CEER

Council of European Energy Regulators

Fostering energy markets, empowering **consumers**.

Cyber Security Work Stream

CEER Cybersecurity Report on Europe’s Electricity and Gas Sectors

Ref: C18-CS-44-04

26-October-2018

Council of European Energy Regulators asbl
Cours Saint-Michel 30a, Box F – 1040 Brussels, Belgium
Arrondissement judiciaire de Bruxelles – RPM 0861.035.445

INFORMATION PAGE

Abstract

This public report (C18-CS-44-04) gives some recommendations that contribute to filling in the gaps between the current situation and the optimal situation of cybersecurity in the energy sector when performed by NRAs. It also describes key regulatory aspects for energy NRAs and looks at Cloud computing and Big Data.

Target Audience

European Commission, energy suppliers, traders, gas/electricity customers, gas/electricity industry, consumer representative groups, network operators, Member States, academics and other interested parties.

Keywords

Security of supply; Consumer rights; Quality of service; Reliability; 3rd Package; National Regulatory Authorities (NRAs); smart meters & smart grids; cybersecurity; Big Data; Cloud computing; NIS Directive; GDPR; Clean Energy for All Europeans Package; Operator of Essential Services

If you have any queries relating to this paper, please contact:
the CEER Secretariat
Tel. +32 (0)2 788 73 30
Email: brussels@ceer.eu

Table of Contents

Related Documents

External documents

- Charter of fundamental rights of the European Union, Ref. 2000/C 364/01. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2000:364:TOC
- Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:211:0055:0093:EN:PDF
- Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in gas and repealing Directive 2003/54/EC. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:211:0094:0136:EN:PDF
- Commission recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems 2012/148/EU. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012H0148
- Big Data — challenges and opportunities for the energy industry. SUNGARD, 2013. https://www.scribd.com/document/350455240/Big-Data-Challenges-Opportunities-Energy-Industry-pdf
- Information Technology – Big Data, Preliminary Report, ISO/IEC JTC 1, 2014. https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/big_data_report-jtc1.pdf
- Data Protection Impact Assessment template for Smart Grid and Smart Metering systems, EC SGTF EG2, March 2014https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf
- Data Protection Impact Assessment template for Smart Grid and Smart Metering systems, EC SGTF EG2, V. 2 - September 2018 https://ec.europa.eu/energy/sites/ener/files/documents/dpia_for_publication_2018.pdf
- Commission Recommendation of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014H0724
- Privacy by design in Big Data, an overview of privacy enhancing technologies in the era of Big Data analytics, ENISA, December 2015. https://www.enisa.europa.eu/publications/big-data-protection
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
- The power sector goes digital - Next generation data management for energy consumers. A EURELECTRIC report, EURELECTRIC, May 2016. http://www.eurelectric.org/media/278067/joint_retail_dso_data_report_final_11may_as-2016-030-0258-01-e.pdf
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information

systems across the Union. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148

- Best Available Techniques Reference document for the cyber-security and privacy of the 10 minimum functional requirements of the Smart Metering Systems, EC SGTF EG2, November 2016. https://ec.europa.eu/energy/sites/ener/files/documents/bat_wp4_bref_smart-metering_systems_final_deliverable.pdf
- Smart grid projects outlook 2017: facts, figures and trends in Europe, EUR 28614 EN, Gangale F., Vasiljevska J., Covrig F., Mengolini A., Fulli G. http://publications.jrc.ec.europa.eu/repository/bitstream/JRC106796/sgp_outlook_2017-online.pdf
- Cyber Security in the Energy Sector: Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector, EECSP, February 2017. https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf
- Proposal for a Regulation of the European Parliament and of the Council on the internal market for electricity, February 2017, COM(2016) 861 final/2. http://eur-lex.europa.eu/resource.html?uri=cellar:9b9d9035-fa9e-11e6-8a35-01aa75ed71a1.0012.02/DOC_1&format=PDF
- Proposal for a Directive of the European Parliament and of the Council on common rules for the internal market in electricity, February 2017, COM(2016) 864 final/2. http://eur-lex.europa.eu/resource.html?uri=cellar:c7e47f46-faa4-11e6-8a35-01aa75ed71a1.0014.02/DOC_1&format=PDF
- Big Data, artificial intelligence, machine learning and data protection, ICO (UK), April 2017. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

Disclaimer

This document was originally created in the summer and early autumn of 2018. The content was updated to the extent possible in October 2018. Every effort has been made to have the document as up-to-date as possible for the date of publication. However, there may be some developments in October 2018 not captured in this report.

EXECUTIVE SUMMARY

Cybersecurity is now considered among the highest priorities for the European Union. This report gives an overview of the state of cybersecurity in the energy sector. EU Member States (MS) are acting to meet the deadlines imposed by the existing legislation, especially now in regard to the Directive on Security of Network and Information Systems (NISD). Nevertheless, there seems to be potential room for improvement when it comes to planning for the medium and long term.

This report also treats important developments in cybersecurity: the need for trust, the use of Cloud computing, Big Data analytics and the European legislative environment.

Trust is a core aspect of any successful security strategy. Actors in energy markets work hard to build their reputations and to make sure that, from a cybersecurity perspective, they can be considered trustworthy parties. Their credibility is clearly a core value in order to operate and inter-operate in such a complex sector. Regulators appropriately promote competition, but should also encourage trust among operators in order to safeguard the public interest in the cyber space occupied by the energy sector

This report also introduces two interesting case studies: Cloud computing and Big Data analytics. The extensive coverage of these two topics has the aim to support the thesis that, while embracing a new technology, the energy market should be conscious of the cybersecurity risks which may be introduced together with the new technology. In this context, a culture promoting informed and conscious digitalisation of the sector may contribute to the avoidance of risks.

Several cybersecurity vulnerabilities have become visible during recent years, and several of those were relevant for the energy sector, with a few even specifically targeting this sector. Although economic motives for the cyberattacks seemed to be evident, other motives were also suspected. The European Union makes use of measures like legislation, strategies and funded research to reduce cyber risks.

