CEER
Council of European Energy Regulators

The Cybersecurity Act in the Energy Context

A CEER Response Paper on the
European Commission's Cybersecurity Proposals

8 December 2017

1. Introduction

CEER considers cybersecurity threats as one of the key risks to a future well-functioning EU energy market as well as to the security of supply of electricity and gas. The increased complexity of information and operation technologies in modern energy systems means that the importance of cybersecurity is rapidly growing in the energy sector. Information Technologies (IT), Operation Technologies (OT - covering industrial control systems and supervisory control and data acquisition (SCADA)) and their cybersecurity are vital to retain the actual level of efficiency, fairness and competitiveness of the EU's energy markets and to assure their stability for the future. CEER believes that a coordinated European approach to cybersecurity/risk-preparedness is critical in securing energy systems and infrastructure and planning their future development.

The European Institutions have issued a number of proposals and adopted Directives and Regulations over the years to deal with cybersecurity, the latest of which was on 23 September 2017, when the European Commission issued a proposal which includes specific articles on the European Cybersecurity Certification Scheme, known as the Cybersecurity Act[1]. The Cybersecurity Act has been presented for public comment, and in response, CEER has formulated this Regulatory Response Paper.

The proposed Cybersecurity Act introduces the following important changes, some of which may eventually affect the cybersecurity ecosystem within the energy sector:

- It proposes a reinforced role for ENISA (the "EU Cybersecurity Agency"), with a permanent and wider mandate;
- It introduces a European Cybersecurity Evaluation framework and its schemes, which will be acceptable at EU level, and can be used on a voluntary basis;
- The European Cybersecurity Evaluation framework and its schemes will entirely replace the existing National Schemes used for the same purpose;
- The proposed resulting certification will attest that information and communications technology (ICT) products and services that have been certified in accordance with such a scheme comply with specified cybersecurity requirements.

As the tool will be valid at EU level, it may allow the national energy regulatory authorities (NRAs) to easily assess up-front the compliance of planned infrastructure with high cybersecurity standards, or with the cybersecurity standards/needs befitting new investments.

[1] 2017/0225 (COD) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") COM(2017) 477 final/2 – see https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF

2. Key Regulators' Recommendations

CEER welcomes the European Commission's proposal to establish a substantial and structured step forward to set up a stronger European system for cybersecurity. CEER sees these new proposals as potentially aiding European energy regulators in their daily regulatory functions. This is especially the case when there is the need to have the proper tools to analyse and authorise specific investments on critical infrastructure which is expected to be in place for more than 20 years and which may be subject to cybersecurity risks. However, the proposed legislation poses some issues which European energy regulators believe should be reconsidered before final legislation is approved. In this context, CEER recommends certain changes that could improve the draft legislation:

- ***Clarify the role and type of certification regarding cybersecurity schemes for energy markets***
  1. The proposed system is crucial to secure important aspects of the functioning of electricity grids and gas pipelines, and to assure security of supply to all citizens, and its application to the crucial energy sector requires further specification. As the electricity sector is still dependent on products and services provided by other industrial sectors (e.g. some distribution system operators (DSOs) may use telecommunication services provided by a third service provider instead managing their own network), extending the use of the same or analogous schemes to those sectors may help in creating a homogeneous ecosystem for cybersecurity for the energy sector. Moreover, the proposed legislation should also take into consideration the considerable efforts resulting from previous legislation and which contributed to the set-up of a secure and safe cybersecurity ecosystem for the energy sector, as well as consider the implications of currently-proposed legislation.

- ***Ensure that existing national and European rules on cybersecurity schemes in the energy sector remain in force***[2]
  2. In some Member States (MSs), certification schemes in the energy sector are already successfully established, for example, in the implementation of Smart Meter systems. These certification schemes are already providing a reliable cybersecurity standard which was established in a complex and detailed process – and where the associated costs for establishing those schemes and standards have already been borne. Where a MS has already established cybersecurity standards, the European regulation must include these standards as a minimum requirement. If the European Commission decides upon a scheme with a lower cyber security standard, it has to be ensured that member states which already have higher developed standards can maintain them.

