Simplified Cause** | - This is not a cyberattack.<br>- A massive loss of load triggered a network protection mechanism.<br>- This phenomenon, although rare, is under control. | Helps to avoid fantasies (sabotage, war, etc.) and shows that it is a known problem. |
| **Location** | - Central and southern Spain are the most affected.<br>- Some areas near Portugal are recovering. | Provides a geographical anchor, allowing people to situate themselves: 'Does this concern me?' |
| **Concrete effects** | - Mobile networks may gradually become unavailable.<br>- Card payments are temporarily unavailable. | Mentally prepare citizens for what is going to happen (and what they should not overinterpret). |
| **What we require of you** | - Do not overload the telephone lines.<br>- Keep your torches ready but avoid using unsecured generators.<br>- Follow the instructions on public radio. | Transforms citizens into responsible actors for collective stability. |

## Structured, multi-level crisis communication plan

REE should have had a clear set of guidelines that could be implemented immediately, including:

- A communication strategy without electricity
- A crisis organisational chart (who decides what, who does what, when, to whom, in which country)
    - Sole official spokesperson for REE, with REN, RTE and ONEE relays.
    - Coordinator of inter-operator messages
    - Internal relays by audience (government, service providers, businesses, general public).
    - Cross-border protocols (alert, response, escalation, etc.) connected to Spanish technical hubs - in this case, REN, Iderdrola, RTE and ONEE - to respond collectively within 15 minutes of the incident.
- Crisis simulations with decision-making interfaces (DirCom, CISO, presidential office, ministries, etc.)
- Ready-to-use fact sheets (who to inform, when, via which channel, with what message, etc.)
- Training to prepare spokespersons
- A validation checklist with the relevant ministries
- A real-time reputation dashboard + dark posts
- A post-crisis learning narrative (what will change)

Objective: To correct the perceived amateurism in the media management of the blackout and bring REE's communication up to the level of its strategic responsibility, ensuring rapid, clear information tailored to different audiences, even in the event of a technological collapse.

multi-level crisis communication

| Audience | Key need | Message / Channel |
|---|---|---|
| **General public** | Be reassured & guided | Simple message via radio + SMS + loud speaker |
| **Government** | Decide quickly + coordinate | Technical bulletin + secure line + briefing |
| **Critical Partners** | Take action + prioritise their resources | Dedicated Hotline + clear message clair on priorities |
| **Companies** | Organise the business continuity | Structured message via federations and associations |
| **Media** | Distribute a consistent and verified version | Press release + common media kit |

# Mesures post-Blackout

Three essential measures must be taken once the situation has stabilised.

- Post-mortem
- Transparent and informative public report on the incident
- Investment plan in 'critical resilience' within 6 months

## Synthetic example of post-mortem

| Analysis Area | Key findings | Recommendations |
|---|---|---|
| **Tech** | Cascading failures, protection vulnerabilities, interconnection limitations. | Strengthen interconnections, modernise protection systems. |
| **Organisation Coordination** | Uneven load shedding protocols, cross-border coordination could be improved. | Harmonise procedures, strengthen cooperation between REE, REN & ENTSO-E. |
| **Human (internal)** | Acute stress among teams, decision fatigue, insufficient psychological preparation. | Integrate the human factor into crisis exercises and ongoing training. |
| **Human (external)** | Feelings of insecurity, loss of confidence, economic disruption. | Develop transparency and establish regular dialogue with civil society. |
| **Global** | Need for greater resilience (technical + human + societal). | Systematically include psychosocial dimensions in post-mortems. |

## Transparent and informative public report on the incident

This report, which is accessible to non-technical readers, should serve three strategic objectives:

- Restore confidence among the general public, institutions and foreign partners.
- Demonstrate technical expertise and a commitment to continuous improvement.
- Cut the ground from under competing narratives, fake news and accusations.

It could be broadcast on a dedicated mini-site and during multilingual press conferences, and, best of all, be backed by an educational campaign on energy stability.

# Transparent and informative public report on the incident

## Report Structure

**Introductory remarks by the Presidency**

- A message of responsibility, delivered in a humble but clear tone.
- Thanks to the teams and partner operators (REN, RTE, ONEE).
- Affirmation of REE's commitment to strengthening national and European resilience.

**What happened — Clear timeline**

- Date and exact time of the incident (e.g. 3:42 p.m.).
- Sudden loss of X GW → desynchronisation → activation of protections.
- Areas affected and duration of outages.
- Minute-by-minute chronology of measures taken.

**What we did — Technical management and coordination**

- Mobilisation of REE teams and coordination with REN, RTE, ONEE.
- Securing interconnections.
- Gradual restoration with prioritisation: health, transport, telecoms.
- Emergency communication: what worked / what was difficult (e.g. blackout + network outage).

**What we have learnt — Feedback**

- Recognition of shortcomings: overly technical communication, initial slowness.
- Points of friction: inter-operator coordination, field feedback, multilingual management.
- Initial technical lessons learned (without assigning blame): imbalance, automation, critical areas.