The General Data Protection Regulation (GDPR) is one such piece of legislation which protects privacy by improving the individual’s rights and enhancing the accountability of data controllers. The GDPR applies to all organisations which process personal data electronically. This includes the majority of energy companies, including operators, suppliers, contractors, and third-party supply chain organisations. Several guidelines and documents for implementation strategies exist. But in addition, data from industrial or commercial customers should be protected for a well-functioning energy market.

The NISD concerns the security of network and information systems. Member States are required to identify Operators of Essential Services (OES), including in the energy sector, on their territory by 9 November 2018 at the latest. Good progress on OES being identified has been achieved in the majority of the EU Member States. The NISD gives OES obligations to address cybersecurity appropriately, using defined standards.

The proposed Clean Energy for All Europeans Package lays down specific provisions on cybersecurity for the electricity sector. The European Commission in its proposal wanted to also ensure that those aspects related to cybersecurity which did not find space in other legislation or that were not specifically designed taking cybersecurity into account are optimised for requirements regarding cybersecurity, via such things as risk preparedness plans, minimum security requirements for Smart Metering Infrastructure, and the possibility of adding other necessary rules. The proposal, at this stage in time, does not include any specific task for national Regulatory Authorities in regard to cybersecurity, although via the Agency for the Cooperation of Energy Regulators (ACER) NRAs would be involved.

In conclusion, there is still much work on cybersecurity in the energy sector to be done. This report states several recommendations (found in full in Table 1 after the conclusion), including increasing the crucial involvement of European Energy Regulators, collaboration between involved parties and giving guidance and clarification. In addition, the issue of how to proceed with cybersecurity in the gas sector is raised.

Introduction

It is an understatement that cybersecurity in the energy sector is crucial for economic and social safety in Europe. Examples of cyberattacks on the energy sector and companies in the recent past have demonstrated that these attacks can lead to economic damage.

Many parties are active in achieving an acceptable cybersecurity posture; to this effort are contributing energy companies, suppliers of energy systems, information and communication technologies (ICT) companies, ICT auditors, legislators and authorities. They all contribute with appropriate efforts in the field. However, they cannot function and act in isolation. The legislation, cybersecurity culture and awareness, the threat landscape, ICT and operational technology (OT) solutions, and the powers of regulators are all constantly changing, and they are inherently interlinked and interdependent.

This report describes the view of the cybersecurity landscape of the National Regulatory Authorities (NRAs) organised in CEER. The task of CEER NRAs is to regulate the electricity sector and (where it exists) the gas sector. The members of CEER are in a unique position to follow legislative developments, to monitor implementation in the energy sector, and to compare the different approaches throughout the European Union (EU), and beyond.

This report describes the initial effect of the current European legislation and related developments. It also addresses the cybersecurity effects of new automation developments towards the energy sector and recommends actions which can improve the state of cybersecurity in the energy sector in Europe.

Finally, the report outlines recommendations of a group of experts from CEER concerning those regulatory and organisational aspects, which may help in improving the effectiveness of the work done until now by all the involved authorities.

1 Regulatory aspects

1.1 Extension of Directive on Security of Network and Information Systems obligations

The NISD concerns the security of network and information systems. Member States are requested to identify OES, including in the energy sector, on their territory by 9 November 2018 at the latest. Companies defined as OES have been identified by the majority of the EU Member States (MS). The NISD gives OES obligations to address cybersecurity appropriately, using defined national standards.

The **definition of essential services** is one of the topics under intensive discussion. One approach is to define essential services in the energy sector depending on the number of customers who are supplied with energy by the operator. In Germany, for example, 500,000 customers is the figure already included as the threshold for the selection of OES in national legislation. If we focus on the energy markets, another issue is that the operators have very different characteristic: operators of electricity generators is one type; grid operators (TSOs or DSOs) is another.

A figure of between 20 and 60 OESs is expected in the energy sector within a single member state.

The NISD gives operators of essential services obligations regarding appropriate cybersecurity. They must operate their network and information utilities in compliance with defined **minimum cybersecurity standards** to be fixed within the national cybersecurity law. In some member states (e.g. Germany), these standards will be based on existing standards such as ISO/EIC 27001 and ISO/EIC 27019[1]. An excessively burdensome administrative approach should be avoided. In other member states, it has not yet been decided how to reach this goal. In any case, it is essential that the scope for the standards is appropriate to the needs and to the real capabilities of the operators.

The exponential growth of new technological resources in the energy sector makes it more and more sensitive to new unpredictable cyber-related risks which may severely affect operations of electricity grids and gas pipelines. The European Energy Cyber Security Platform (EECSP) report[2] identifies challenges in cybersecurity specific to the energy sector, given that interdependence is the norm. Therefore, the level of the resilience of the energy system to cyber-attacks cannot simply be estimated by the level of the weakest link in the network. We should consider that elements of the energy system can oftentimes operate in isolation when needed, as well as in a more-normal wider interconnected configuration. Being able to isolate the affected components of a grid within an acceptable time frame in the event of an attack/incident may oftentimes be a winning strategy in case of an attack (either distributed or small-scale). This however depends on the capability to efficiently switch the configuration of highly interconnected components of the grid to an isolated-parts configuration while limiting the effects on standard on-going operations. This may deserve further specific analysis and studies involving CEER, ACER, NRAs, ENTSO-E, TSOs and DSOs in a coordinated effort to estimate conditions and parameters which may help in the design phase. This can aid in reducing the impact of an incident and to allow containment actions through proper design and coordinated reaction efforts based on the type of cyber-attack. Also, such an effort may conclude with the identification of optimal high-level design patterns to apply to future network projects.

