Framework Guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows

(Draft)

PC_2021_E_04

30 April 2021

European Union Agency for the Cooperation of Energy Regulators
Trg Republike 3
1000 Ljubljana, Slovenia

This Document contains the Framework Guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows, which the European Union Agency for the Cooperation of Energy Regulators (ACER) has prepared pursuant to Article 59.2(e) of Regulation (EU) 2019/943 and on the basis of the request from the European Commission.

EU reference documents

- 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 - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148
- Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R1485
- COMMISSION RECOMMENDATION (EU) 2019/553 of 3 April 2019 on cybersecurity in the energy sector - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H0553
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) - https://eur-lex.europa.eu/eli/reg/2019/881/oj
- Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC - https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2019%3A158%3ATOC&uri=uriserv%3AOJ.L_.2019.158.01.0001.01.ENG
- Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity - https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0943
- Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0944
- Smart Grids Task Force - Expert Group 2 – Cybersecurity - Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management. - https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_report_final_report_2019.pdf
- Commission Implementing Decision (EU) 2020/1479 of 14 October 2020 establishing priority lists for the development of network codes and guidelines for electricity for the period from 2020 to 2023 and for gas in 2020 - https://eur-lex.europa.eu/eli/dec_impl/2020/1479/oj
- Summary of the responses to the targeted stakeholder consultation to set up the priority list, published by the European Commission – DG Energy on July 2020 - https://ec.europa.eu/energy/sites/ener/files/summary_for_publication_ares.pdf

- Joint Communication to the European Parliament and the Council - The EU's Cybersecurity Strategy for the Digital Decade - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=JOIN:2020:18:FIN
- Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM(2020) 823 final) - https://ec.europa.eu/transparency/regdoc/rep/1/2020/EN/COM-2020-823-F1-EN-MAIN-PART-1.PDF
- Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities (COM(2020) 829 final) - https://ec.europa.eu/transparency/regdoc/rep/1/2020/EN/COM-2020-829-F1-EN-MAIN-PART-1.PDF
- European Commission: Invitation to draft framework guideline on sector-specific rules for cybersecurity aspect of cross-border electricity flows, Reference ARES(2021)653629, 27/01/2021- https://www.acer.europa.eu/Media/News/Documents/2021.01.22%20MK%20585504%20letter%20to%20ACER_cybersecurity_final_22.1.2021%20amended.docx.pdf

Table of Contents

1 General Provisions

1.1 Scope

This Framework Guideline aims at setting out clear and objective principles for the development of a network code on cybersecurity pursuant to Article 59, paragraph 2(e) of Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (henceforth referred to as the "Electricity Market Regulation").[1] The Electricity Market Regulation provides for the establishment of a network code on sector-specific rules for cyber security aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management (henceforth referred to as the "Network Code").

On 28 January 2021 the European Commission invited the European Union Agency for the Cooperation of Energy Regulators (henceforth referred to as ACER) to start drafting a Framework Guideline for a Network Code on cybersecurity, taking into account some high-level objectives [2] and the extensive preparatory work completed so far (e.g. the recommendations of the Smart Grid Task Force Expert Group 2 report[3] and the recommendations of the European Network of Transmission System Operators for Electricity (ENTSO-E) and Distribution System Operator (DSO) associations included in the final report[4]). After the drafting process, the network code will be evaluated by ACER, taking into account its degree of compliance with this Framework Guideline.

1.2 Definitions and acronyms

The following definitions shall apply to this Framework Guideline:

- Definitions in Article 2 of the Electricity Market Regulation.
- Definitions in Article 2 of Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (henceforth referred to as the "Electricity Market Directive").[5]
- Definitions in Article 4 of COM/2020/823 final - Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (henceforth referred to as the "Proposal for a NIS2 Directive").[6]

The following definitions are intended to further clarify the provisions of this Framework Guideline and are without prejudice to the definitions to be included in the network code.

- **Critical assets:** see "essential assets".

[1] OJ L 158, 14.6.2019, p. 54–124
[2] Objectives for the network code was communicated in the invitation letter from EC to ACER to draft a framework guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows.
[2] OJ L 158, 14.6.2019, p. 125–199
[3]
[4] Final Report 19 February 2021, Recommendations for the European Commission on a Network Code on Cybersecurity - https://ec.europa.eu/energy/sites/default/files/nccs_report_network_code_on_cybersecurity.pdf.
[5] OJ L 158, 14.6.2019, p. 125–199
[6] https://ec.europa.eu/transparency/regdoc/rep/1/2020/EN/COM-2020-823-F1-EN-MAIN-PART-1.PDF

- **Computer Security Incident Response Team (CSIRT):** CSIRT refers to a team of Information Technology (IT) experts who handle security related incidents. The term CSIRT is normally equivalent to and interchangeable with CERT (Computer Emergency Response Team).

- **Cyber-attack:** any cyber incident triggered by malicious intent where damages, disruptions or dysfunctionalities are caused.[7]

- **Cybersecurity posture:** refers to an organisation's overall defence (including procedures and processes) against cyber-attacks and incidents.

- **Early warning:** a provision of concrete, serious, reliable information indicating that an event may occur which is likely to result in a significant deterioration of the electricity supply situation and is likely to lead to electricity crisis.[8]

- **Electricity cybersecurity perimeter:** the cybersecurity perimeter that includes all essential assets, all important assets and all assets that belong to the electricity undertakings concerned by the obligations of the network code. Cybersecurity perimeter refers to the cyber systems (hardware or software) to either keep intruders out or to keep captives contained within the surrounding boundary.

- **Electricity cybersecurity region:** all electricity undertakings, including all assets included in their cyber perimeter, that report and belong to the same Regional Coordination Centre[9] for the purpose of electricity operations.

- **Electricity Cybersecurity Risk-Index(es) (ECRIs):** the indexes that synthesise the risk level of an electricity undertaking or of a group of electricity undertakings in a single or in a set of risk of index(es);

- **ECRI Caps (ECRICs):** the value of the index above which an electricity undertaking or a group of electricity undertakings are considered to be an "essential electricity undertaking", otherwise is considered to be "important electricity undertaking".

- **Electricity undertaking:** as defined in Article 2(57) of the Directive 944/2019 of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU means a natural or legal person carrying out at least one of the following functions: generation, transmission, distribution, aggregation, demand response, energy storage, supply or purchase of electricity, and who is responsible for the commercial, technical or maintenance tasks related to those functions, but does not include final customers.

- **Essential assets:** the minimum set of assets without which cross-border electricity flows cannot be ensured in a single electricity cybersecurity region. Asset types include people, products, information and processes which are assessed as essential by an electricity undertaking.

[7] https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology - Page 7

[8] Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC.

[9] Regional Coordination Centres established pursuant to Article 35 of the Energy Market Regulation.

- **Essential electricity undertaking:** an electricity undertaking that, in the event of a cybersecurity incident or attack impacting its operations, presents a high-risk to suffer and cause a relevant impact to cross-border electricity flows.

- **Essential perimeter**: the cybersecurity perimeter that includes all essential assets (or those assets owned or operated by essential electricity undertakings).

- **Essential service suppliers:** a natural or legal person who operates or provides directly or on behalf of an operator any IT and/or Operational Technology (OT) system, sub-system, service or product, or any of their combinations, that is/are indispensable to allow efficient cross-border electricity flows with the purpose to store, deliver, produce, aggregate or commercialise electricity to final customers.

- **Important electricity undertaking:** an electricity undertaking which is not defined as essential but is larger than the small and micro enterprises, and therefore plays an important role in the context of cross-border electricity flows.

- **Important perimeter**: the cybersecurity perimeter that includes all assets that are owned by an important electricity undertaking.

- **Information Technology (IT):** Involves information being processed in computers and transferred across data networks.

- **Legacy systems:** hardware and/or software systems that need to be interconnected and that are used in the context of electricity cross-border flows and because of their obsolescence, cannot be modified or updated in order to meet minimum cybersecurity requirements. They include also hardware and/or software systems that cannot be protected by other means without causing damages, disruptions or dysfunctionalities to electricity cross-border flows operations.

- **Managed Security Service Provider (MSSP):** a provider of Security Operation Centre (SOC) services for entities who lack such capabilities themselves and/or prefer to outsource such services.

- **National Competent Authorities for cybersecurity in Energy (CS-NCA):** all national competent authorities with specific competence for the energy sector and responsible for the implementation of cybersecurity in the energy sector at National level.

- **National Competent Authorities for Risk Preparedness (RP-NCA):** all authorities established under Article 3 of Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC (henceforth referred to as the “Risk Preparedness Regulation”).

- **National Regulatory Authorities (NRAs):** all regulatory authorities, in accordance with Article 57(1) of the Electricity Market Directive and Article 39(1) of Directive 2009/73/EC.

- **Operational technology (OT):** involves the use of computers and data networks to operate physical systems, e.g. electric grid operation.

- **Originator**: An entity that initiates an information exchange, sharing or storage event.

- **Processor**: An entity that legitimately processes information, independently from its ownership.

- **Regional Cooperation Centres (RCCs):** as defined in Article 35 of the Electricity Market Regulation.

- **Security Operation Centre (SOC):** refers to an entity staffed with one or more IT and/or OT experts who perform security related tasks such as log analysis, incident detection, incident handling and security configuration.

1.3 Applicability of the network code

The network code is addressed to public and private entities defined in Table 1 that shall be referred to in general as electricity undertakings. The list in Table 1 is constructed with respect to paragraph (57) of Article 2 of the Electricity Market Directive. The network code shall apply only to entities in Table 1 which are classified as essential or important electricity undertakings.

Table 1: Entities to whom the network code shall apply

#	Entity definition
1.	Electricity undertakings referred to in paragraph (57) of Article 2 of the Electricity Market Directive
2.	ENTSO-E, the EU-DSO Entity, ACER and NRAs
3.	National Competent Authorities for Risk Preparedness, SOCs, National Competent Authorities for cybersecurity in Energy and CSIRTs
4.	Regional Coordination Centres referred to in Article 35 of the Electricity Market Regulation
5.	Essential Service suppliers as defined in this Framework Guideline

As a general principle, the network code shall not apply to small[10] and micro[11], unless explicitly stated otherwise. As an exception to this principle, the proposal for a NIS 2 Directive foresees the possibility to include in the list of essential/important services also small and micro enterprises when they have a relevance on cybersecurity matters. On these bases, the network code could also apply to those small and micro enterprises that cover specific essential or important roles in the cybersecurity value chain of cross-border electricity flows.