- ***Clarify energy regulators' role and the need for an energy cybersecurity strategy***
  3. Clarify what is the exact role of Europe's Energy Regulators in the cybersecurity scheme development process and what their interaction is to be with Security Agencies and other involved authorities. It is also important to explain if the new proposed regulation is part of a wider medium- and long-term strategy for NRAs to allow effective use of the Cybersecurity Certification Schemes in the energy sector.

[2] Note that this point is not further elaborated upon in following sections of this paper, given the relatively simple proposal.

- ***Set a clear obligation for the active participation of energy regulators prior to setting up schemes which may impact energy markets***

4. Energy market participants (which may be among the end-users of the proposed legislation), assisted by Energy Regulators, must be given the possibility to influence and/or help in the definition of Cybersecurity Certification Schemes. Experience has shown that it is vital that regulators have a fair say in the cybersecurity scheme development process – this is crucial since ENISA provides IT-knowledge but to protect ICT-products in the energy sector an advanced level of knowledge about the sector itself is required. Without the involvement of regulators, it might be certified that certain ICT products comply with a particular (EU) cybersecurity standard but it would remain unclear if those products can actually fulfil their functionality regarding the market and system rules.

- ***Allow for a more-gradual and better-defined transition phase, particularly when it has an impact on critical infrastructure, in line with the evolution of cyber threats***

5. In order to be effective in the energy sector, the proposed schemes should include a reasoned and coherent way to adapt the standards to the technological and national/regional context in which they are going to be applied. They should allow for certain well-justified exceptions and deviations in order to prevent any distortion of energy markets, as well as to prevent any unnecessary increase of costs for the operators and tariffs for the consumers. It should also be possible to use more severe standards in those countries which are technologically mature and where more-stringent rules would not have unreasonable economic implications.

- ***Increase cooperation among sectors for defining cybersecurity schemes and for subsequent activities to implement controls***

6. Create an explicit means for cooperation amongst interdependent sectors to create schemes that take into account a wide range of variables and scenarios for greater effectiveness. These means of cooperation should also contribute to more-effective post-implementation controls.

- ***Strengthen the role of ENISA (the "EU Cybersecurity Agency") in respect to the use of the European Cybersecurity Certification Framework and its schemes***

7. It is understood that ENISA will play a key role in the long-term strategy for cybersecurity of the EU. ENISA will also play a key role in the processes of drafting and adoption of the cybersecurity certification schemes: In addition to the proposed permanent mandate, it would be beneficial for ENISA to be tasked with the ability to provide advice and guidance on the use of the schemes in specific sectors, in coordination with other EU agencies. This is because in some MSs such cybersecurity certification schemes do not exist yet. Therefore, ENISA could create a catalogue of minimum-standard requirements on ICT products but the MSs should be given the right to develop/develop further and implement those schemes based on their national particularities.

3. Clarify the role and type of certification regarding cybersecurity schemes for energy markets

If the certification schemes are not meant for energy markets, this should be clarified, and the European Commission should state which measures need to be implemented in order to provide a minimum common level of cybersecurity for the European electricity grid and for the continent's gas pipelines. In particular, energy market experts have proposed two main strategies to achieve a common level for cybersecurity:

- The first strategy focuses on the adoption of a flat system of minimum security standards, at a central level, which would become compulsory for all market participants in order for them to operate in that market. Compliance is based on a periodic self-assessment and declaration by energy sector participants, with sporadic audits carried out by NRAs or by an accredited third party.
- The second envisaged strategy would instead focus on a "security in-depth" approach: this approach would make use of the proposed certification pattern whereby ICT and OT products used in the context of electricity grids and gas pipelines will have to be certified prior their deployment. This approach would be greatly enhanced by having an independent third party providing assurance on compliance of the operators and the suitability of the deployed solutions chosen. In this approach, a certification will be issued under the new proposed schemes, and the certification framework would remove the burden from Energy Regulators on performing inspections, as the cybersecurity certification schemes would already include a process for renewal and verification of compliance.