Trust among all involved parties is a core aspect of any successful security strategy. Actors in energy markets work hard to build their reputation and to ensure that, from a cybersecurity perspective, they can be considered trustworthy parties. Their credibility is clearly a core value in order to operate and inter-operate in such a complex sector. A lack of trust may result from [perceived] differences in cybersecurity preparedness maturity, and the ability to isolate perceived non-trustworthy parties from the energy system. This lack of trust can limit data flow between stakeholders and may penalise some of them from a market point of view, as the stronger parties may simply not be able to accept the risk of establishing a relationship with a perceived non-fully-trustworthy party. Regulators have a key role in promoting competitive energy markets, but they should also look for ways to encourage trust among operators, in order to preserve the public interest in the cyber space occupied by the energy sector.

[1] These are International Standards Organisation/International Electrotechnical Commission family of standards for information security management systems. See https://www.iso.org/isoiec-27001-information-security.html

[2] Cyber Security in the Energy Sector Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector. See https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf

National Regulatory Authorities (NRAs) can play different roles in relation to cybersecurity: Cybersecurity needs personnel and financial resources for the operators of essential services and also for those operators who simply want to have an acceptable cybersecurity posture. It is within the bailiwick of NRAs to decide upon **acceptable costs** of regulated monopoly grid operators. Information Technologies (IT) account for these costs. Given that expenditure for cybersecurity could increase from currently 1% to 2% of the IT and OT budget to 5% to 10%, NRAs will in the future examine precisely as to which cybersecurity costs service operators declare, if they are not already doing so.

In some MS (e.g. Austria), the NRA has the legal obligation to **manage threats to security of supply**. System Operators (SOs), therefore, must report cybersecurity incidents to the NRA if they result in potential risks to security of supply. The Austrian NRA (E-Control) has established a Public-Private Dialogue (PPD) with IT experts of the energy sector (electricity and gas) who identify the risks and adequate measures. In some MS, the NRA sets out a **catalogue of obligations** for OES referring to cybersecurity. For example, in Germany the NRA (*Bundesnetzagentur* – BNetzA) – which is also a multisector regulator) has the legal obligation to set out such a catalogue. It includes the need for an IT-security management system, the relevant structure plan of the grid, a risk assessment of IT-security, appropriate reactions to handle the risks and a contact person for IT-security. In some MS, such as Luxembourg, the energy NRA (ILR) was designated as the national competent authority and single contact point under the NISD. In MS where SOs are in competition, being an OES could provide a competitive advantage as the company will already have in place the structure to follow the specific OES rules. That is, it is already OES-regulation compatible and needs little or no costly adaptation. However, not being an OES may imply less OPEX and so provide competitive advantage in a different way. Hence, being or not being defined as an OES is a potential bias in the market.

For the three reasons mentioned in the previous paragraphs (potential contagion(s), lack of trust, cost/bias in the market), CEER recommends that all parties interacting with the grid not included in the list of Operators of Essential Services should nevertheless, aim to develop and apply cybersecurity standards and measures. This may contribute to the creation of a homogenous and secure ecosystem which will allow the development of a secure culture for further innovation and digitalisation in the energy sector.

1.2 NRAs' engagement for compliance with NISD and GDPR

Taking into consideration different circumstances and experiences from the processes of national cybersecurity strategies preparation, the activities in each MS concerning the implementation of the NISD have varying intensities. In the implementation NRAs are or have been involved at different levels and intensities as well. Nevertheless, for NISD the course of actions is toward full implementation – MS have already concluded the first stage with the transposal into national legislation. The governance frameworks are being created: new bodies established, e.g. National Information Security Agencies, new relations with existent authorities formed e.g. Computer Emergency Response Team (CERT) – Energy NRA – National Cybersecurity Authority; and new roles assigned or re-defined with regulated entities.

In the energy sector, as the first amongst the essential services, the most fragile and with greatest inter-sectoral influence, the identification of essential services providers is of the utmost importance. The activities of the European Commission towards emphasising the importance of "the" essential service could potentially culminate in an additional and dedicated network code for electricity cybersecurity rules.[3] MS' initial step toward the identification of OES is, therefore, essential for comparable and effective transposal of requirements to stakeholders, taking into account financial burdens.

Additionally, more and more smart metering platforms are rolled out and smart grid applications are implemented on top of them, Market Operators (MO) and System Operators (SO) have much more data to deal with. To meet (sometimes implied) reporting obligations and to economically extract value from this large amount of data, big data technologies are implemented by those operators. The trend in optimising data access through data hubs, whether in form of retail hubs or grid hubs, is to foster efficient data access/exchange for stakeholders on the retail market, service market and grid operation which enable:

- For grid operation transmission and distribution operators to use the data to develop more accurate projections to balance the networks, contract flexibility etc.;
- For the service market, a much more detailed tracking of energy consumption and production such that developers can use this data to provide new services to the consumers that go beyond established retail services;
- For the retail market, simplification of switching processes in order to apply time-of-use tariffs and for billing processes as well. Furthermore, smart meter data can help to increase the efficiency of market party communication: e.g. the data exchange between retailers and network operators for billing and balancing processes.

The Clean Energy for All Europeans Package (henceforth, "Clean Energy Package") as proposed by the European Commission stated that "…independently of the data management model it is important that MS put in place transparent rules under which data can be accessed under non-discriminatory conditions and ensure the highest level of cybersecurity and data protection as well as the impartiality of the entities which handle data."[4]

The General Data Protection Regulation (GDPR) applies to all organisations handling personal data electronically, regardless of size and function. This includes the majority of energy companies, including operators, suppliers, contractors, and third-party supply chain organisations. GDPR focuses on protection of personal data and does not address the content of the information and does not prescribe the cybersecurity measures in relation to specific sectors. Through the implementation of Internet of Things devices (such as smart meters, sensors and actuators), the energy sector also participates in the "internet of everything" development. Smart meters offer functionalities for more effective demand/supply management, use of greener energy, and the opportunity for customers to control their own consumption and to eventually save money through informed decisions on energy consumption. At the same time, the introduction of smart grids and advanced metering infrastructures require energy companies to comply with privacy and data protection legislation.