Therefore, the network code must provide for the possibility of applying it to small and micro enterprises at the initiative of:

i) any entity listed in Table 1;
ii) the CS-NCA jointly with the respective NRA of the concerned Member State; and
iii) the European Commission, ACER, after consulting and having obtained a positive opinion from the competent NRA(s) and the CS-NCAs.

To determine objectively if the concerned small or micro enterprise be classified either as important or essential electricity undertaking, the network code shall define an index (that may take into consideration parameters such as financial turn over, company size in terms of average number

[10] In the Electricity Market Directive, a small enterprise is defined as an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million.
[11] In the Electricity Market Directive, a micro enterprise is defined as an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million.

of staff employed, etc.). The network code shall clearly indicate the method to calculate such index and the thresholds to apply this exception, referred as “size cap”.

The network code shall establish for all small and micro enterprises below the size cap and not classified as important electricity undertakings or as essential electricity undertakings the implementation of basic cyber hygiene requirements in line with the “Review of Cyber Hygiene practices”[12] from the European Union Cybersecurity Agency (ENISA), or with any specific guidance document for energy small and micro enterprises in the energy or electricity sector which ENISA may release in the future.

1.4 Territorial scope and representatives of essential service suppliers not established in the Union

The network code shall apply to electricity undertakings in Table 1 which are classified as essential or important electricity undertakings and that are established and operating in the EU. The network code shall also apply to essential service suppliers (Table 1 at point 10) not established in the Union when delivering services to electricity undertakings in the Union.

Where an essential service supplier not established in the Union is delivering services to an Electricity undertaking who is in the Union, that essential service supplier should designate a representative unless the processing is occasional, does not include data processing, is not on a large scale, or is unlikely to result in a risk to electricity undertakings in the EU. The representative should act on behalf of the essential service supplier and may be addressed by any supervisory authority. The representative should be subject to enforcement proceedings in the event of non-compliance with the network code by the essential service supplier.

1.5 Classification of entities subject to the network code by Electricity Cybersecurity Risk Index (ECRI)

The notion of cybersecurity risk may have a relative connotation depending on the entity assessing it. Hence, the network code shall allow to determine the cybersecurity risks exposures of different electricity undertakings. This determination shall allow for prioritisation of interventions, and categorisation of the electricity undertakings on objective grounds with the purpose to apply proportionate cybersecurity measures. In order to do the above, the network code shall set up a clear methodology to classify entities at Table 1 and essential or important small and micro enterprises. In particular, a relevant methodology shall:

i) assess objectively the risk level(s) to which each electricity undertaking is exposed, both in isolation and in correlation with any other electricity undertaking or group of them to which the entity is connected for the purpose of information and cross-border electricity flow operations, through one or more risk index(es), named Electricity Cybersecurity Risk-Index(es) (ECRIs); and

ii) define one or more ECRI Caps (ECRICs), above/below which an electricity undertaking or group of them shall be classified as “essential electricity undertaking”/”important electricity undertaking”.

The network code shall foresee the regular revision and publication of the list of “Essential electricity undertakings” and of the “Important electricity undertakings” on a web site accessible to

[12] https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport

all potential stakeholders and managed by ENTSO-E and/or the EU DSO Entity. It shall be jointly managed by ENTSO-E and the EU DSO Entity.

For new entities covered by the list in Table 1, the network code shall establish that their start of operations shall be subject to the prior execution of an information asset inventory and a risk assessment as well as their final classification in one of the two categories (essential/important).

1.6 Transitional measures for the classification of entities

In the absence of a standard risk assessment methodology, ENTSO-E and the EU-DSO Entity, advised by ENISA and ACER, and with the assistance of the National Regulatory Authorities and of the National Competent Authorities for Cybersecurity, shall propose to European Commission a transitional lists of "**Essential electricity undertakings**" and of the "**Important electricity undertakings**". The transitional lists shall be published on a web site accessible to all potential stakeholders and jointly managed by ENTSO-E and/or the EU DSO Entity.

The classification of entities shall be justified by factual information that shall focus on the risks that digital interconnected systems and sub-systems of each electricity undertaking or group of them may impact cross-border electricity flows. To do so, the network code shall take into consideration at least the following areas in the risk assessment:

- the level of digitalisation of the electricity undertaking or groups of electricity undertakings involved in cross-border electricity flows;
- the level of interconnection and information exchange of the concerned electricity undertaking with other entities listed in Table 1;
- the level of cybersecurity posture of the electricity undertaking or the lowest level of cybersecurity posture when a group is involved;
- an estimation of the contribution of the electricity undertaking or the group of electricity undertakings to the reliability of the cross border electricity flows.

2 Cybersecurity Electricity Governance

2.1 General principles

The implementation of 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 (henceforth referred to as the "NIS Directive")[13] has shown the importance, especially in cybersecurity, to establish a solid governance that shall distinguish between the strategic and decisional role and the operational roles. In addition, the EU Cybersecurity Act[14] has also stressed the importance of a central support and advisory role for ENISA.

These two main principles will be reflected in the governance of the cybersecurity for the electricity sector in the network code, providing a role, where possible, to the same actors that have already demonstrated the ability to lead such efforts.

[13] OJ L 194, 19.7.2016, p. 1–30
[14] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) - https://eur-lex.europa.eu/eli/reg/2019/881/oj

At the same time, the network code shall take into account that, in order to carry out cross-border operations of the electricity system efficiently, there is already a governance that shall be maintained to ensure the reliability of the energy system, and not to interfere or jeopardise the objectives already reached through other network codes.

The network code shall limit the creation of its governance to the essential bodies that shall be able to participate in the decisions and operations described in the following chapters, without invalidating the role of EU entities with existing competences in cybersecurity and operation of the electricity system.

To enact this, the network code will need to consider the following:

Article 8 of the NIS Directive already establishes the **"National Competent Authorities for Cybersecurity in Energy (CS-NCA)"**: the authorities work as a single point of contact, serving the purpose to have an overview also on sectors (like the telecommunication sector and the gas/oil sector) which the electricity sector is highly dependent on. Those authorities are already provided with a liaison function to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States. Therefore, the network code shall not aim to create new national authorities but shall take into consideration the possibility that the National Competent Authorities for Cybersecurity in Energy will work in close cooperation with National Regulatory Authorities in charge of the Electricity sector, when there is any need to coordinate, institutionalise and supervise operators involved in the implementation and execution of the network code. Therefore, coordination of all national competent authorities of each Member State shall be handled at national level, and not raised at EU level when it concerns the first cycle of risk assessment and risk management, as well as when it concerns the monitoring of the implementation of minimum and advances cybersecurity standards, the monitoring of the security requirements and the close control of the supply chain for the electricity sector involved in cross border of electricity flows;

Article 9 of the NIS Directive establishes the **"Computer Security Incident Response Teams (CSIRTs)"**: the CSIRTs already monitor incidents at national level. They can therefore also provide early warnings, alerts, announcements and dissemination of information to the relevant stakeholders about risks and incidents, and they can respond to incidents. Nevertheless, they may not possess the knowledge and skills necessary to process information in the context of cross border electricity flows and they may be unable to operate in a highly technical and specialised environment. Therefore, while recognising their leadership in being cybersecurity information hubs to receive cybersecurity incident reports, early warning reports and reports on vulnerabilities affecting the grid, the CSIRTs shall be supported in their work by a team of specialists in cross-border electricity flows when the cybersecurity issue affects entities listed in Table 1.

The network code shall recognise the need for a close collaboration among the CSIRTs network, on the one hand, the National CSIRTs and, on the other hand, the **Regional Coordination Centres**, which are cross-border electricity flow specialists. This cooperation should be clearly defined. The rules for cooperation shall apply to the handling of a cross-border electricity incidents with the potential of a cascading effect on one or more cybersecurity electricity regions. In this case, the network code shall provide clear rules for an escalation and a clear leadership role on decisions regarding the handling of an incident that may need the involvement of all those entities.

Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC (henceforth referred to as the "Risk Preparedness Regulation")[15] established **National Competent Authorities for Risk**

[15] OJ L 158, 14.6.2019, p. 1–21

Preparedness (RP-NCA) to carry out risk assessments, prepare risk preparedness plans at the national level and participate in the preparation of regional plans that include scenarios related to cybersecurity risks. Therefore, to establish consistency between specific new cybersecurity risks and the cybersecurity scenarios, the network code shall foresee active participation of such entities in cross-border risk assessment and make sure that the methodologies do not overlap.

National Regulatory Authorities in charge of the electricity sector took already part to the elaboration of this Framework Guideline and possess specific knowledge of the electricity sector and relevant knowledge of the cybersecurity cross-border risks. Therefore, their active participation in cooperation with the national competent authorities for cybersecurity and risk preparedness is essential to assure consistency and play their competences. Furthermore, they are crucial to assess the cost-effectiveness of cybersecurity investments as well as to help ACER in monitoring the implementation of the network code and benchmarking costs at EU level.

Finally, the **Electricity Coordination Group (ECG)**, established pursuant "Commission Decision of 15 November 2012 setting up the Electricity Coordination Group" has among its tasks to "serve as a platform for the exchange of information and coordination of electricity policy measures having a cross-border impact". Thus, the ECG shall be informed periodically on the establishment and implementation of this network code.

3 Cross-Border Risk Assessment

As clearly described in chapter 8 of the SGTF EG2 / Cybersecurity Report of June 2019, the objective of the Cross-Border Risk Assessment is to identify risk scenarios for the operational reliability of the electricity systems that, through a cyber-incident or -attack, can generate adverse events that impede the regular circulation of cross-border electricity flows and/or the regular distribution of electricity to a relevant part of the consumer audience.

3.1 Requirement of asset inventory

The cybersecurity network code shall foresee an asset inventory as a preliminary step for the electricity cybersecurity risk assessment. Therefore, the network code shall set rules to clearly identify the cybersecurity perimeter through harmonised individual asset inventory of each electricity undertaking. These individual inventories shall be compiled by each electricity undertaking or through their own representatives and/or associations. They shall include both physical and information assets for cross-border electricity flows and shall be extended to processes and procedures that contribute to cross-border electricity flows or that are interconnected to any of those systems or processes enabling such electricity flows.