In any case, existing regulations are still vague on which sectors and contexts may benefit and shall use the cybersecurity certification schemes. This would need to be further elaborated and clarified to allow an efficient and effective use of the proposed Cybersecurity Act. It is CEER's general view that if all critical sectors are to apply the schemes in a consistent way, the EU will need to have the assurance that all Critical Information Infrastructure, in the medium-to-long term, will be protected applying a "security in-depth" approach, certified by a pool of accredited and independent third parties.

The use of a set of minimum required security standards, with a light degree of control, would remove the possibility of having a higher standard that is regularly verified by a third-party authority. In addition, it would prevent regulators from using the certification as a way to have a certain assurance for authorising ICT products in line with the highest standards. Moreover, while such a system may set a common baseline based on simple rules, it would eventually weaken the efforts of those MSs already adopting and using higher cybersecurity standards. Therefore, CEER would tend to support the "security in-depth" approach.

In order to undertake this approach, the proposed legislation should be reviewed in order to more-specifically address the envisaged use of such schemes and the context in which they would be used. Moreover, if the certification is aimed to be used in the context of the implementation of a "security in-depth" strategy applicable to the energy sector, this may require study and consideration of the current measures listed in the "Clean Energy for All Europeans" (Clean Energy) package which seem to approach an analogous issue with perhaps a different strategic perspective. The "Smart metering functionalities" related to cybersecurity in Article 20 (b) of the Electricity Directive[3] could be compared with the simple obligation of a certification based on a dedicated scheme established on the security features already identified by the European Commission. That scheme may easily refer to the "best available techniques" referred to in the same article. The network code on cyber security rules proposed in Article 55 (o) of the Electricity Regulation[4] could also be considered for further study in light of the proposed Cybersecurity Act.

[3] Proposals regarding the Directive on common rules for the internal market in electricity (COM(2016) 864 final/2) and its Annexes (recast).

[4] Proposals regarding the Regulation on common rules for the internal market in electricity COM(2016) 861 final/2 and its Annexes (recast).

More generally, there is a need to coordinate efforts included different proposed legislative packages such as the Clean Energy package, the Cybersecurity Act, and potentially, others. There is also the need to avoid any change which may contradict or simply nullify the existing proposed texts, or even confuse market actors on the aims and strategic objectives that the European Commission intended to achieve. As mentioned previously, while the rules proposed in the Clean Energy package would aim to provide a minimum level of security, it is the opinion of CEER that, following the line proposed by the Title III "Cybersecurity Certification Framework" of the Cybersecurity Act, a certification scheme for smart meters would be an option to consider in respect to the existing proposals with the purpose of maintaining open competition on manufacturing markets related to the energy markets and achieving a secure smart grid.

4. Clarify energy regulators' role and the need for an energy cybersecurity strategy

The formulation of a clear and coherent cybersecurity energy strategy is essential to understand the extent to which existing and proposed legislation need to converge in order to provide guidance for energy markets. Energy markets need clarity on these issues in order to function efficiently and to make adequate investment to mitigate cybersecurity risks. In order to effectively carry out such legislation, energy (and other sectors) regulators' role needs to be clear in such legislation, and in particular, in the proposed Cybersecurity Act. Likewise, financial responsibilities should be clearly defined.

In addition, in the recent "Joint Communication to the European Parliament and the Council – Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"[5], it is stressed that there is a need to have specific strategies and approaches to allow the financial services, energy, transport and health sectors to tackle specific issues. In this respect, it is suggested that "…general cybersecurity strategies would be complemented by sector-specific cybersecurity strategies in areas like financial services, energy, transport and health."[6] While the need for specific cybersecurity strategies at sector level is clearly recognised, those strategies should also clearly identify the required actors and their respective roles. In the proposed European Cybersecurity Certification framework, it would be important to embed already-known aspects of those sector-specific strategies, and assign roles and responsibilities in order to gain some clarity. This applies particularly to the provision of clarity at sector-specific level and for companies operating in the sector. This will also help in building trust within the energy cybersecurity eco-system, and remove uncertainties for the future.