[3] As has been proposed in the Electricity Regulation of the Clean Energy for All Europeans Package.

[4] Recital 38 of the proposed Electricity Directive of the Clean Energy for All Europeans Package.

When including security measures for protecting customer information, there will probably be an overlap between measures linked to data protection and those aimed at protecting information systems or cybersecurity measures. Such overlap can allow for optimising involvement of resources (technical and human) through the organisation of work in parallel processes.

For NRAs, as for most other organisations, knowledge about cybersecurity will become an increasingly important asset. In the future, NRAs may have a more active role in the cybersecurity game for the energy sector: being the institutional bodies closer to the markets, with specific energy-related technical knowledge, they may contribute to better analysis of trends and help the national competent authorities (when they themselves are not the national competent authority) in performing their own tasks and promoting awareness, knowledge of sectoral standards, best practices and training/awareness campaigns for the operators in the sector.

1.3 Clean Energy for All Europeans Package: an opportunity for cybersecurity

Following the adoption of the NISD and of the GDPR, further analysis was needed to assess if the two new pieces of legislation were enough to accommodate all the cybersecurity needs of the energy sector.

The NISD was the result of a very long negotiation based on a cybersecurity strategy of the EU that was already 3 years old. To better explain this, one can note that while normally there is space to evaluate the results of a strategy on a five-year time frame, cybersecurity strategies and tactics can be obsolete in less than two years. This is all linked to constant technological advancement and to research cycles which often move at an unexpected speed. The most expeditious solution was the establishment of a group of experts with the remit to analyse existing national and European regulation, and to assess if the energy sector was sufficiently covered in terms of cybersecurity measures, and, if not, which areas needed be further developed and reinforced. This was the meaning of the Energy Expert Cyber Security Platform (EECSP), which, via a study of more than one year, provided some inputs on further actions to be developed by the European Commission in the scope of cybersecurity for the energy sector.

The “Proposal for a regulation of the European Parliament and of the Council on the internal market for electricity ”, the “Proposal for a regulation of the European Parliament and of the Council on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC ”, the “Proposal for a directive of the European Parliament and of the Council on common rules for the internal market in electricity” of the Clean Energy Package laid down provisions on cybersecurity for electricity, filling some of the gaps which emerged from the work of the EECSP. The selection of the topics for further legislation by the European Commission was most probably dictated by the emerging technological trends and the work already done in the past years by other expert groups. It was noted that Smart Grids, and especially Smart Metering infrastructure, are developing quickly, and the grid, largely developed for the state of technological development of the 1970s or 1980s, is progressing fast in and running toward a massive wave of digitalisation.

The proposed measures in the Clean Energy Package tackle cybersecurity for smart meters, highlighting issues particularly pertinent to DSOs and TSOs in recognition of their key role. In the Clean Energy Package’s Electricity Regulation, the European Commission also has proposed a Network Code “on cybersecurity rules” (Art. 55), which may allow the market’s cybersecurity experts to select the appropriate cybersecurity standards and cybersecurity measures in order to operate consistently and efficiently in such a critical sector. In this context, the new proposed entity representing DSOs in the Electricity Regulation (the EU DSO entity) will share the responsibility to define the network code provisions with ENTSO-E. The Clean Energy Package also sets obligations for electricity operators to contribute to the development of resilience in the energy sector in respect to the risk of malicious cybersecurity attacks, or incidents related to the information and operational technologies widely used in the electricity sector. The final target of all the legislative proposals is to monitor and operate the grid effectively and efficiently, while taking into account the cybersecurity risks resulting from the use of new technologies and from the adaptation of old technologies to a new digitalised and complex environment.

The proposed package would touch upon some unresolved aspects of cybersecurity for energy. In particular, risk preparedness plans to be kept consistent and updated at national and regional level, and which must also be effective in potential scenarios related to cybersecurity.

The European Commission also introduced mandatory minimum-security requirements to be used in Smart Metering infrastructure (possibly already at the design phase), in order to avoid that emerging technologies would be deployed without minimum cybersecurity standards. Additionally, the proposed Clean Energy Package mandates the MS, in order to implement the plan on risk preparedness, to designate and mandate a specific authority.

An interesting part of the proposed package is the need to perform an exercise in order to validate cybersecurity scenarios, and also to verify preparedness at any level of the overall value chain within the grid.

The Clean Energy Package, as proposed by the European Commission, does not include any task for individual NRAs [on cybersecurity], but does for the ACER. The subject matter covered would surely require the input and intervention of NRAs themselves, which may be asked to work in cooperation, at national level, with National Security Agencies or National Competent Authorities for cybersecurity in Critical Infrastructure at a governmental level.

A final consideration is in relation to timing: the full or partial adoption of the proposed package through a standard co-decision process, that is, the agreement of both the European Parliament and the European Council, may be expected by the end of 2018, or, if not achievable, by the next EU Parliament which will start its work in 2019. Independently from the on-going negotiations, and taking into consideration the actual text, the Risk Preparedness Regulation may be the quickest relevant part of the package to enter into force after its formal adoption. All this depends on the order that the negotiations will be tabled. In an optimistic scenario, the complete entry into force of all the package may be completed by 2020-2021. This would be go in parallel with the possibility of having a cybersecurity-related Network Code (in the proposed Electricity Regulation) which may require still some years, and which may eventually start at the end of 2019.

NRAs, based on the mandate of the European Commission to ACER, will need to contribute to the definition of the Framework Guidelines on Cybersecurity Rules for Electricity, which would work as a baseline for the definition of the cybersecurity rules (i.e. a network code). They may also eventually be involved in the monitoring of the use of Best Available Technics (BATs) for Smart Meters and assess if Smart Meters are in line with the European Commission’s recommendations.