The asset inventory shall assess and clarify the existence and interdependence of:

i) Physical and virtual assets
ii) Information assets
iii) Processes
iv) Procedures
v) Roles and skills
vi) Existing procedural rules implementing cybersecurity concepts
vii) Existing capabilities embedded in physical and virtual assets capable to improve cybersecurity posture
viii) Existing compliance of IT and OT assets operated by electricity undertakings with applicable cybersecurity standards.

All assets shall contribute actively to the system operations for cross-border electricity flows.

Among other benefits, the network code shall also allow, through the asset inventory, to easily identify legacy systems that will not be able to reach a sufficient minimum level of cybersecurity. Therefore, the network code shall also provide specific mechanisms for the identification and treatment of the legacy systems, the protection and/or replacement of which shall be considered carefully in a broader context and with a long-term perspective.

3.2 Definition of the scope applicable to the asset inventory and definition of the electricity cybersecurity perimeter

The network code shall emphasize that the asset inventory and the definition of the electricity cybersecurity perimeter shall be essential to:

i) the identification and mitigation of the risks related to legacy systems with interconnection and limited or no capability to implement cybersecurity protection features;
ii) the identification of critical assets subject to advanced cybersecurity requirements;
iii) the prioritisation of further actions to control the supply chain in the context of the electricity critical infrastructures subject to elevated cybersecurity risks; and
iv) the identification of geographical areas where electricity cybersecurity exercises may help preparing and testing plans to mitigate the effect of an adverse event.

Once the potential cyber-attack surface and the specific scope of the asset inventory have been defined, the network code shall define the methodologies and tools to perform the asset inventory and shall define the electricity cybersecurity perimeter based on clear rules and harmonised templates.

Since the nature of cybersecurity threats may change over time, the network code shall foresee a mechanism to set a dynamic scope for the asset inventory and for the definition of the cybersecurity perimeter, taking into consideration the variability of the threats, the overall security context of the cybersecurity region and also the level of vulnerability associated with the assets within a certain cybersecurity perimeter.

The scope applicable to the asset inventory and to the subsequent definition of the electricity cybersecurity perimeter shall be reviewed on regular basis (at least once every two years). It shall be detailed enough to include new assets subject to new threats and vulnerabilities of the electricity system, with the potential to disrupt cross-border electricity flows.

3.3 Definition of the scope of the cybersecurity risk assessment of cross-border electricity flows

The network code shall emphasize that the cybersecurity risk assessment for cross-border electricity flows shall be essential to:

i) application of the principle of proportionality to all the measures based on the level of cybersecurity exposure, capabilities and on a risk based approach;
ii) identification of electricity undertakings that may be essential in certain scenarios that are not considered critical in the current risk preparedness framework;
iii) identification and application of fair cybersecurity standards based on a more heuristic perspective of cybersecurity threats; and

iv) identification of candidate scenarios for the electricity cybersecurity exercises that may help to mitigate the effect of an adverse event in complex conditions.

As already stated, the ongoing mutations of cybersecurity threats that may affect cross-border electricity flows will require the network code to provide a mechanism to set a dynamic scope for the cybersecurity risk assessment.

In other words, the scope of application of the cybersecurity risk assessment of cross-border electricity flows shall be periodically reviewed. The experience gained in recent and past attacks shall be taken into account as well as all incidents and impacts recorded in the past, isolated or aggregated, that affect the regular execution of cross-border electricity flows.

The review shall be detailed enough and shall include new assets subject to new threats and vulnerabilities of the electricity system that could disrupt cross-border electricity flows.

3.4 Rules, methodologies and tools for the execution of the cybersecurity risk assessment of cross-border electricity flows

Once the potential cyber-attack surface and the specific perimeter of concern have been defined, the network code shall define the rules, methodologies and tools to perform a risk assessment on multiple levels of the electricity sector. The cybersecurity risk assessment shall especially focus on the effects of cyber-attacks on cross-border electricity flows.

To carry out the risk assessment and establish the rules, methodologies and tools, the network code must take into account that the Risk Preparedness Regulation already provides for the identification and updating of risk preparedness plans, at three levels: regional crisis scenarios (Article 5), national crisis scenarios (Article 7) and more general electricity scenarios (Article 6). Taking as a guiding principle, the network code, in the absence of a better system, will have to set rules to carry out a risk assessment at these three levels in order to allow all stakeholders to express their concerns and to identify where they may be affected by an incident, taking into account:

i. their asset inventory and electricity cybersecurity perimeter (first level of cybersecurity risk assessment);

ii. Member States to identify scenarios that may potentially escalate to a trans-national cybersecurity incident or attack (second level of risk assessment); and

iii. cybersecurity electricity regions to assess, together with the risk assessments performed and consolidated on the previous two levels, which scenarios would likely disturb or impede the regular execution of cross-border electricity flows (third level of risk assessment).

The development in three levels and rounds may further narrow down the list of essential assets and the essential perimeter that may cause a critical incident for electricity cross-border electricity flows.

The network code shall take into account the definition of the important and essential perimeters and assets resulting from the second level of risk assessment.

The methodology will provide the rules for the definition of the ECRIs and ECRICs as described in chapter 1.5 which, together with the distinction of important vs essential electricity undertakings, will allow to clearly identify the stakeholders subject to minimum vs advanced cybersecurity standards.

All methodologies shall be able not only to measure compliance with specific technical requirements, but also to provide means to assess the cybersecurity maturity of energy operators, Member States and electricity regions for cross border electricity flows. This is required to properly guide further actions and spending, as well as incentivise long-term investments and innovative measures in cybersecurity after the adoption of the network code.

The network code shall enforce existing methodologies for the transition period to be used for cross-border risk assessment purposes until the final methodology described below is delivered. In this line, for the first level, after defining a suitable scope, the risk assessment methodologies described and/or further developed in ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 and ISO/IEC 27019, can provide solid foundation for conducting a cybersecurity risk assessment. For second and third levels, after defining the proper scope, the risk assessment methodologies described and/or further developed in ISO/IEC 27005 and ISO 31000, can provide the basis for conducting a cybersecurity risk assessment for cross-border electricity flows**.**

3.5.1 Governance of the steps of the cybersecurity risk assessment for cross-border electricity flows

For the purposes of preparatory work and the execution of the risk assessment, the network code shall provide for the following specific governance that allows all relevant stakeholders to appropriately participate in the network code implementation activities:

1. all entities included in the list in Table 1 through their own representatives and/or associations should be consulted and shall actively participate in the definition and revision of the scope dedicated to the first level of the asset inventory, the electricity cybersecurity perimeter and the cybersecurity risk assessment of cross-border electricity flows;
2. all Member States through their Cybersecurity National Competent Authorities, in cooperation with the National Regulatory Authorities in charge of the electricity sector and the National Competent Authorities for Risk Preparedness, shall be consulted and shall actively participate in the definition and revision of the scope dedicated to the second level of asset inventory, the electricity cybersecurity perimeter and the cybersecurity risk assessment of electricity cross-border flows;
3. the cybersecurity electricity region through the Regional Coordination Centres shall be consulted and shall actively participate in drafting the definition and revision of the scope dedicated to the third level of asset inventory, the electricity cybersecurity perimeter and cybersecurity risk assessment of electricity cross-border flows; and
4. the ECG, assisted by ACER and advised by ENISA, shall be informed and consulted in order to provide an opinion on the scope per each level and eventually align with the risk assessment already done in the scope of implementation of the Risk Preparedness Regulation.

For the drafting of the methodologies concerning asset inventory and electricity cybersecurity perimeter definition, as well as the rules, methodologies and tools for the execution of the cybersecurity risk assessment of cross-border electricity flows based on the scope defined at the previous point:

5. All entities that have mandated or delegated other entities for the purpose of the drafting shall be consulted on the draft of the methodology;
6. the ECG, assisted by ACER, and advised by ENISA, shall be informed and consulted in order to provide an opinion on the methodology; and
7. The ECG shall eventually align with the risk assessment already done in the scope of implementation of the Risk Preparedness Regulation.

For the purpose of the execution of the cybersecurity Cross-Border Risk Assessment for the first level, each electricity undertaking will be responsible,

8. For the execution of the cybersecurity Cross-Border Risk Assessment for the first level, all entities listed in Table 1 shall execute the risk assessment based on scopes at point 4 and rules, methodologies and tools at point 6. Results shall be provided for further escalation to the Cybersecurity National Competent Authorities, in cooperation with the National regulatory authorities in charge of the electricity sector, and in cooperation with the National Competent Authorities for Risk Preparedness for further escalation.
9. For the execution of the cybersecurity Cross-Border Risk Assessment for the second level, all Member States through their Cybersecurity National Competent Authorities, in cooperation with the National regulatory authorities in charge of the electricity sector, and in cooperation with the National Competent Authorities for Risk Preparedness shall execute the risk assessment based on scopes at point 4 and rules, methodologies and tools at point 6, and relevant results shall be provided to the respective cybersecurity electricity region for further escalation;
10. For the execution of the cybersecurity Cross-Border Risk Assessment for the third level, the cybersecurity electricity regions through the Regional Coordination Centres, after receiving all necessary information as result of the risk assessment at point 9, shall execute the risk assessment based on scopes at 4 and rules, methodologies and tools at point 6. The results shall be consolidate in a Cross-Border Electricity Cybersecurity Risk Assessment Report (see chapter 7) that shall be provided to the NIS Coordination Group for further analysis, and especially to identify crucial interdependencies with other sectors where an additional level of harmonisation may be needed.
11. The Cross-Border Electricity Cybersecurity Risk Assessment Report shall assess and certify the improved state of the cybersecurity posture of the electricity sector. It shall be prepared jointly by ENTSO-E and the EU DSO Entity with contribution from the stakeholders listed in Table 1 and shall be submitted to the European Commission and to ACER.
12. Within three months of receipt the report at point 11, ACER shall provide the European Commission with its opinion after consulting ENISA and the ECG.
13. Within three months of receipt ACER's opinion, the European Commission shall deliver an opinion on the Cross-Border Electricity Cybersecurity Risk Assessment Report.
14. Within three months of receipt of the positive opinion from the European Commission, ENTSO-E and the EU DSO Entity shall adapt and publish the final version of the Cross-Border Electricity Cybersecurity Risk Assessment Report.
15. The ECG shall eventually align with the risk assessment already done in the scope of implementation of the Risk Preparedness Regulation.

