Fonds européen de développement régional (FEDER)
Europäischer Fonds für regionale Entwicklung (EFRE)

Report 7.3.1: Recommendations on trinational protection against cyberattacks to enhance energy security

Bushra Canaan, Djaffar Ould Abdeslam

Université de Haute-Alsace (UHA), Institut de Recherche en Informatique, Mathématiques, Automatique et Signal (IRIMAS)

Introduction

Climate change and energy do not respect national boundaries. Public policies, on the other hand, are executed within national frameworks that vary from country to country. Cross-border regions, which serve as testing grounds for European integration, are the places where these disparities collide. Moreover, as participants in the energy transition, they may achieve a maximum benefit of the offered development opportunities.

The European Green Deal and the 2030 energy and climate policy framework has emphasized on the important weight that cross-border cooperation of renewable energy takes, in which two or more neighbouring countries create a cooperative RES project or support mechanism. Regional cooperation was clearly indicated in the recast of the Renewable Energy Directive (Directive (EU) 2018/2001) and the Energy Union Governance Regulation (Regulation (EU) 2018/1999) as a relevance tool for attaining EU climate and energy targets in a cost-effective manner.

With multiple research projects showing that taking a cooperative approach to meeting national and EU renewable energy targets can reduce overall costs and maximize benefits for European citizens, the economic rationale for cross-border collaboration is compelling and goes even beyond the economic rewards to include creating long-term relationships to driving innovation.

The development of cross-border processes also boosts market confidence and provides investors with safer trading conditions, since any needed changes to be reviewed, adjusted and approved by the partnering countries. These initiatives offer learning and testing opportunities for the involved countries, in addition to opening the door in front of many sorts of energy cooperation, including science, technical innovation, energy policy, and more.

Therefore, Cross-border collaborations have the potential to benefit the EU as a whole, as well as the direct benefits for member countries. It could help to create a more dynamic, efficient, and integrated internal energy market by building equal competitive conditions field between Member States and encouraging the harmonization of national legislative and policy approaches. At the same time, it might help the Energy Union fulfilling its goals more effectively while also improving the energy system's security and resilience.

Designing and implementing cross-border cooperation projects depends deeply on the existence of a strong political will to reach an agreement. Which is often encountered by complex processing of technological, political, and legal complications of such an arrangement. For this reason, adequate time and resources need to be allocated to negotiations to allow the participation of various stakeholders and to ensure that the participating countries' specific legal, economic, and political circumstances are identified and taken into account.

The efficacy of the cooperation mechanism is a key factor in gaining political support for the selected cases. As agreements can only be established when tangible advantages outweigh the costs and risks which in turn highlights the significance of recognizing and quantifying them as much as possible.

However, individual Countries should always keep in mind that maintaining a flexible attitude toward cross-border collaboration might help them achieve their goals at a lower cost than acting alone. taking into consideration that national circumstances in terms of taxes, spatial planning restrictions have a radical impact on both expenses and outputs. Especially when some of the advantages may be difficult to quantify or manifest at different periods. Whereas it is an indispensable condition that costs and benefits should be evenly distributed among participating countries, understanding the fact that collaborating counterparts never possess identical conditions would facilitate the process of establishing agreements that put up with the extremely challenging equal distribution item.

This message, nevertheless, may be difficult to convey to individuals, particularly if citizens believe costs and benefits are not appropriately linked. Public approval and political support may suffer because of such actions.

This report evokes research questions on potential cross border collaboration on energy security in terms of regional resilience and data management policies. It provides guidance to policymakers, electric utilities, and other stakeholders on how policies and actions might improve the cyber resilience of electrical networks.

It tackles the issue from a multidisciplinary approach: first by preparing a detailed review of the latest European legislation on security of energy data including recent regulations and incentives that address ways to improve cybersecurity capabilities at the national level all along with encouraging the EU-level of cooperation. It also sets the rules for risk management and incident reporting obligations for operators of essential services and digital service providers.

The next pillar of the present work has taken a technical turn by means of attempting to develop predictive models of data security vulnerabilities. An in-depth examination of the existing approaches attending to cyber-physical security in power systems from a microgrid-oriented perspective has been carried out in addition to a comprehensive presentation of the recent efforts explored. We then propose a new artificial intelligence (AI)-based method for the detection of cyber-attacks jeopardizing connected microgrids as examples of vulnerable CPS. Driven by the apprehension of triggering cascading failure events generated by a violated entity that communicates with the grid on both the physical and cyber levels, especially with the ambiguity surrounding governing norms that define microgrids functionality, ownership and operation access control.