Looking to the work done in the context of the Clean Energy Package, which only covers the electricity sector, and being cognisant of the fact that other parts of the energy sector are subject to a lower level of risk (because of the reduced complexity of the underlining systems), it is already expected that similar measures eventually will be extended to gas, and most probably, to oil. Nuclear power, due to its specific needs and characteristics, its regulation by treaties, and, in particular, the need to cover also the full fuel lifecycle and not only the generation phase, may be regulated on different grounds.

Given that the Clean Energy Package seems to introduce a number of aspects on cybersecurity which are in favour of establishing a minimum level of cybersecurity, regulators may choose to provide guidance on parallel rules which may regulate other actors of the energy market, starting with gas. While current regulations do not require this, a forum for regulators at EU level from different sectors may be established, with the aim to agree on a cross-sectoral approach for cyber security.

Where there is no specific regulation applicable, regulators may offer their knowledge and expertise in forums and meetings with the aim of fostering understanding and the application of preventive measures related to cybersecurity matters.

The “Clean Energy Package does provide chances for more tailor-made obligations for TSOs/DSOs/suppliers in the electricity sub-sector, and, in order to be even more effective, it may be extended and adapted to the needs of entire value chain of the electricity sub-sector (e.g. to generation). It may also serve as a basis to define the additional cybersecurity needs of the rest of the energy sector (e.g. including the gas and oil sub-sectors).

1.4 NRAs’ monitoring of cybersecurity expenditure

Within the scope of increased digitalisation, the systems, the application and the components of electricity and gas system operators have been affected. Whereas previously, interventions in the grid have been made manually, especially in the grids of the larger electricity and gas operators, today most interventions are made digitally. Hence, control systems and digital services gain more importance as well as cybersecurity implications.

Even before the transformation process in digital systems, electricity and gas system operators had been investing in cybersecurity. In this area the system operator especially needs labour force and financial resources. It is within the bailiwick of NRAs to decide upon acceptable costs of regulated monopoly grid operators. Among the acceptable costs are those costs that are necessary to fulfil legal requirements. One such requirement for system operators is the responsibility for secure network operation, which also includes the mitigation of cybersecurity risks.

At date of publication, most NRAs have not distinguished cyber security costs within the cost examination for regulated entities. It can be assumed that Information Technologies (IT) is usually part of operation expenses (OPEX, e.g. IT counselling and other IT services) as well as CAPEX (e.g. software and licenses). Given that the expenditure for cybersecurity will certainly increase, NRAs should in the future make a precise and careful examination of which cybersecurity costs service operators declare.

Furthermore, and also within the implementation of the NISD, legislators have started to enforce investments in cybersecurity. For example, the German NRA has published an IT-security-requirements catalogue to define a minimum standard on what electricity and gas system operators should do concerning cybersecurity. Also, in other European countries, system operators have already defined essential service providers according to the NIS-Directive. Hence, the discussion about a minimum cybersecurity standard for energy operators is increasing.

Since the beginning of digitalisation, the number of cyber-attacks and the legal security requirements have constantly increased; system operators are expanding their action plans to ensure cyber security and are investing more in cyber security. Hence, the costs are rising. Therefore, it must be evaluated how NRAs will need to adapt their standards of cost examination in order to ensure an adequate implementation of cybersecurity costs into the revenue cap.

It is foreseeable that the costs on cybersecurity will further increase, but it is not foreseeable whether those costs will represent a significant proportion of the total costs. Therefore, specific monitoring is needed. However, to monitor those costs, the objective(s) of cybersecurity must be defined. In most European countries such definition is in process.

Within the definition of those objectives, for example, minimum cybersecurity standards for electricity and gas system operators, NRAs will be able to monitor the costs and can examine whether those costs are appropriate or not. NRAs may monitor cybersecurity related expenditure if the objective of cybersecurity is defined. Within this monitoring, the effects of those cybersecurity-related investments to the risk landscape of the energy system and of the single operator might be taken into account.

2 Organisational aspects

2.1 Change of culture

Cybersecurity for energy requires, among many things, deep knowledge of the topics, continuous awareness for staff who may be subject to those threats, continuous situational awareness for those in managerial roles and a complete change in the culture of all affected companies, especially those in the energy sector. Where this knowledge and culture is sometimes still at an early stage the change of culture means: understanding if we are over- or underestimating the threats and their impact; being able to propose simple, workable and effective solutions without disrupting existing compliance and operations; monitoring progress and acknowledging incidents and failures in policies; learning and teaching by example, especially improving information sharing; and being aware of sustainable costs. In this context regulators, having access to a number of pieces of privileged information, and having the possibility to generalise and survey at a high level the surrounding landscape, can help in efforts to boost the speed of information dissemination and to promote a fast awareness penetration speed for the energy sector, especially in the promotion of sustainability campaigns.

NRAs and in some cases, Cybersecurity National Competent Authorities, are already heavily involved in awareness activities/campaigns, at times specifically for the energy sector. The continuing sector-specific alerts coming from authorities, in addition to the press coverage on potential risks for energy and non-energy utilities, helped to keep the level of attention high at all levels of the energy supply and value chain. In this respect, there are a number of problems in preparing and providing proper awareness and training campaigns to the energy sector: the lack of technical and regulatory skills and knowledge specific for the cybersecurity in the energy sector; language barriers, especially in the lower levels of energy utilities; and the rapid development of new regulations at National and European level, sometimes energy-specific. These issues are of concern and becoming a barrier and a delaying factor which has impact on the effectiveness of the existing national and European policies. These obstacles to an efficient provisioning of awareness and training can be reduced with the intervention and support of the NRAs. NRAs may help in promoting the right awareness level and liaise with the right stakeholders, using the proper language and vocabulary, and adopting on a case-by-case basis a correct level of detail. Also, they may tailor cybersecurity awareness and training campaigns specifically for the energy sector. Moreover, the credibility, authority and independence of such institutions can help to avoid an under/overestimate the risks of cybersecurity attacks to the electricity grid and to gas pipelines and set appropriate controls and measures while still respecting pre-existing regulatory frameworks. In some cases, likely in the near future, such campaigns may also be able to be customised for the specific financial needs of each area where they are proposed, and for each class of energy operators, providing all with a suitable and consistent level of knowledge.