4 Common Electricity Cybersecurity framework

The network code shall promote the harmonisation of cybersecurity maturity across the EU. To foster a common minimum electricity cybersecurity level, the network code shall aim to make all electricity undertakings apply a framework of principles, requirements and standards which will have a positive impact on the cybersecurity posture of the electricity undertakings and on the overall cybersecurity posture of the EU cross-border electricity flows.
To harmonise the cybersecurity landscape while ensuring proportionality between the actual risk profiles of each undertaking[16] and the cybersecurity requirements to be standardized, the network

[16] with the exclusion of small and micro enterprises that do not contribute in any way to cross-border electricity flows, for which simple norms on cyber hygiene are considered to be just sufficient

code shall list a set of common minimum cybersecurity principles and obligations -the baseline maturity level- that all undertakings listed in Table 1 must apply. In addition, the network code shall define an advanced cybersecurity standard only for essential electricity undertakings involved in cross-border electricity flows -the advanced maturity level-.

In order to preserve investments and security plans already in place, the network code shall ask ENTSO-E and the EU-DSO Entity, assisted by ACER and ENISA, to provide **an electricity principles/standards mapping matrix (EPSMM)** with a list of all applicable cybersecurity electricity standards that provide instruction on the implementation of a specific principle, as well as a definition of the level of maturity in electricity cybersecurity that shall be associated with such implementation.

The network code may entrust ENISA, assisted by ACER and by the Joint Research Centre of the European Commission, with the development of a **European Cybersecurity Electricity Maturity Model (ECEMM)**, the objective of which will be to guide all electricity undertakings in the implementation of the minimum and advanced cybersecurity maturity levels that are not present in the available standards. In this respect, the ECEMM shall complement and later may replace the EPSMM.

The aim of the harmonisation of minimum and advanced cybersecurity maturity levels, and of the EPSMM and ECEMM, is to allow the electricity undertakings to continue investing in cybersecurity plans without interfering with the selection of standards. It will also allow the use of existing international and national standards and legislations, while harmonising the requirements for all the electricity undertakings.

The application of the principles shall be verifiable by a third party, which shall be accredited through an accreditation model and considered as a conformity assessment body in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council.

Existing national legal obligations that impose already the implementation of certain cybersecurity principles to the electricity undertakings shall be introduced and listed as well in the EPSMM as they will be equivalent to a certifiable standard.

Non-certifiable standards, or those for which there is no certification process, shall be excluded from the EPSMM unless it includes an explanation of the requirement to certify their implementation and verification of compliance based on another existing international standard.

The two sets of principles (i.e. for the minimum cybersecurity requirements and for the advanced cybersecurity requirements) shall cover the areas presented in Table 2.

Table 2: Cybersecurity areas the network code shall address, mapped to electricity undertakings who shall be subject to requirements in the listed cybersecurity areas. V = Compulsory, V* = Implicit but not enforced

	Cybersecurity areas	Small and Micro Enterprises[17]	Minimum Requirements (Important electricity undertakings)	Advanced Requirements (Essential electricity undertakings)
1	Basic Cybersecurity Hygiene requirements (see last paragraph of Chapter 1.3)	✓	✓*	✓*
2	Obligation to compile an asset inventory and to define the internal electricity cybersecurity perimeter		✓	✓
3	The assets potential impact on cross-border electricity flows shall be described in the inventory.			✓
4	Obligation to perform a cybersecurity risk assessment, including the evaluation of the cybersecurity maturity of the implemented measures/controls to manage risks at point 2 of this table.		✓	✓
5	Take part to a cross-border cybersecurity Risk assessment for electricity cross-border flows, including the evaluation of the cybersecurity maturity of the implemented measures/controls to manage risks identified at point 2 of this table.			✓
6	Obligation to implement measures and controls to mitigate risks, based on the minimum set of cybersecurity principles/standards to manage risks at point 4 of this table.		✓	✓
7	Obligation to apply common Functional and Non-functional requirements to all inventory assets		✓	✓
8	Prioritize application of common Functional and Non-functional requirements to assets that take part to cross-border electricity flows.			✓
9	Obligation to take part and contribute to the information sharing and dissemination system for the electricity cybersecurity cross-border flows and monitoring, benchmarking and additional reporting obligations.		✓	✓
10	Obligation to establish incident handling procedures.		✓	✓
11	Obligation to set procedures in case of a disruption to cross-border electricity flows.			✓
12	Obligation to take part to the Crisis Management System (CyCLONe)		✓	✓
13	Obligations on the Supply Chain Security and on the Certification of Components taking part to the operations of cross-border electricity flows.			✓
14	Participation in electricity cybersecurity exercises (see chapter 6).			✓

Such list may be complemented where ENTSO-E and the EU-DSO Entity deem it necessary and justifiable to further improve the cybersecurity posture of the electricity cross-border flows.

[17] In this context, Small and Micro Enterprises below the Size Cap defined at chapter 1.3 and not classified as either important electricity undertaking or essential electricity undertaking

Point 2 and point 4 of Table 2 shall be considered to comply with the obligations set and described in chapter 3, as most of the current standards include those steps. In this case the obligation shall be deemed to be fulfilled also in case the asset inventory and the risk management are compiled/performed using a different standard but including at least the scope in Table 2 for the asset inventory, electricity cybersecurity perimeter, and the cybersecurity risk assessment of cross-border electricity flows.

Within a period of three months from the entry into force of the network code and in absence of a minimum and/or an advanced cybersecurity standards, ENTSO-E and the EU-DSO entity, advised by ENISA and ACER and with the assistance of the National Regulatory Authorities and the National Competent Authorities for Cybersecurity, shall prepare a **transitional list** of national regulations of electricity cybersecurity and EU/International standards to be implemented by the important electricity undertakings or essential electricity undertakings in preparation for the implementation of the minimum cybersecurity standard or advanced cybersecurity standard, respectively.

The transitional list of electricity cybersecurity national regulations and EU/International standards shall be published on the web site of ENTSO-E and EU-DSO Entity, and shall be made accessible to all potential stakeholders.

4.1 Governance for the definition of minimum and advanced lists of principles, and for the preliminary EPSMM

For the purposes of definition of minimum and advanced list of principles and the preliminary EPSMM, the following specific governance shall be followed to ensure the appropriately participation of all relevant stakeholders in the network code implementation activities:

1. All entities listed in Table 1 (through their own representatives and/or associations) and all Member States (through their National Competent Authorities for Cybersecurity, in cooperation with the National Regulatory Authorities responsible for the electricity sector and the National Competent Authorities for Risk Preparedness) shall be consulted and should actively participate in drafting the list of principles to be implemented by the minimum/advanced cybersecurity electricity standards for the cybersecurity of cross-border electricity flows.

2. ENTSO-E and the EU-DSO Entity jointly, assisted by ENISA, shall consolidate the list of principles at point 1 of this list.

3. ACER, assisted by ENISA, shall issue an opinion on the drafted list of principles at point 2 of this list.

4. The European Commission shall adopt the drafted list of principles based on their compliance with the mandate for the network code and the strategic objectives of the EU.

5. All entities listed at Table 1 (through their own representatives and/or associations) and all Member States (through their National Competent Authorities for Cybersecurity in cooperation with the National Regulatory Authorities in charge of the electricity sector and the National Competent Authorities for Risk Preparedness), taking into account the principles of the list at point 4, shall be consulted and actively participate in the elaboration the list of standards, national regulations and non-certifiable standards to be introduced in the EPSMM as well as in its prioritisation for the implementation of minimum and advanced cybersecurity standards in the network code.

6. ENTSO-E and the EU-DSO Entity jointly, assisted by ENISA, shall consolidate the list of standards, regulations and non-certifiable standards, to add to the EPSMM.

7. ACER, assisted by ENISA, shall issue an opinion on the consolidated list of standards, regulations and non-certifiable standards, to add to the EPSMM at point 6 of this list.

8. The European Commission shall adopt the drafted EPSMM resulting from point 7 of this list, based on their compliance with the mandate for the network code and the strategic objectives of the EU.

The network code shall foresee a reasonable timeline for the implementation and certification of the principles/minimum requirements following the adoption of the list of principles at point 4 and of the EPSMM at point 8. In particular, the network code shall ensure that its implementation is given priority, and that the certification of the principles and of the requirements that may derive from the standards, is established 24 months after the implementation, as this is the average time line for a cybersecurity certification framework to be implemented in medium enterprises.

The network code shall acknowledge (by reducing the requirement of certification) all those entities that already possess a certification listed in the EPSMM, can prove that they are already implementing the cybersecurity principles without the need for any further obligation.

The network code shall foresee **temporary derogations from the requirement of certification** when:

A. The cost of the certification may exceed the benefits from the implementation of the cybersecurity principles at point 4, and when the requirement of a certification may generate risks that would result from the late implementation of the cybersecurity principles resulting from point 4.
B. A cybersecurity plan already exists in the concerned electricity undertaking, and the cybersecurity plan covers at least 80% of the principles in the list at point 4. This shall verified and certified by an accredited third party.
C. A legal obligation from the Member State conflicts with the need of certification.

The list of the temporary derogations resulting from the verification of conditions at point 1, 2 and 3, shall be added to the “Cross-Border Electricity Cybersecurity Risk Assessment Report” as an annex, and kept regularly updated jointly by ENTSO-E and the EU-DSO Entity.

4.2 Advanced requirements: Supply Chain Security and cybersecurity certification of components

The network code shall encourage the essential electricity undertakings, among all risk assessment and risk management tasks, to manage cybersecurity risks concerning their supply chain. It therefore shall define specific requirements for the supply chain security to ensure that the asset owners, and/or those who operate the assets on behalf of the owners, can control the whole asset supply chain from the design of the product/system along the entire process to install, configure and operate/maintain the system.