5. Set a clear obligation for the active participation of energy regulators prior to setting up schemes which may impact energy markets

If the use of specific obligatory schemes is the chosen methodology to tackle the supply chain problem,[7] then these schemes must take into account that the benefits of the use of such a scheme cannot jeopardise already-existing policy efforts, nor create an unacceptable impact on operators, consumers and the quality of services. In sum, the implementation of cybersecurity measures needs to be part of the same type of heuristic analysis which is done for any new

[5] JOIN(2017) 450 final – see http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN.

[6] Ibid., p. 6.

[7] Sharing information with suppliers is essential yet increases the risk of that information being compromised, as some of them are several tiers removed from the originating organisation. The issue is that these suppliers' ability to protect data can be highly variable.

investment. Therefore, certification should be a type of baseline in order to authorise investments and evaluate cost recovery on cybersecurity related investments. In this context, the position of NRAs in the cooperation framework of the Agency for the Cooperation of Energy Regulators (ACER) must to be taken into account and NRAs must have a greater say in the preparatory phase of those schemes which may impact the energy sector. This means that Article 44 (2) of the proposed Cybersecurity Act[8] should define regulators as among the relevant stakeholders and ENISA should not merely consult with them, but be required to accept a degree of guidance on pertinent issues. Moreover, bearing in mind that the certifications schemes also define processes and procedures to issue certificates, when those certificates relate to products which are meant to be used in the energy sector and which may be part of investments, Energy Regulators must participate actively in order to provide opinions on the most efficient processes to be applied for certification and renewal. Regulators also need to be closely involved so as to understand the concerns of DSOs and TSOs involved in the process, and, in particular, their assessments of the size and allocation of financial resources toward cybersecurity. Finally, energy regulators are best-placed to define metrics which may help in establishing standards for a prudent approach to cybersecurity investments. Those metrics and associated monitoring activities may be helpful for the fine tuning of the cybersecurity certification schemes.

6. Allow for a more-gradual and better-defined transition phase, particularly when it has an impact on critical infrastructure, in line with the evolution of cyber threats

The adoption of new cybersecurity schemes, policies and procedures should have a well-defined transition phase. This is necessary, as on-going work and already-existing interactions between regulators and authorities managing certification schemes and certifications cannot be viewed simply on the level of a new scheme at an EU level. This may jeopardise existing cybersecurity efforts and create risks for the transition phase. It should not be forgotten that the proposed Cybersecurity Act comes from the need to defragment the cybersecurity certification market, but European energy regulators also see an opportunity to make use of the new certification to harmonise cybersecurity in the EU in various sectors, including the energy sector. This requires a proper transition, which may depend on the way that the certification schemes are meant to be used. The transition, even with a very gradual approach, should still take into consideration the need to keep the existing national schemes in parallel with the future European Schemes for the certification of ICT products and services. The proposed schemes should also adapt to the rapid evolution of the threat landscape, and allow agile ways to deal with newly emerging threats. Finally, it must be understood that the success of the proposed Cybersecurity Act lies not so much in its required security features and their use, but rather, on the field of applicability, scope and use that its resulting certified products may have.

7. Increase cooperation among sectors for defining cybersecurity schemes and for subsequent activities to implement controls

As already emphasised, ENISA will need to consult stakeholders at the start of the adoption of new schemes, which would allow any stakeholder, including CEER and individual NRAs, to provide feedback. An additional layer of cross-sectoral cooperation focusing specifically on new schemes may have a large and positive influence on achieving a safe cybersecurity space overall. For the

[8] Article 44: "Preparation and adoption of a European Cybersecurity Certification Scheme".