Among noteworthy activities already on-going, an example is the Slovene Cyber Security Forum, which is organised every year by the Slovenian Regulator (AGEN) in Maribor. Similar events, with a high level of international participation, may create the perfect set-up to share knowledge, create awareness and consolidate relationships between all the involved authorities and the energy markets. They can also serve as platforms to share concerns, needs and ideas which may help to speed improvements, optimise use of the scarce financial resources and, eventually, to gather concerns which may be addressed by further regulatory actions.

Another notable example is the annual workshop on cybersecurity held by the Norwegian Regulator (NVE) in Oslo: the workshop focuses on cybersecurity and resilience and has an international dimension. NVE already had organised two events in early Summer 2017 and 2018, where local authorities, together with the regulator and other international organisations (including ACER and CEER) had the chance to present the work already done in this field as well as work to be done in the near future. All participants were able to share ideas on activities yet to be done. The event was also a platform to share any information which could be used to create a more secure and resilient cyber landscape suitable for energy activities in various countries. With the cooperation of industry and of energy companies (and the presence of regulated entities from electricity, gas and petroleum) it became a highly appreciated event, and an opportunity to share information and knowledge, but also a place where operators can learn specific approaches to cybersecurity. This platform also was used to promote active cooperation: with the presence of the Norwegian Police Service, the national CERT, regulators, industry and market participants, it was an informal place to work together and to enable and push forward substantial culture change.

Other similar activities in EU and non-EU countries are becoming regular platforms to provide regulated entities with information on legal obligations, risks, threats, emerging issues, and to let people understand that energy regulators, even if not responsible for or in control of cybersecurity actions and activities, may still act as facilitators. They may also be open to discuss how they may further facilitate and help in the achievement of common shared goals in the context of cybersecurity for energy directly with the affected stakeholders, creating an open dialogue and preventing unnecessary discussions or those not kept at the right level.

While at national level many activities are regularly promoted and followed up by regulators together with Local Competent Authorities, at the European Level there are still a number of actors with different responsibilities and mandates, which may further contribute to the culture change and to on-going awareness and training campaigns. Being at a different level, those stakeholders may serve a different important audience. There could be an interesting progression whereby there is the possibility that ACER and CEER may initiate work with ENTSOs and DSO associations, and those ENTSOs and associations may then further provide awareness, training and guidance to all associated entities, trying to optimise the use of the scarce resources. This will not interfere with the work done at National Level by the Competent Authorities and regulators and may serve the need to have cross-border-specific awareness and training.

In sum, CEER recommends that NRAs and ACER promote culture change through activities such as partnerships and awareness campaigns which may contribute to the achievement of cybersecurity strategic objectives.

2.2 Cloud & Big Data

2.2.1 Cloud Computing and the Energy Sector

There is a strong trend for the energy sector to implement information systems, solutions and applications using Cloud computing. To take an example from the energy sector, one can look to new smart grids operators and the management and analysis of smart metering data. Looking more broadly in the energy sector, oil and gas companies and energy consulting firms are increasingly relying on partners, service organisations, and individuals outside the company firewall. Cloud-based systems naturally allow for much broader collaboration, as stakeholders are no longer bound to internal fixed assets and sites.

Cloud computing allows rapid business deployment, removes physical barriers to fast development of integrated infrastructures, accelerates process innovation, avoids large investments in expensive centralised IT infrastructures and reduces costs. However, a critical point for enterprise Cloud adoption is security considerations. Energy businesses are not clear how secure Cloud computing really is relative to risk factors such as hackers, ransomware, outages, data security flaws and data breaches. For example, the use of ransomware on a Cloud used to store utility data could risk a much higher degree of devastation if this technology is not embraced with a solid and well-structured backup and disaster and recovery policy.

Another issue emerges when we consider data protection and privacy, particularly in light of the GDPR: if a Cloud is used, data originated by an energy system may go beyond the company boundaries and can potentially create severe problems if unauthorised entities/persons have access to that data. Data classification is an essential first step to specifying security measures to which data shall be subject.

To indicate that the Cloud is already extensively used in the energy sector, some examples of Cloud computing in the Energy sector are given below, without implying any judgement on how it is used.

- The industrial conglomerate GE recently cooperated with Alstom Grid to form GE Grid Solutions, offering interactive Cloud-based tools for exploration of grid challenges and solutions in areas like substation digitisation, distribution automation, and system integrity protection.
- ChargePoint operates an electric-vehicles charging network. ChargePoint uses the Cloud to manage the charging stations and is able to provide real-time data usage and use this data to make business decisions.
- Locus Energy provides data acquisition hardware and software Cloud solutions in order to help to plan the roll out for solar power investments by collecting monitoring data on solar systems.
- Enviance's Cloud-based platform provides a number of environmental, health, safety, and sustainability solutions in order to help energy companies in effectively managing compliance obligations and regulatory responsibilities.
- GridIO is a platform that aggregates electric water heaters for use in the power reserve market. GridIO runs a self-learning algorithm to predict the consumption pattern of each electric water heater for the coming days. It can remotely switch off the electric water heaters.
- Clebox provides a service that consists of hardware and software in the Cloud. The system controls various electricity-consuming applications so that the hourly electricity market price, distribution tariff and weather information are used to minimise the energy cost.
- Reactive Technologies delivers services through the Cloud connected to Generators, grid operators and Businesses. It provides opportunities for grid operations, and wholesale and balancing markets.

Cloud computing technology is deploying steadily in energy sector systems. Cloud services need to directly incorporate security from the beginning of the solution design. End users (utilities and customers) should be informed of the potential security risks and existing protection measures when the solution is implemented. The applicable security measures should be in line with the security classification of the energy information stored within the Cloud boundaries, and both the classification and the applicable security measures, should be regularly reviewed by an independent accredited cybersecurity body if used in the provision of essential energy services.