Upon the previous explanation, recommendations were conceived on three key aspects

Recommendations for policymakers

Energy sector actions for Europe’s short-term recovery should be boosted using large-scale programmes for renovation that lifts barriers standing against the full investment in energy projects promoting the clean energy industries and infrastructure of the future.

The implementation of the 2030 framework of the National energy and climate plans must be maintained a cost-effective approach while policies are reviewed to scale up energy action towards climate neutrality all along with ensuring competitiveness, security of supply, sustainability and affordability.

This needs to be accompanied by a full operationalisation of the energy efficiency principles side by side with strengthening standards across end-users. While fostering the cross-sectors policy integration, including for energy efficiency, renewables, the internal energy market, and carbon pricing by reducing regulatory and pricing barriers and enabling digitalisation and electrification.

The European Commission is laying out a plan to create a new Joint Cyber Unit to combat the escalating number of significant cyber events affecting public services, enterprises, and citizens throughout the EU. As cyberattacks rise in quantity, scale, and consequences, advanced and coordinated responses in the field of cybersecurity have become increasingly required, posing a serious threat to our security. All relevant EU actors must be ready to respond collectively and disclose pertinent information based on a 'need to share' rather than a 'need to know' premise.

Governments, utilities, and other stakeholders in the power value chain must be proactive in their search for solutions that can adapt to changing cyberthreats. It will be vital to maintain a long-term commitment to cooperation and partnership.

Smart application functionalities are not clearly framed in official norms that usually define and impose quantifying criteria in terms of technical specifications. This is why working and elaborating on the standardization enclosure, especially for the most affiliated pieces of the smart grid, becomes an urgent need.

Coordination between Member States is vital in order for Member States to be compliant with the NIS Directive. This requires not only cooperation nationally between the single point of contact of each Member State and the CSIRTs but also among Member States' governments and enforcement agencies.

The cooperation is expected on many levels: firstly, between the CSIRTs, which will create a CSIRTs network to effectively exchange information and support one another, but also between national competent authorities that need to assess the compliance of operations of essential services.

Lastly, the legal instrument utilised by the European Union legislators - a Directive, means that even though it is a legally binding act, it requires each Member State to implement the set of objectives and further specifications in its national legislation. Unavoidably, this represents a further level of difficulty in the harmonisation of a high common level of security of network and information systems across the European Union.

There is a need for a more coordinated approach to crisis response so that Member States promptly share relevant critical information with each other and also alignment and consistency of messages to the public takes place resulting in containment of the damaging impacts of cyber-attacks.

In conclusion, there is no simple response to such questions: the NIS Directive is viewed as a baseline for critical infrastructure cyber security, with a focus on measures such as the establishment of CSIRTs inside Member States and coordination through a CSIRT network. Any additional law or legislation should clearly build on and complement the frameworks created by the NIS Directive and GDPR to the greatest extent practicable.

Cross boarder collaborations

A comprehensive risk analysis and risk treatment plan tailored to the highly interdependent European energy sector must be established, enriched and completed by the creation of two parallel frameworks. the first one aims at setting up acceptable and efficient governance, with regional cooperation on cyber security topics as a key component. Whereas the other one enables the controlling and securitizing disclosure of vulnerabilities and incidents.

Another strategic objective is to obtain an effective cyber response architecture that will allow for a quick and coordinated reaction in the event of a cyber security emergency. That is why working on defining and implementing a cyber response and coordination structure specifically targeted at the energy sector which could take into account the essential role of energy in a digital society, would be one of the recommended strategic priorities. Simultaneously with strengthening the regional cooperation in the event of a cyber emergency involving or affecting energy systems.

At the same time, improving the energy sector's organisational readiness and protection by addressing the need to improve cyber resilience necessitate a consensus agreement. Creating a European cyber security maturity framework tailored to the energy industry is a proposition that holds great potential in guaranteeing the supply chain integrity and allows public institutions and the energy industry to discuss feasible solutions to the unsolved problem of ensuring supply chain integrity in a complex and ever-changing environment.

Overall, the greatest approach to engaging EU actors in cyber security for energy while also strengthening international relationships is to develop internal coordination and explore international collaboration through mutual experience sharing across borders.

Technical recommendations

In comparison with the partly robust power primitive system, the research into security enhancement of the electrical power data system is in its infancy, with many unidentified security vulnerabilities.