energy sector in particular, one can note that all certifications for smart meters and smart grid solutions are likely to have a great impact. Hence, cooperative arrangements may help in setting up an efficient flow of information, together with a more-coherent network of adoption/implementation controls on several dimensions. In addition, in the "Joint Communication to the European Parliament and the Council - Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" has already identified that a relatively small number of sectors may need a specific approach: all those sectors are already cooperating in some respects, but due to their operational differences, have never established real cooperation on cybersecurity topics. Nevertheless, in general, it is highly unlikely that the schemes, if they were formulated having a particular sector in mind, would achieve the same objectives on the same products in any another sector: in this respect, the European Commission should establish a system of cooperation and coordination which aims to adopt best practices, with the long-term objective to have a limited number of schemes applicable to many sectors. The same element of cooperation and coordination may be beneficial in the control phase as well, where multiple entities may be able to identify risks independently from their expertise and sector where ICT products and services are used. Finally, regulators may also provide assistance to the national certification supervisory authorities. These factors should all be taken into consideration for the revision and extension of Articles 49 and 50 of the proposed Cybersecurity Act.[9]

8. Strengthen the role of ENISA (the "EU Cybersecurity Agency") in respect to the use of the European Cybersecurity Certification Framework and its schemes

The proposed legislation of the European Commission aims to provide ENISA with a permanent and comprehensive mandate focused on markets and, more in particular, cybersecurity. Nevertheless, under Article 8 "Tasks relating to the market, cybersecurity certification, and standardisation" the task of providing guidance and assistance to MSs and their public authorities, including regulators, is not addressed neither mentioned. Taking into consideration the need to prepare the markets for the use of the EU Cybersecurity Certification Framework (which implies use of the specific legislative tools that were never used before in the context of some of the regulated sectors, e.g., of the energy sector), CEER views it as beneficial to provide ENISA with a central role in this respect to this task. ENISA, under the new proposed mandate, may additionally coordinate efforts with other relevant EU Agencies (e.g. ACER) in order to increase efficiency in the use of already-scarce resources. The extension of the mandate in this direction will provide regulators, and not only energy-related ones, with the possibility to synchronise their efforts toward the adoption of appropriate forthcoming schemes. It will provide them with the possibility to rapidly adapt to the change of strategies at EU level, and, at the same time, provide the EU with the possibility to gain an overview on the actual level of fragmentation in respect to the use of the cybersecurity certification schemes. This permits the EU to have both a vertical and a sectorial view.

Annex 1: Other background Information

European Energy Regulators have been dealing with a number of requests for new investments on EU electricity grids and gas pipelines: while some investments are simply improving the existing quality of service and assuring to all citizens access to energy resources, some others have had the aim of increasing the level of automation of both grids and pipelines. The latter type increased

[9] Article 49 "National cybersecurity certification schemes and certificates"; Article 50 "National certification supervisory authorities".

efficiency and reduced costs for operators and thereby, consumers. Some of those investments helped increase transparency, which is a key element in establishing well-functioning and competitive markets. The need to improve on efficiency, which can be achieved only by the intensive use of distributed automated decision-making systems, fits with the need to deliver energy at an affordable price to all EU consumers, but it requires a comprehensive evaluation of risks, including those that may derive from the use of new automated systems.

European Energy Regulators have experienced reduced capacity in terms of their human resources, together with an increased technological complexity of the grid that requires specific ICT and OT knowledge in order to be properly assessed. European cybersecurity measures will need to take into consideration a large diversity in capacity, both human and financial, among NRAs as well.

CEER has observed cybersecurity trends with great attention. In this respect, the attacks on the grids of countries neighbouring the EU has created some anxiety for both regulators and national security agencies (NSAs). NRAs and NSAs have begun cooperating closely in order to mitigate the risks of cybersecurity-related incidents with an extensive impact on energy grids in the EU.

Among various activities, some NRAs have started to work on delivering clear instructions to all regulated entities on the acceptable use of ICT and OT products and solutions on grids and pipelines. There are several examples of successful stories (e.g. from MS NRAs BNetzA (Germany), CRE (France), E-Control (Austria)) which focus on different methods and processes, but which all aim to substantially improve the security posture of those MSs that decided to make substantial investments in this area.

Many experts have expressed to the European Commission (Directorate General of Energy) the need to define ex-ante the cybersecurity requirements that would apply to all systems connected to grids and pipelines, and to set up a clear process which would involve, when necessary, the judgement of European Energy Regulators which are responsible to authorise investments at a national level.