2.2.2 Use of Big Data in the energy sector

Whilst ICT technologies have long been incorporated into large generation facilities, trading floors, dispatch centres and transmission grids, they are now spreading into distributed energy resources, distribution grids and even appliances in consumers' homes. Advances in technologies, telecommunications and data analytics – digitalisation 4.0[5] – are progressively changing the consumer environment.[6] Home devices can be connected to one another, generate and exchange massive sets of data (Big Data) – yielding new insights into consumer habits and preferences. Consumers will have more control over their energy usage and have a greater potential to be active consumers in the energy market. The 2020 roll-out target for Automated Meter Infrastructure (AMI) is approaching and investments into Smart Grid domain are on the rise.

Full sector digitalisation allows suppliers to have a deeper and improved relationship with their customers. Data is becoming more granular and new tools are being developed to better tailor communication, increase transparency and, most importantly, develop more personalised offers and services.

Digitalisation holds a lot of promise, but it also provides consumers, regulated entities (DSOs and TSOs) and commercial players with new challenges. One of the major issues is exchange and handling of Big Data in a safe and regulatory-compliant way[7]. The European Union Agency for Network and Information Security (ENISA) has rightly recommended in its paper[8] several measures for treating Big Data, which are restated here in summary:

- **Privacy by Design Applied** (Anonymisation in Big Data) - Data Protection Authorities, data controllers and the Big Data analytics industry need to actively interact in order to define how privacy by design can be practically implemented (and demonstrated) in the area of Big Data analytics, including relevant support processes and tools.
- **Decentralised versus centralised data analytics** - The research community and the Big Data analytics industry need to continue their efforts in combination towards decentralised privacy-preserving analytics models. Policy makers need to encourage and promote such efforts, both at research and at implementation levels.
- **Transparency and control** - The Big Data analytics industry and the data controllers need to work on new transparency and control measures, putting the individuals in charge of the processing of their data. Data Protection Authorities need to support these efforts, encouraging the implementation of practical use cases and effective examples of transparency and control mechanisms that are compatible with legal obligations.
- **User awareness and promotion of Privacy Enhancing Technologies (PETs)** - The research community needs to adequately address aspects related to the reliability and usability of online PETs. The role of the Data Protection Authorities is central in user awareness and promotion of privacy preserving processes and tools in online and mobile applications.

[5] CEER co-organised a 2018 EUSEW event on this: https://eusew.eu/clean-energy-40-designing-new-era-all-europeans-together

[6] For more on this, see also the CEER Report on Smart Technology Development, 5 June 2018.

[7] EURELECTRIC. The power sector goes digital: Next generation data management for energy consumers, A EURELECTRIC report, 2016. https://cdn.eurelectric.org/media/2029/joint_retail_dso_data_report_final_11may_as-2016-030-0258-01-e-h-4CFC4569.pdf

[8] ENISA. Privacy by design in Big Data. An overview of privacy enhancing technologies in the era of Big Data analytics, 17 December 2015. https://www.enisa.europa.eu/publications/big-data-protection

- **A coherent approach towards privacy and Big Data** - Policy makers need to approach privacy and data protection principles (and technologies) as a core aspect of Big Data projects and relevant decision-making processes.

2.3 Stakeholders' cybersecurity strategy

In the scope of a holistic policy protection plan for the energy system, stakeholders should be setting out the strategy and concrete, feasible actions – a clear and effective cybersecurity strategy – for the gradual and structured implementation of the appropriate security measures and policy standards, in order to ensure the smooth functioning of the energy system which supports vital services for the community.

So, prior to embracing new technologies such as Cloud computing or systems for the handling of Big Data and Cloud computing, certain actions should be considered. What follows are a few crucial actions for consideration.

2.3.1 Action 1: Identification and evaluation of national Critical Infrastructure and processes

Energy Stakeholders are the most appropriate for this action and should have it be a priority as it is essential for the effective implementation of national strategies for the protection of Critical Infrastructure (CI). The listing of all stakeholders with responsibilities related to CI protection issues is an important prerequisite for the optimal sharing of responsibilities, the avoidance of duplication and for facilitating the implementation of monitoring and coordination of relevant actions. There are many scattered actions of actors that could be used as part of a structured strategy. However, the necessary coordination is lacking.

A prerequisite for the protection of the CI is the continuous and systematic recording of these critical elements (sections, subdomains, services and systems). The development and validation methodology should include all the necessary procedures for identifying and evaluating CI to be implemented by the relevant national bodies in the framework of a national strategy for the protection of national CI.

2.3.2 Action 2: Strategic Protection Planning for Critical Infrastructure

The strategy and the proposed actions must ensure the following objectives:

- Maintaining the integrity, resilience and availability of CI.
- Minimising the impact of threats and ensuring an effective response to emergencies, by increasing the resilience of the CI and the ability to recover in the event of an incident. This will involve establishing a task force to review legal impediments to reconstitution and recovery after an attack against a piece of critical infrastructure or key asset.
- Supporting the goals for the country's development, thereby contributing to the well-being of citizens.

2.3.3 Action 3: Collaboration with the designated Responsible Bodies

Stakeholders should develop and implement properly Crisis Management Strategies, National Digital Strategies and National Security Policies, developed in terms of the needs, objectives, priorities and orientation of the Civil Protection of the national CI.

2.3.4 Action 4: Planning and Resource Allocation

Stakeholders should identify six major initiatives in this area:

- Create collaborative mechanisms for government and industry critical infrastructure and key asset protection planning.
- Identify key protection priorities and develop appropriate supporting mechanisms for these priorities.
- Foster increased sharing of risk-management expertise between the public and private sectors.
- Identify options for incentives for private organisations that proactively implement enhanced security measures.
- Coordinate and consolidate national protection plans.
- Develop an integrated CI and key asset geospatial database.