The complexity level of the actual power networks and the critical role that it plays in every domain form a double-edged challenge, especially when the introduced technologies might itself be the source of threat.

Electricity systems work in real-time, with availability and reliability taking precedence. Electricity industrial control systems must react in fractions of a second, necessitating the use of cybersecurity processes such as authentication to ensure that the underlying industrial control system functions run smoothly. Because of the real-time nature of electricity, basic cybersecurity operations such as patching and rebooting are more complicated than those done on less critical situations, which are easy to pull out of service for a short period of time.

Similarly susceptible to cascading effects, electrical systems can be subjected to assault spreading across their both digital and physical systems. An outage induced in a particular part of the system could cause problems elsewhere and a single event, as with other energy security issues, can cascade across the whole electricity network, resulting in widespread disruptions.

The design and deployment of CPS and IoT are at a crossroads. A wide range of new devices has been enabled through advancements in networking, processing, sensing, and control systems. These technologies are being created and deployed right now, but security is frequently put off until later. Functional requirements and fast-moving markets drive industry and design trends change quickly, and standards are only now beginning to emerge. Because many technologies already in use have lifespans measured in decades, current design choices will have an impact on the transportation, health care, building controls, emergency response, energy, and other sectors over the next several decades.

New types of communication and data-management systems must handle not just the different emerging media trends and smart equipment (e.g., computer-based or microprocessor-based), it also needs to cope with existing legacy systems in a manner that is adjustable to scalability and above all, resistant to cyber intrusion. To this end, smart grids have to come as a complementary solution and not an eliminating or excluding one. These technical uncertainties, plus the additional investment costs, have evoked the political reluctance practiced by energy operators against this shift.

Europe has been working on energy transition and smart grids since 2005, starting by creating the smart grid technology platform. There were also several initiatives that carried out the development of experimental testbeds for smart grids solutions which aimed to highlight the most critical challenges and potentials accompanied by this evolution and their influence on the European power systems. Nevertheless, a further and more holistic analysis that is based on a profound technical understanding of each individual system architecture and basically includes the impact of both social and economic aspects on such heterogeneous systems, is yet to be accomplished in order to be able to trade-off between the existing approaches and pilot experiences, choosing a unique and valid experience that is suitable to be scaled up and replicated.

On the other hand, a very promising approach to overcome the majority of previous issues appears through energy communities, in which current grid problems are managed in a coordinated way such that avoiding costly network reinforcement along with maintaining aspired values of the smart grid. That is why we might be able to envisage the future smart grid as a sort of aggregation of multiple integrated entities or microgrids supervised, monitored, and controlled via a reliable communication-based layer. Accordingly, the increasing interest in microgrid development as the core of the smart grid systems is completely justified, although this increasing interdependency between physical and nonphysical power system components, which forms the so-called cyber-physical systems, raises a whole new level of complications.

The work on the smart grid application, in general, lacks approach intersections, and is still being dealt with from separate domains in the research world. Although using the microgrid model to carry out experiments on the cyber-physical security has plenty of practical justifications attributed to the important role it plays in paving the way towards smart grids, regional resiliency and facilitating the introduction of small medium scale renewable generation units, the microgrid's context was mainly consulted owing to the relative simplicity in capturing and recording interventions, either as an injected attack or control modification. For example, the islanded microgrids broached by a fair number of papers, especially the DC type, have unarguable merits in terms of autonomy. However, this will only leave us with specially tailored methods and solutions that do not necessarily fit all cases. This reflects the high level of complexity needed to carry out experiments and designing testbed that corresponds to the actual topology of the smart grid. Not to mention the unwillingness of grid operators to publicly sharing any sort of data that might has the potentials of tampering the integrity of their systems.

On a larger spectrum, cybersecurity measures for energy systems still come as accessories and not as a built-in function. In particular, for most of part, the electricity-related equipment that gets evolved at an exponential rate makes it extremely difficult for cyber defences' mechanisms to keep pace with this development in the absence of up-to-date standards and common market trends. At least, securing the smart grid requires a multidisciplinary approach, and economic and social development are usually forgotten or neglected aspects in this process. Even the most remarkable technology inventions are useless without being approved by clients.

Then again, embedding a culture of cyber hygiene and implementing risk management strategies for a cyber-resilient application of the intensified digital modern life is extremely critical across all sectors, the energy system included, with a growing need for sector-specific characterization methods.

Finally, human competencies that acquire relevant knowledge to address cyber security in the energy sector and promote research within the energy industry have to be a strategic priority to be worked on in Europe.