**What we will do — Concrete commitments**

Implementation of a five-part action plan:

- Multi-level crisis communication without electricity.
- Continuous strategic monitoring unit.
- Coordination protocol with neighbouring countries.
- Annual training and simulation plan.
- Strengthening ties with users and communities.

📌 Include a visible calendar for the next 3, 6 and 12 months.

On 18 June 2025, REE published a three-page press release summarising the technical points of the incident report. Even the 15 recommendations contained in the report sidestep the issue of communication.

Read the press release

**Questions and answers — For all audiences**

Explain in plain language:

- Why did this happen?
- Could it happen again?
- Was it a cyberattack?
- Why did the phones stop working?
- Who is responsible?
- What should we do if it happens again tomorrow?

**Appendixes**

- Technical maps (interconnections, affected areas).
- Glossary of terms (GW, SCADA, desynchronisation, etc.).
- Regulatory references (European NIS Directive, ENTSO-E standards).
- Contact details for press enquiries and citizen feedback.
- Summary in several languages,
- evolving Q&A section.

## Critical Resilience Investment Plan

It is essential for REE to establish a critical resilience investment plan (2025–2026), developed around five strategic areas, with a budget estimate for each area:

- Technical infrastructure & systems
- Cyber & technological posture
- Communication & multi-stakeholder management
- Internal culture of resilience
- European dialogue and cross-border cooperation

Objective: To demonstrate that REE takes systemic threats seriously and to strengthen the operational, human, digital and geopolitical foundations of the Spanish energy system and its interconnections in the face of new hybrid threats.

### Area 1. Technical Infrastructure & Systems

- Audit of structural imbalances in the Iberian network.
- Modernisation of automatic protection and load relays.
- Strengthening of the national grid → reducing 'energy weak spots'.
- Investment in rapid reserve stations (batteries + capacitors) in five critical areas.

### Area 2. Cyber & Technological Posture

- Update all SCADA and critical OT systems with physical and software hardening.
- Recruit 10 OT cyber analysts + 2 permanent red team experts.
- Double the SOC budget + threat intelligence shared with REN, RTE, ONEE.
- Implement a cyber-electric simulator to test hybrid attacks.

### Area 3. Communication & Multi-stakeholder Management

- Creation of a crisis communication coordination centre (digital bunker + low-voltage line).
- Production of communication kits for degraded mode (radio, SMS, display, voice).
- Annual simulations incorporating blackouts, rumours, poor coordination.

### Area 4. Internal Resilience Culture

- Training programme for all managers: "Communication in times of crisis".
- Identification of roles at risk/critical functions in the event of a crisis.
- Establishment of a network of internal cyber ambassadors (one per region).
- Post-crisis coaching for agents who have experienced acute stress.

### Area 5. European dialogue & Cross-border cooperation

- Creation of a joint Iberian electricity crisis management protocol, signed with REN, RTE and ONEE.
- Integration into ENTSO-E task forces on hybrid crises.
- Data sharing and joint exercises with NATO (for critical resilience).

**Implementation – Possible 6-month timeline**

| Month | Leading initiative launched |
|---|---|
| Month 1 | Network audit + government communication |
| Month 2 | Launch of cyber recruitment + communication plan |
| Month 3 | Purchase of initial energy resilience equipment |
| Month 4 | REE–REN–ONEE–RTE Protocol signature |
| Month 5 | Pilot deployment of continuous monitoring unit |
| Month 6 | Publication of the first progress report |

# What Companies can do

## in the event of a blackout

Imagine you have an urgent delivery to send. You are in the middle of a webinar or a highly urgent video conference. And suddenly...

### Some basic tips

**Business Continuity**

- Implement business continuity plans (BCPs) and crisis scenarios that include power loss.
- Provide for energy redundancy solutions: generators, inverters, backup batteries.
- Identify critical processes (IT, production, security) that must be maintained as a priority.

**Technical Preparation**

- Regularly check the condition and autonomy of backup systems.
- Install controlled disconnection systems to prevent damage to sensitive equipment.
- Secure IT and communication systems using backup solutions (cloud, redundant data centres).

**Internal Organisation**

- Train and raise awareness among employees about the procedures to follow during a blackout.
- Set up an internal crisis unit with clearly defined roles (communication, technical, customer relations).
- Conduct simulation exercises (blackout drills).

**Communication**

- Maintain alternative communication channels (radios, offline messaging, satellite lines).
- Prepare standard messages to quickly inform customers, partners and authorities.
- Monitor official instructions from network operators and local authorities.

### Example of REE recommendations

In its post-incident analysis report, REE makes 15 recommendations to prevent such a blackout from happening again, including:

- Implement a dynamic voltage control service applicable to the entire production fleet. Red Eléctrica
- Improve coordination between production entities and the network operator so that power stations comply with regulatory voltage control requirements.
- Review the calculations for scheduling technical constraints, taking into account increased variability in renewable sources.
- Strengthen black start mechanisms (the ability to restart the grid from a disconnected state) so that restoration does not depend excessively on external sources.

## The Treat is evolving.

## So is your communication

Oz'n'gO, a community of experts
in various fields
at your service

✉ contact@ozngo.com

▦ Planifier un call

🌐 www.ozngo.com

**Act Right**
**Last Strong**