The network code shall suggest a “zero trust[18]” approach to the supply chain when it impacts critical infrastructures and critical cross border electricity flows. As recent threats have clearly

[18] A security model that assumes everything (processes, information, actions, and actors) can be potentially hostile, therefore, shall be questioned and properly checked.

shown that the risk may emerge from any aspect of the supply chain, the control on the supply chain shall focus on the following points:

i) The risk assessment at chapter 3 shall also take into consideration a severe and unexpected corruption of the supply chain, the unavailability of products/systems/services from the supply chain and the possibility that an attack may be initiated by an actor that takes part in the supply chain. Those risks shall lead to set clear rules for the acquisition of system and services, and the diversification of the supply sources, where possible.
ii) Selection of systems with security by design, and security embedded in all the processes during system design and production phase. Secure processes for design and production of systems shall provide assurance of traceability of security operations in each phase of the lifecycle and until the delivery of the system to the production.
iii) Careful selection of essential vendors and essential service providers that apply security rules to the delivery of their systems and products and that can clearly show their capability to fulfil the same security requirements as the electricity undertaking. The selection of essential vendors and service providers shall also ensure that the commercial relationships are based on mutual trust, but that the electricity undertaking will always have control over the systems and services provided. This will contribute to the harmonisation of the sector, also in the case of outsourcing of systems and services.
iv) Concerning products and systems, in the absence of specific European Cybersecurity Certification schemes that may cover the systems in use in the context of cross-border electricity flows, the electricity undertakings may rely on National schemes, especially if such schemes provide the possibility to be certified by an accredited third party. This shall be considered under the condition that all essential producers/vendors/service providers have equal access to both the schemes and the certification capabilities, without negative impact on the acquisition of more secure electricity systems. The network code shall promote the use of cybersecurity certification under the existing and under the European Cybersecurity Certification schemes, providing a fast track to those products/services/systems that have been certified, and therefore, can assure a certain level of security of the supply chain. The network code shall anyway foresee a transitional phase that, starting from international standards and/or National Schemes, will converge in the European Cybersecurity Certification schemes, once suitable schemes will be available.

All the above points can be implemented by setting up clear procurement templates and procurement protocols in line with relevant procurement rules. To promote proper control of the supply chain at an early stage, such rules shall include tools (e.g. mapping tables for which ENISA may be consulted) based on international standards and national schemes applicable for the transitional certification. Templates and protocols for procurement may be also used to assess if existing contracts are in line with the need to further enhance the control of the supply chain underlying cross-border electricity flows.

The use of EU Cybersecurity Certification Schemes may be voluntary if the scarcity of the schemes could impact the harmonised and secure growth of cross-border electricity flows, but efforts should be made to make EU Cybersecurity Certification Schemes mandatory at the latest by 2027. In the context of the EU Cybersecurity Certification Framework, it could be elaborated a standard to facilitate technical requirements of conformity evaluation, that may further support the implementation cybersecurity network code, containing more detailed steps than into the code.

To prevent that an inappropriate exchange of information concerning critical assets/systems/processes may constitute a risk for the entire electricity system, the network code shall, to the extent possible, set clear rules to require confidentiality and traceability of information exchanges between the electricity undertakings and all actors in the supply chain. The rules to

require confidentiality and traceability of information exchanges between the electricity undertakings shall be applicable also to the communication related to risks between SOCs and CSIRTs of the electricity undertakings. The network code may consider appropriate penalties for the infringement that, in case of an excess of disclosure of information related to the cybersecurity of cross-border electricity flows, shall be proportionate with the generated level of risk for the grid.

The network code may impose rules for the roll out of new systems that may be classified as critical systems for cross-border electricity flows or for the systems that take part to the execution of any critical process in the scope of cross border electricity flows. In absence of a certification, the roll-out of such new systems shall be subject to a penetration testing session, whose aim is identifying the conditions under which the system (a single device or the entire branch of the system of which it will be part of) may become unstable or unusable due to specific cybersecurity and non-cybersecurity conditions or due to known or emerging vulnerabilities.

Finally, the following additional measures may be considered in order to further secure the supply chain for cross-border electricity flows:

i) The network code may establish rules for the integration of cybersecurity requirements into tender specifications, setting clear obligations to allow the selection of only those products that comply with current security principles at point 7 and point 8 of Table 2.
   - The use of cybersecurity requirements in Request for Information, Requests for Proposals and their further agreements;
   - The use of supplier due diligence;
   - The reliance on cybersecurity certified systems and on vendors that have followed a specific clearance process.

ii) The network code may consider obligations for full lifetime support with regular security updates to critical assets and systems.

iii) The network code may set provisions to impede or limit attempts of supply chain tracking and supply chain infiltration both in the systems development and in the systems operations.

iv) The network code shall promote the secure termination or transition of contracts having relevance for the development and operations of critical assets, especially in case of severe cybersecurity incidents having an impact on cross-border electricity flows, for which the negligence of an essential service supplier/provider/ vendor can be demonstrated by the lack of application of known security rules and by international standards.

4.3 Cybersecurity inspections

The network code shall ensure that the measures applied for supervision or enforcement imposed on essential electricity undertaking and important electricity undertaking are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

The network code shall ensure that National Competent Authorities for Cybersecurity and/or National Regulatory Authorities, where exercising their supervisory tasks, have the power to subject important and essential electricity undertakings to:

a) on-site individual and coordinated multi-site joint inspections and off-site supervision, including random checks, especially following a cybersecurity incident, or when the network of CSIRTs will signal, through the Early Warning System, an imminent risk related to cybersecurity of critical systems, processes, operations that take part to the cross border electricity flows
b) random security audits aimed to verify the conformity on risk assessments and of their results;
c) requests of information necessary to assess the cybersecurity measures adopted by an electricity undertaking, including documented cybersecurity policies, as well as compliance with minimum or advanced standards.

For joint and coordinated inspection at point (b), that may involve also cross-border incidents, the network code may foresee the involvement of ACER, and the possibility to consult ENISA.

A summary and the results of the inspections shall be consolidated in an “Electricity Cybersecurity Risk Assessment Report”.

5 Essential information flows, Incident and Crisis Management

5.1 Data Collection, Sanitisation and Dissemination

The network code shall establish an information collection and sharing system to further support all the electricity undertakings in the EU with key security-related information for operations of cross border electricity flows, such as near real-time reporting of cybersecurity incidents, early warnings related to cybersecurity matters and undisclosed vulnerabilities on equipment in use in the electricity system.

The information collection and sharing system for the cross-border electricity flows shall foresee data collection from all electricity undertakings included in Table 1, sanitisation and anonymisation of information and the prompt dissemination within 20 hours to all relevant essential and important electricity undertakings. Proper sanitisation and anonymisation is especially important in case of information that may allow to identify an electricity undertaking and may impact reputation of anyone part of the information sharing system. The information sharing system shall play a key role in effective and timely sharing of security-related information between electricity undertakings, thus enhancing protection from current threats and risks, and allowing them to proactively act on imminent risks. The system to be established through the network code shall complement the information gathering and dissemination flows of the existing CSIRTs Network[19] established through Article 12 of the NIS Directive.

The network code shall require all electricity undertakings to actively participate and contribute to the information collection and sharing network. To ensure they benefit from such participation, electricity undertakings shall establish a SOC or access SOC services through an MSSP.

A main objective of requiring SOC activities is to make electricity undertakings capable to detecting malicious activities to alert other electricity undertakings, and to be able to react when alerted to malicious activities of other electricity undertakings with minimal delay and with the appropriate combination of cybersecurity and operational skills. The activities of electricity undertaking SOCs and MSSPs shall include at least the following:

i) Monitoring and management of cybersecurity devices and general systems within the electricity undertaking.
ii) Intrusion detection, vulnerability scanning and general cyber hygiene within the electricity undertaking.
iii) Participating in a European information-sharing program through national SOC networks established by the network code, including sharing of data about important attacks and vulnerabilities discovered.
iv) Analysing and if needed reacting properly to data received through the information sharing program established by the network code.
v) General cybersecurity incident response and participation in crisis management within the electricity undertaking.

SOC activities and services may be shared by more electricity undertakings as this will increase efficiency and may provide a viable way to slowly contribute to the creation of additional capacity

[19] The CSIRTs Network, under the NIS Directive, is a network composed of EU Member States' appointed CSIRTs. ENISA has the role of secretariat and actively supports incident coordination upon request. Appointed CSIRTs are responsible for data collection, sanitisation and dissemination at Member State level, with a focus on Operators of Essential Services. Further information available at https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network

in terms of human resources and skills. Furthermore, it shall be considered that the terms SOC, MSSP and CSIRT may be used interchangeably or combined in different ways by electricity undertakings. The network code shall allow electricity undertakings to choose how to organise their SOCs or MSSPs and what terms to use, provided they meet the functional requirements of the network code.

Built on the CSIRT Network already established through the NIS directive, the network code shall establish national information sharing networks following the mesh topology as illustrated in Figure 1. The national information sharing mesh networks shall be composed of SOCs and MSSPs of electricity undertakings, national CSIRTs and national Energy Sector CSIRT (where present) or similar. The national CSIRTs and Energy Sector CISRTs of the states that have them, shall also be connected in a similar EU mesh, as illustrated in Figure 1. The organisation in mesh topology ensures rapid exchange of information within networks, first at national level, and when information is sanitised and cleared by a national CSIRT, fast sharing at EU level.

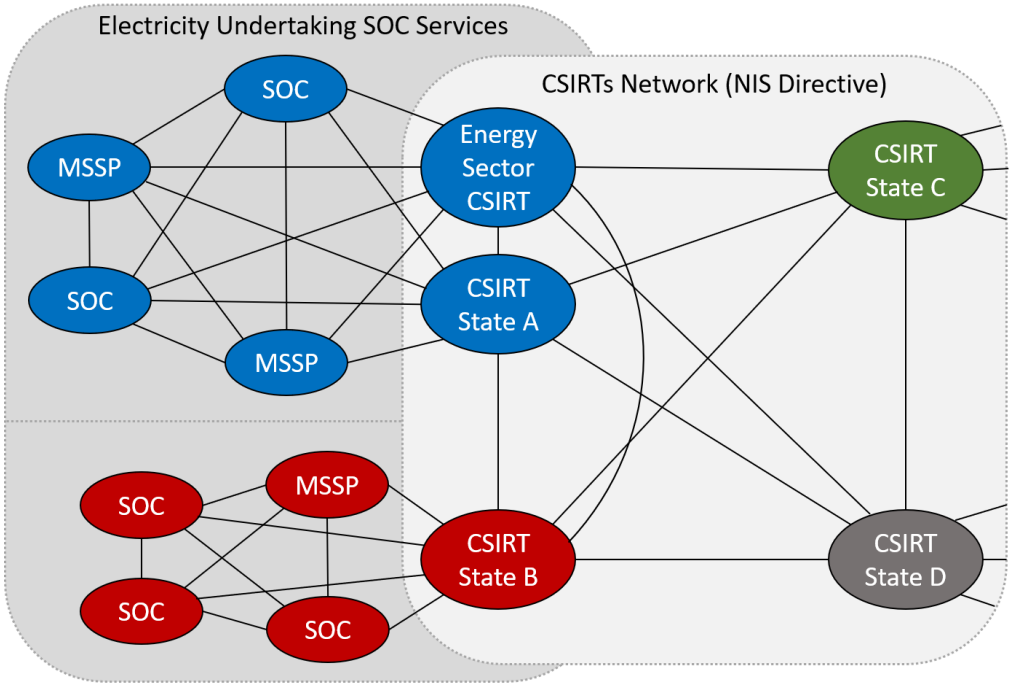

Figure 1: Illustration of the information sharing meshed relationships between the electricity undertaking SOCs or MSSPs and the CSIRTs Network as of the NIS Directive.