The European Commission proposes a unified approach based on a European Cybersecurity Certification Scheme, which, whilst trying to address security issues related to supply chain processes, also creates a number of discrepancies in respect to the processes and methods already in place at MS level. This unified approach should, however, consider the effect of a similar change on the existing Cybersecurity Certification Schemes already used by some NRAs. Regulators play a key role not only within MSs, but also at a European level, and have the responsibility to assure that their regulated infrastructures are secure from a cybersecurity perspective. Additionally, regulators are already involved in complex escalation systems which make very good use of National Cybersecurity Evaluation Schemes. Those escalation systems and patterns must be reviewed constantly to also allow an active role for regulators, something not easy to achieve.

Going more in detail, the European Certification Scheme takes into consideration different assessment levels, which fits very well with the need to secure different assets with different risk profiles, especially if pertaining to Critical Information Infrastructure. In this respect, the certification scheme takes into consideration only products and services, but not the full range of energy systems and their priorities from a pure global operational perspective (e.g. the need for availability which can require the sacrifice other security elements, such as integrity and confidentiality in extreme circumstances). This would require a more careful analysis of the specific needs of the sector, which is already clearly stated in the "Joint Communication to the European Parliament and the Council – Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", released the same day as the Cybersecurity Package, and which aims to complement the existing EU Cybersecurity strategy.

In addition, when discussing critical infrastructure, it should be taken into consideration that the cybersecurity maturity level of the grid very much depends on a number of elements and on the maturity of the actors involved. Moreover, it is contingent on factors which may influence the grid but which are not depending solely on ICT solutions and services. Finally, the proposed schemes are generic, such that in the existing formulation it is not clear if there is any space for sector-specific schemes for specific product categories and classes. The schemes and the proposal, if seen together with the Network Information Security (NIS) Directive[10] and the Directives and Regulation covering other aspects on Cybersecurity on Energy,[11] aim to stabilise and standardise cybersecurity scenarios, without taking into consideration the different level of maturities, nor providing a clear indication on the patterns that all MSs and their NRAs should follow. In the case of the energy sector, a clear and well-defined EU cybersecurity strategy that is sector-specific but with a common direction may help to avoid and mitigate risks for MSs (one or multiple), which have different levels of understanding of cybersecurity and different appetites for risk.

Moreover, European Cybersecurity Certification Schemes and the accompanying certifications are voluntary, and may be compulsory only if requested by [new] EU rules. NRAs may need to have clear guidance if this tool is the most appropriate one to deal with already-existing acquisitions of new strategic assets, and may need to remind the markets that the energy sector will never be completely risk free from a cybersecurity perspective.

CEER recognises that the proposed Cybersecurity Act is a remarkable effort to standardise the certification of cybersecurity products at the European Union Level and in the energy sector. Moreover, when the schemes start to be applicable to the energy sector, this tool will allow all regulators to easily assess compliance with the requirements in terms of security for critical and non-critical infrastructure in the energy sector. Nevertheless, such a system, if applied at European level and in absence of any transition phase, may have a financial impact on markets, including that of energy, which may not be correspond to the expected results in terms of risk mitigation. In fact, it does not really take into due consideration (particularly in the case of energy markets) the technological gaps and difficulties which some regulators may face if the same scheme is applicable to all of the EU, independent of the level of maturity and the underlining technologies deployed on field. The European transmission and distribution system networks are highly technological and all implementation connected to these requires careful planning and implementation. The cost of implementing cyber security measures is likely to be very high for the market participants, government agencies and other actors. However, to not implement cybersecurity measures will mean, in the final analysis, putting electricity transmission in the entire EU at risk, which would strike at the very heart of modern society and is, prima facie, unacceptable.

[10] 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 – see http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

[11] These include: the Risk-Preparedness Directive (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 (COM(2016) 862 final) and its Annexes – see http://eur-lex.europa.eu/resource.html?uri=cellar:1d8d2670-b7b2-11e6-9e3c-01aa75ed71a1.0001.02/DOC_1&format=PDF; the aforementioned Electricity Directive; and the aforementioned Electricity Regulation.