2.3.5 Action 5: Coordination of actions

A framework for cooperation and exchange of information between all the involved (public or private) bodies with the public authorities should be clearly defined, so that the response strategy to the protection of national CI will be more efficient. Without underestimating the security measures for the protection of individual national infrastructure and information systems, it is clear that the implementation of individual Security Plans without the national Cyber Security Strategy is not enough. Implementation of the Critical Infrastructure Protection Policy should be implemented through an Action Plan which sets out a clear and defined timetable.

In addition to a CI assessment methodology, it is necessary to systematically identify and assess the threats, weaknesses and security risks of CI. A National Risk Assessment Methodology should be adopted to categorise national critical data on the consequences and threats to the safety of CI.

3 Conclusions

Based on the analysis presented in this report, CEER has developed the following recommendations. They address different aspects of cybersecurity which, in the view of CEER, are crucial to establishing a sufficient cybersecurity posture in line with the needs of the current energy markets in the European Union and current legislative projects. The recommendations take into consideration the on-going efforts in implementing already-existing cybersecurity-related regulation.

The recommendations are directed to different actors who are playing, or may play in future, an active role in the complex resolution of the cybersecurity issues for the energy system. Among the actors we describe an obvious active role for are TSOs, DSOs, suppliers, generators and market operators, though this is not an exclusive list. In the view of the CEER, a more pro-active role may be assigned to NRAs, as they will have to face many of the issues raised in this report quite soon (if not already), and, in particular, they will oftentimes have to come to an understanding of how to deal with the financial/budgeting aspects of cybersecurity.

Finally, a role is also foreseen for CEER and ACER: they can play a crucial role in the establishment of an international cybersecurity culture (including in CEER Members/Observers that are not from EU MS), which can support and complement the work of the NRAs.

Recommendations
All parties interacting with the grid not included in the list of Operators of Essential Services should, nevertheless, aim to develop and apply cybersecurity standards and measures. This may contribute to the creation of a homogenous and secure ecosystem, which will allow the development of a secure culture for further innovation and digitalisation in the energy sector.
NRAs should, as far as possible within their legal powers, proactively engage with energy stakeholders in order to encourage them to be in compliance with the NIS Directive and provide support for transposing horizontal regulation into sector-specific best practices which may help with an effective implementation of that directive.
The Clean Energy for All Europeans Package does provide opportunities for more tailor-made obligations for TSOs/DSOs/Suppliers in the electricity sub-sector, and, in order to be even more effective, it may need to be extended and adapted to the needs of entire value chain of the electricity sub-sector (e.g. to generation). This legislative package may also serve as a basis to define the additional cybersecurity needs of the rest of the energy sector (e.g. including the gas and oil sub-sectors).
NRAs may also want to/be required to monitor the cybersecurity related expenditure and the effects of those cybersecurity-related investments to the risk landscape of the energy system and of individual operators. NRAs, in particular, need to be prepared to monitor and evaluate cybersecurity expenditure of certain regulated entities
CEER and ACER can promote culture change through activities such as partnerships and awareness campaigns which may contribute to the achievement of cybersecurity strategic objectives and which may complement the work of the NRAs.
Management in energy-sector entities, including NRAs, should provide clear guidance on cybersecurity governance, including the role and, eventually, as in other international examples, the proper place and role for the chief information security officer (CISO). Having a reference contact point in all operators, provided with independence, resources, and a proper mandate from top executive management, may further develop in a positive way the cybersecurity landscape. Providing CISOs with proper skills and resources, and with proper executive commitment, may help in achieving ambitious goals in a shorter time.
TSOs/DSOs/Suppliers should have a cybersecurity strategy and they should set clear and effective cybersecurity measures prior embracing new technologies such as Cloud computing or systems for the handling of Big Data: this may allow the further development of a cybersecurity culture within the energy sector.

Table 1 – List of cybersecurity recommendations of CEER

Annex 1 – List of abbreviations

Term	Definition
AMI	Advanced Metering Infrastructure
BATs	Best Available Technics
CAPEX	capital expenditure
CEER	Council of European Energy Regulators
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
DSO	Distribution System Operator
EECSP	European Energy Cyber Security Platform
ENISA	European Union Agency for Network and Information Security
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
ID number	Identity number
IoT	Internet of Things
IT	Information Technologies
MO	Metering Operator
MS	Member State (of the European Union)
NISD	Directive concerning measures for a high common level of security of Network and Information Systems across the Union
NRA	National Regulatory Agency
OES	Operators of Essential Services
OPEX	operational expenditure
OT	operational technology
SO	System Operator
TSO	Transmission System Operator

Annex 2 – About CEER

The Council of European Energy Regulators (CEER) is the voice of Europe's national regulators of electricity and gas at EU and international level. CEER's members and observers (from 36 European countries) are the statutory bodies responsible for energy regulation at national level.

One of CEER's key objectives is to facilitate the creation of a single, competitive, efficient and sustainable EU internal energy market that works in the public interest. CEER actively promotes an investment-friendly and harmonised regulatory environment, and consistent application of existing EU legislation. Moreover, CEER champions consumer issues in our belief that a competitive and secure EU single energy market is not a goal in itself, but should deliver benefits for energy consumers.

CEER, based in Brussels, deals with a broad range of energy issues including retail markets and consumers; distribution networks; smart grids; flexibility; sustainability; and international cooperation. European energy regulators are committed to a holistic approach to energy regulation in Europe. Through CEER, NRAs cooperate and develop common position papers, advice and forward-thinking recommendations to improve the electricity and gas markets for the benefit of consumers and businesses.

The work of CEER is structured according to a number of working groups and task forces, composed of staff members of the national energy regulatory authorities, and supported by the CEER Secretariat. This report was prepared by the Cyber Security Work Stream of CEER's Distribution System Working Group.

CEER wishes to thank in particular the following regulatory experts for their work in preparing this report: Stefano Bracco, Leontini Kaffentzaki, Roman Picard, Janez Stergar, Elbert Jan van Veldhuizen and Carolin Wagner.

More information at www.ceer.eu.