As illustrated in Figure 2, an important role of electricity undertaking SOCs or MSSPs shall be to ensure detection capabilities. When a vulnerability or incident is detected, electricity undertakings shall have routines for how related information shall be shared within their national mesh networks. Data may be shared directly between the electricity undertakings in the state, or through a CSIRT at national level for anonymity or sanitisation reasons.

A CSIRT on national level shall be the main responsible for data collection, sanitisation and dissemination internationally. During data sanitisation, the CSIRT on national level shall ensure that data has been properly anonymised, and that sharing information does not conflict with national legal requirements. The competent CSIRT may be appointed by each Member State. In most cases it would be expected that this will be either the national CSIRT established in compliance with the NIS Directive, or a dedicated Energy CSIRT who will receive this role.

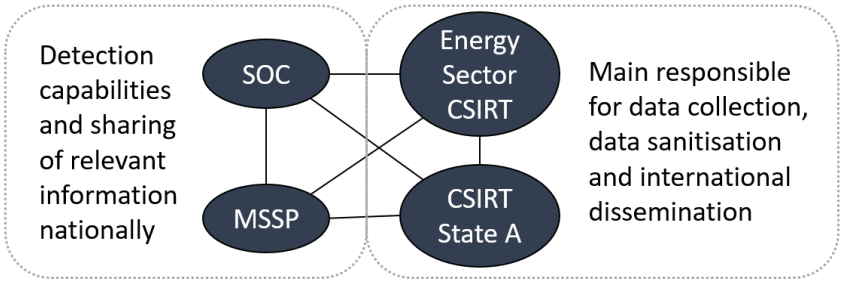

Figure 2: Main roles of electricity undertaking SOCs or MSSPs and CSIRT(s) on national mesh network level.

The network code shall ensure frequent use of a suitable and highly trustable environment to exchange security information between electricity undertakings in EU Member States. This environment should provide electricity undertakings with the needed confidence to share incident related information with each other. Electricity undertaking SOCs or MSSPs shall have one single point of contact for the purpose of information sharing. Contact points shall not be person-dependent but could e.g. consist of functional email-address (with a backup email address) and a phone number. Communication on national and international information sharing mesh networks shall be encrypted, otherwise protected using best practice techniques and standards.

Figure 3 illustrates an example of data dissemination routes in the national and international mesh networks when a reportable incident has occurred. In the example, the national CSIRT has been given the responsibility of sharing information internationally from the electricity undertaking SOCs and MSSPs. The network code shall also allow different settings, e.g. a national Energy Sector CSIRT may be in charge of the international dissemination of data. Such a solution may be beneficial for sharing speed, as national CSIRTs are cross-sectorial and may be delayed in disseminating national information to different sectors before the focus shifts to international dissemination.

Once the information has been sanitised on a national level and approved to be shared at international level, the information shall immediately be made available to the SOCs or MSSPs of all other electricity undertakings across EU that can and wish to receive such information directly. This means that international information sharing may not follow the meshed routes used for data collection when information is disseminated. Instead, the information may be disseminated directly. This information sharing shortcut is illustrated in Figure 3. The example in Figure 3 also illustrates that a Micro SOC is still receiving information over the national mesh net. An advantage of that possibility is that a national CSIRT on the side of the receiving electricity undertaking SOCs or MSSPs may then first analyse the data. This should work as a support for SOCs or MSSPs with less analytic capabilities. The network code shall be open for Member States and their electricity undertaking SOCs or MSSPs to choose for themselves whether they want their SOCs or MSSPs to receive information either directly from a CSIRT in the state the information originated, from a CSIRT in their own state, or from both the two previous.

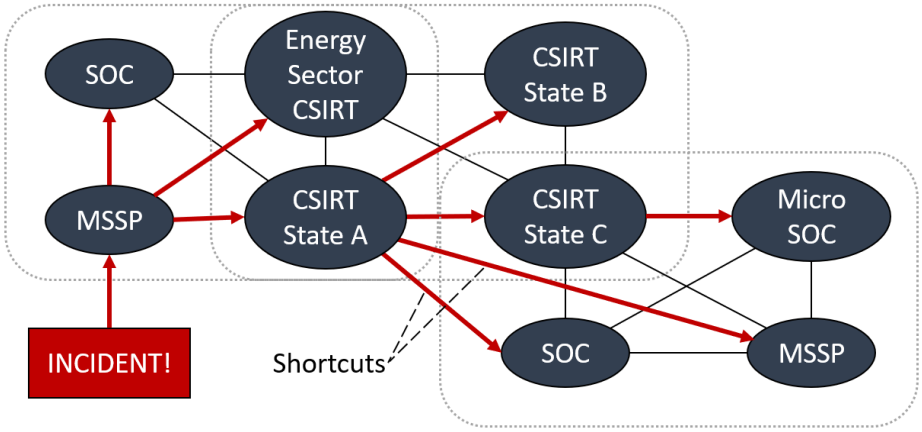

Figure 3: Example of data dissemination routes in the information sharing mesh network when a reportable incident has occurred. The paths are illustrated with red arrows.

All electricity undertakings shall report the following information within the national mesh:

i) Detected cyber-attacks, cyber threats and near misses.
ii) Vulnerabilities and attacks connected to third parties with which they have any commercial or working related relationship or suppliers and their services.
iii) When identified, Indicators of Compromise (IoCs): e.g. virus signatures, compromised URL and IP addresses, hashes of malware files, etc.
iv) Other information of importance for preventing, detecting, responding to or mitigating cybersecurity incidents.

All electricity undertakings shall share information without undue delay, and routines shall ensure that electricity undertakings issue an initial notification to the national CSIRT within the following timelines:

- Two hours after the determination of a Reportable Cyber Security Incident.

All CSIRTs on a national level shall be required to share information without undue delay, and initial notification shall be given within the following timelines:

- 18 hours after the determination of a Reportable Cyber Security Incident.
- Further delay than 12 hours must be justified by the national CSIRT.

ENISA shall provide electricity undertakings with guidance on establishing SOC capabilities or engaging with MSSPs. ENISA shall also keep up to date an illustration of the information sharing network by mapping different information sharing initiatives and their connections. This may be done by extending the CSIRTs Network inventory that ENISA are maintaining today.[20]

Regional Coordination Centres, ENTSO-E and the EU-DSO Entity, shall be treated as any other electricity undertakings, but their access point to the European CSIRT Network shall be through a central entity, that may be CERT-EU of which they shall become constituents.

The network code shall promote cost efficiency. One example is that the network code shall allow two or more Member States to have a shared Energy Sector CSIRT.

[20] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory

CERT-EU, may, with support from ENISA, keep a track record of events such as incidents, crises and vulnerabilities that have been reported in the international information sharing network.

5.2 Incident Detection and Handling

The network code shall establish effective processes to identify, classify and respond to cross border Cybersecurity Incidents that will or may affect cross-border electricity flows. The processes shall aim to minimise the impact of a cyber-incident or attack and to react quickly to restore the cross--border electricity flows. The network code shall focus particularly on the management of cyber-attacks or incidents that:

i) may reoccur in different cybersecurity electricity regions, multiplying the effects of cross-border electricity flows;
ii) may, through cyber means, generate a general instability that may have a potential impact on the electricity flows (e.g., in operational aspects such as frequency, voltage, balancing);
iii) involve legacy systems in which attacks on equipment cannot be mitigated in a normal fashion or in a reasonable time and at a justifiable cost.

Electricity undertakings shall have the necessary capabilities to detect cyber incidents and manage such incidents with the necessary support from national, regional and EU wide resources.

The electricity undertaking SOCs or MSSPs shall have the means and capabilities to detect incidents under the supervision of the National CSIRT or following a formal delegation from the CSIRT when specific conditions request a prompt reaction and put the SOC in a better position to respond to an escalation that may result from an incident/attack. The conditions for enacting the temporary delegation of powers shall be clearly identified by the National CSIRT in cooperation with the CS-NCAs, and the NRAs.

The network code shall establish a system in which, in the event of major incidents, personnel from affected electricity undertaking SOCs or MSSPs are dispatched to join and cooperate in an ad hoc CSIRT. Rules shall be defined on how to appoint the entity which shall run the ad hoc CSIRT. This function of the ad hoc CSIRT shall be exercised periodically to ensure its efficiency in the case of major incidents.

The network code shall:

i) Ensure the SOCs and MSSPs have access to information at a level equivalent to that of all other members of the CSIRT network.
ii) Describe how incidents shall be classified based on an incident classification scale[21] established prior to reporting to the national information sharing network or just a national CSIRT.
iii) Provide a frequency for how often incident response plans shall be executed (e.g., at least every year).
iv) Provide criteria to determine if an identified cybersecurity Incident is a **Reportable Cyber Security Incident**.[22]

[21] One example on an established incident classification scale is: https://eepublicdownloads.entsoe.eu/clean-documents/SOC%20documents/Incident_Classification_Scale/2014_ICS_Methodology.pdf

[22] Criteria may be based upon the definition of a Reportable Cyber Security Incident from the NERC Implementation Guidance for the CIP-008-6 Standard: A Cyber Security Incident that compromised or disrupted i) A Bulk Energy System Cyber System that performs one or more reliability tasks of a functional

v) Require electricity undertakings to establish incident management procedures for cybersecurity incidents, including roles and responsibilities, standardising tasks and reactions based on the observable evolution of the incident within the undertaking and in the nearby cybersecurity perimeters.
vi) Provide specific requirements to handle incidents with potential cross-border effects, based on the principle of proximity to the incident.

Cross border cybersecurity incidents shall be dealt in accordance with the principle of proximity, which implies that an incident shall be handled as closely as possible, both geographically and organisationally. Examples of involvement in incident management are provided in Figure 4. Incident X illustrates a smaller incident that is handled locally by an electricity undertaking and its MSSP without the involvement of any other entities on the network.

Incident Y illustrates a larger incident impacting two electricity undertakings. Here, the national CSIRT is involved to support the SOCs of the affected undertakings. In this case the incident shall be handled by an ad hoc CSIRT made up of personnel from the affected electricity undertakings and with support from the national CSIRT.

Incident Z illustrates an incident with cross-border effects, in which an electricity undertaking in state A and one or more undertaking(s) in state C are affected. As in the case of incident Y, the affected undertakings will establish an ad hoc CSIRT. The ad hoc CSIRT shall, upon request, be supported by national CSIRTs from all affected Member States. In cases of cross-border incidents, the ad hoc CSIRT shall keep the relevant Regional Coordination Centre updated with summaries of the situation on a regular basis. The CSIRTs network shall be informed of ongoing developments and changes at regular intervals. Ad hoc CSIRTs dealing with cross-border incidents should also be able to count on the support of ENISA and other EU resources.

The Regional Coordination Centres, ENTSO-E and the EU-DSO Entity, shall handle incidents at their respective level (EU Level). In cases of larger incidents, and under the condition that they will become members of the CERT-EU, they will be able to receive support through the CERT EU.

The network code shall take into account the reporting guidelines developed by the NIS coordination group pursuant to Article 14(3) of the NIS Directive, including the circumstances for reporting incidents and the format and procedure for such reporting. The CSIRTs Network shall be consulted when defining criteria to define Reportable Cyber Security Incidents.

ENTSO-E and the EU-DSO Entity will report large-scale incidents[23] arising from cyber-attacks to Europol's European Cybercrime Centre as soon as there is a reasonable certainty that the disruption is the result of a cyber-attack. The network code shall define a threshold for incidents to be defined as large.

entity, ii) An Electronic Security Perimeter of a high or medium impact Bulk Energy System Cyber System, or iii) An Electronic Access Control or Monitoring System of a high or medium impact Bulk Energy System Cyber System.

[23] We apply the NIS Directive's definition of a large-scale incident: An incident with a significant impact on at least two Member States or whose disruption exceeds a Member State's capacity to respond to it. Depending on their cause and impact, large-scale incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market.

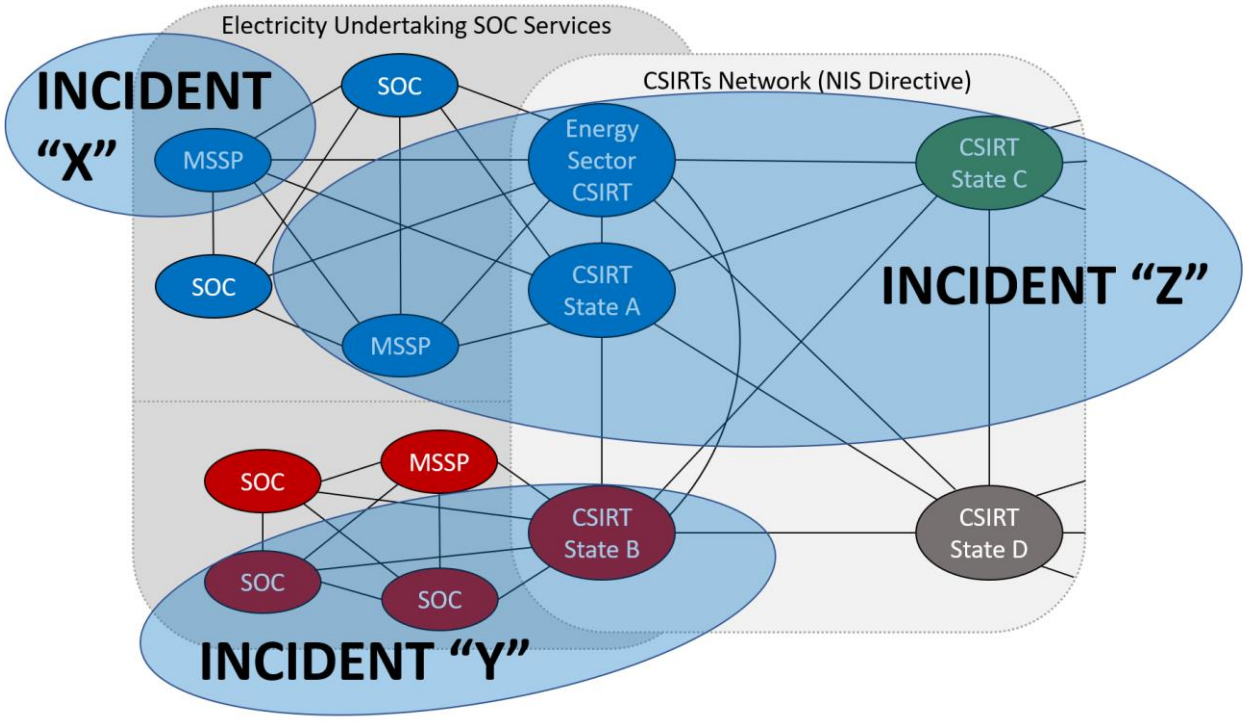

Figure 4: Examples of involvement of response environments for incident handling on electricity undertaking (X), national (Y) and regional (Z) level. Involvement shall follow the principle of proximity.

5.3 Crisis Management[24]

The Crisis Management processes shall build on the Incident Handling processes described in chapter 5.2. A combination of incidents may lead to a crisis and in such cases, the principle of geographic and organisational proximity shall still be respected. This means that if, for example, an Ad Hoc CSIRT has been established to handle an incident as described in Chapter 5.2, and that incident leads to a crisis, the Ad Hoc CSIRT shall simply be expanded as needed and combined with one or more crisis management team(s) in charge of crisis management.

Electricity undertakings shall have the necessary crisis management capabilities to manage crises, depending on the nature of the crisis, with the necessary support from national, regional and European resources.

The network code shall support the functioning of the European Union society and economy in a crisis by increasing the capability of electricity undertakings to handle crisis situations caused by cyber incidents. This includes the ability of electricity undertakings to keep business processes running during a crisis.

Additional rules shall be established in the network code on how the cross-border cybersecurity crisis shall be managed in a joint effort between affected electricity undertakings, National Energy CERTs, National Regulatory Authorities, National Competent Authorities for Cybersecurity and/or Risk Preparedness, National CSIRTs and Regional Coordination Centre(s).

The network code shall include general requirements on crisis management, including:

[24] With crisis is meant a cybersecurity related incident with potential of generating a cascading effect that would make it impossible to supply electricity to customers

i) Testing and exercise routines for the electricity undertakings Crisis Management, Business Continuity and Recovery Plans.
ii) How electricity undertakings shall analyse and share lessons learned after managing a crisis.
iii) An obligation to take part in the Crisis Management System CyCLONe.[25]

The network code shall define specific requirements related to:

i) Minimum content of Crisis Management Plans for electricity undertakings, including:
   - Metrics to define a crisis, including metrics to activate cross-border crisis management plans.
   - Roles and responsibilities for crisis management within the electricity undertakings and the CSIRT Network.
   - Rules for communication and information sharing during a crisis situation.
   - The Crisis Management Plan shall also specify the rules for the use of the metrics defined above.

ii) Minimum content of Business Continuity Plans for electricity undertakings, including:
   - Cyber business continuity processes.
   - Business continuity locations including hardware and software.
   - Roles and responsibilities connected to Business Continuity Processes.

iii) Minimum content of Recovery Plans for electricity undertakings, including:
   - Processes for the backup and storage of information required to recover Cyber System functionality of electricity undertakings.
   - Processes to complete a full cyber recovery.

Finally, the network code shall also take into account the following:

- The network code shall give ENISA the task to provide expert help and advice for electricity undertakings on crisis management, with special attention for ICS/SCADA cybersecurity events.
- The network code shall complement existing rules in the Risk Preparedness Regulation. In particular, the declaration of an electricity cybersecurity crisis shall follow the methodology for declaring an electricity crisis described in Point 2 and 3 of Article 14 of the Risk Preparedness Regulation.
- Crisis situations with cross border effects and stemming from cyber-attacks, shall be reported to Europol following the same method as described in chapter 5.2.
- If the crisis entails an important EU external or an EU Common Security and Defence Policy dimension, the European External Action Service shall be promptly informed, enabling them to activate their Crisis Response Mechanism.

[25] The Cyber Crises Liaison Organisation Network (CyCLONe) was established in 2020 to support the implementation of rapid emergency response during larger cross-border cyber incidents or crisis. CyCLONe links cooperation at technical (e.g. CSIRTs) and political levels (e.g. Integrated Political Crisis Response), thus enabling consultations on national response strategies and coordinated impact assessment on the anticipated or observed impacts of a crisis, both at national and EU level.

5.4 Electricity Cybersecurity Early Warning System (ECEWS)

An early warning system[26] can be described as a solution for threat information gathering, processing and notification of threat information. It is about systematically providing the right information to the right people at the right time – connecting the dots across relevant actors.[27] The network code shall establish an early warning system specific for cybersecurity events, which shall identify conditions and indicators that frequently correlate with larger cyber-attacks within the electricity sector or, in general, within the energy sector. By identifying such conditions and indicators, the ECEWS shall advise EU CSIRT and SOC networks on early preventive actions before incidents materialise and/or lead to cross-border effects. The ECEWS shall be jointly operated by ENISA and CERT-EU.

The ECEWS shall focus on innovation in methodologies and follow trends in digital development. The ECEWS shall cooperate closely with relevant working groups and research communities, especially the Electricity Coordination Group and EU Cybersecurity Competence Centre.

The ECEWS process may follow four main steps:

1. Global scan of cyber risk conditions and relevant indicators for the electricity sector.
2. Identification of risk factors and indicators that do require further EU analysis and preventive actions.
3. Analysis that combine the relevant data available and investigate the potential risk, as well as effectiveness of possible preventive actions.
4. Notification to EU electricity undertakings through the CSIRT Network about the identified risks and recommended preventive actions.

The steps shall be repeated as illustrated in Figure 5.

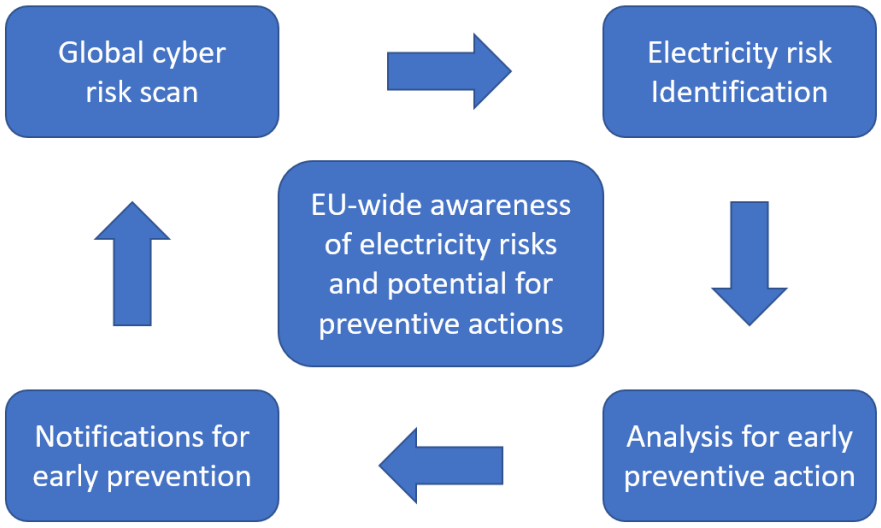

Figure 5: Illustration of steps of a ECEWS for the EU Energy Sector.

[26] Smart Grid Task Force Expert Group 2 - Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management. Final Report June 2019, p. 75.

[27] Factsheet - EU Conflict Early Warning System: https://eeas.europa.eu/archives/docs/cfsp/conflict_prevention/docs/201409_factsheet_conflict_earth_warning_en.pdf

The global scan of cyber risk factors and indicators should include information shared through the EU CSIRT Network.

ENTSO-E and the EU-DSO Entity shall monitor the effectiveness of ECEWS. The European Commission, ACER, NCAs, NRAs and national CSIRTs shall be regularly informed. A report on the effectiveness of ECEWS will be sent annually to the European Commission and ACER. ACER, advised by ENISA and after consulting the CS-NCAs, NRAs, SOCs and CSIRTs, if deemed necessary, will issue an opinion on the report on the effectiveness of the ECEWS.

6 Electricity cybersecurity exercise framework

The network code shall require the establishment of a multi-year programme of electricity cybersecurity exercises. The programme shall affect different levels of the electricity system each year, with the aim of providing all actors involved with the possibility of becoming familiar with these exercises and to contributing to the improvement of the programme and to the preparedness of the entire sector. While cybersecurity exercises are time-consuming, they offer the possibility to gather lessons learned at any level of the electricity value chain, through a simulated event and in a simulated environment/situation.

In the context of cybersecurity exercises, the network code shall include the provision to plan and execute the following activities:

1. A mandatory internal cybersecurity exercise for all essential electricity undertakings, simulating a situation that will impact cross-border electricity flows, at least every two years after entering into force the network code.

2. For each member state, national cybersecurity exercise of all national essential electricity undertakings of the considered member state, in substitution of point 1.

3. A mandatory regional or cross regional cybersecurity exercise: such exercise shall be organised by one or more Regional Coordination Centres and shall involve all essential electricity undertakings within the cooperating under the same RCC. The cybersecurity exercise shall take place at least every three years after entering into force the network code.

4. Exercises at point 1, 2 and 3, shall include and alternate, to the extent possible, Table Top Cybersecurity Exercises, Red/Blue team exercises and exercises focused on hybrid threats.

Even though the cybersecurity exercises are not compulsory for all electricity undertakings, all electricity undertakings should be encouraged to organise their own cybersecurity exercises or to take part in the exercises at point 2 and 3.

The network code shall allow the possibility to remunerate costs that may arise from exercises at point 1 and 2. ENTSO-E and the EU-DSO Entity, with the support of ACER and ENISA, shall prepare on a yearly basis an exercise template for exercises at point 1 and 2, based on major risks that would emerge in the risk assessment exercise. The NRAs, with the support of the respective CS-NCA, shall supervise, when a supervisory role is attributed at national level, the execution of cybersecurity exercises at point 1 and 2.

ENTSO-E and the EU-DSO Entity, supported by ACER, ENISA and by the Joint Research Centre of the European Commission, shall prepare every three years an exercise scenario for the exercises in point 3, based on the indication of the European Commission – Directorate for Energy.

Finally, the network code may lay the foundation for the creation of a shared and distributed electricity cybersecurity simulation testbed to give access to a realistic setup for the cybersecurity exercises. The testbed may be used to better understand, ex-post, the underlying dynamics of cyber incidents and attacks, as well as to assess the actual consequences of specific incidents or attacks on cross-border electricity flows. In this respect, the network code may request all electricity undertakings to contribute to the creation of the electricity cybersecurity testbed by sharing the costs in a proportionate manner.

7 Protection of information exchanged in the context of this data processing

All information exchanged among all stakeholders for the implementation of the network code, shall be protected, considering the level of classification of the information applied to the information by the stakeholder who is the originator. The classification system shall consider the risk of loss, modification, or alteration of essential information to allow cross-border electricity flows.

The protection of information exchanged in the context of this network code shall follow the following principles:

1. Each electricity undertaking, when dealing with information internally and when transferring information related, shall assure that all information is properly classified and protected, and classification and ownership are correctly indicated.
2. Each stakeholder shall refuse any information without classification or ownership and shall inform NRAs/CS-NCAs and ACER in case of any breach of information protection rules.
3. Each originator of information shall set the level of classification and ownership in compliance with rules at point (1) of the methodology. As a way of derogation, ownership can be omitted if the information is classified and the National Regulation allows this.
4. It is the responsibility of each processor to protect, respect and further disseminate the level and classification.
5. Information shall only be exchanged internally and externally as part of necessary information processing and following the “need to know” principle[28].
6. ENTSO-E and the EU-DSO Entity are responsible for defining the rules for the classification and protection of information as defined in the scope and objectives in points (1), (2) and (3), after consulting all the electricity undertakings listed in Table 1 as well as all CS-NCAs and NRAs, representing the EU member States.
7. ACER, advised by ENISA, and after receiving the opinion of the NIS Cooperation Group - WS 8[29] , is responsible for providing an opinion on the rules described in point 6 to the European Commission.
8. The NRAs and CS-NCAs are responsible vis-à-vis with the identified operators to whom the network code applies, for the monitoring compliance of the rules for protection of information, as well as defining sanctions when rules are not respected (this is, for the first level of asset management and risk assessment).

[28] The general security principle under which an information can be provided to any other actor, only if it is a stict requirement for the actorser to fulfil its current role.
[29] WS 8 is the work stream of the NIS Cooperation Group for the energy sector which consists of the national authorities which are responsible for the implementation of the NIS Directive requirements for the energy sector.

9. ACER, with the support of ENISA, is responsible vis-à-vis with the operators for the supervising compliance with the information protection regulations in the Member States and RCC.
10. Each stakeholder shall, when exchanging information, always verify that the information transferred includes information on the classification level prior initiating any processing and promptly report to the counterparty when a discrepancy may occur.
11. Each operator and Member State may classify the same information at a different level according with national legislation. When the same information is classified at a different level by different entities, the highest classification level will prevail as the applicable one, in order to safeguard the security of information against the entire information system.
12. Regarding litigation over classification, or about the refusal to process or exchange information involving entities from the same Member State, the National Competent Authorities for Cybersecurity must decide. In the case of an exchange of information that involves more than one Member State, ACER, advised by ENISA, will have to decide.

The network code shall also cover the following aspects:

i) The rules for the classification of the information exchanged and for the definition of the information ownership shall be defined in the context of the network code.
ii) The rules and methods for the secure transfer of information shall be defined in the context of the network code based on the information classification in point (i).
iii) The rules for the secure treatment of the information will be defined in the context of the network code based on the classification of the information in point (i).
iv) The classification shall foresee two levels of classification: one level of classification for sensitive information but not classified, and one level of classification for sensitive classified information.
v) The classification shall foresee the indication of the ownership of the information. When dealing with sensitive classified information, ownership may be omitted depending on national regulation.
vi) When multiple sets of information are aggregated into a single set, the applicable level of classification is equal to the highest level of information classification among the original sets.
vii) Excluding classified information sets, when multiple sets of information are aggregated into a single set, the property of the resulting information set is equal to the list of all owners of the original sets.

13. Rules in point (i), (ii), (iii) are applicable to all information in the scope of processes described in the network code, without the possibility to obtain any derogation.

8 Monitoring, benchmarking and reporting

8.1 Monitoring

The monitoring shall assess if the network code actively contributes to the strategic objectives set in the "Joint Communication to the European Parliament and the Council - The EU's Cybersecurity Strategy for the Digital Decade[30]".

The main objectives of the monitoring activities shall be, in particular:

- regularly verify the status of implementation of the applicable cybersecurity standards, in regard to the electricity undertakings listed in Table 1, prioritising the monitoring on the essential electricity undertakings and later on important electricity undertakings;
- assess the compliance with the respective cybersecurity rules/measures and the maturity of the overall electricity sector;
- verify whether the size cap (at chapter 1.3) does not directly or indirectly cause a systemic cybersecurity risk for cross-border electricity flows and whether it is necessary to introduce additional measures in this respect to prevent risks for the electricity sector.

Monitoring activities shall be able to determine and offer performance indicators that allow assessing operational reliability that can be related to cybersecurity matters. Monitoring activities shall also help identifying areas of improvement for the revisions of the network code, or to determine uncovered areas and new priorities that may emerge due to technological advances.

ACER, in cooperation with ENTSO-E and the EU-DSO Entity, advised by ENISA, shall agree on the information to collect for the purpose of the regular (at least biannually) monitoring of the network code, the methodology and the rules to collect such information.

The process to collect information shall minimise the efforts for all involved stakeholders and avoid double reporting by the concerned electricity undertakings and by their associations. ACER, ENTSO-E and the EU-DSO Entity shall agree on a reasonable time frame to update such information and on common standardised ways of analysing the information. The network code shall allow access to such information also to National Regulatory Authorities and to National Competent Authorities for Cybersecurity.

8.2 Benchmarking

The benchmarking shall assess whether current investments in cybersecurity to protect cross-border electricity flows provide the desired results and do not generate adverse effects on the development of the electricity systems. In addition, it shall assess whether such investments are efficient and integrated into the overall procurement of assets and services. The main objectives of the benchmarking activities in the context of the network code shall verify:

i) the average expenditure in cybersecurity for the protection of electricity cross-border flows, especially in respect to the essential electricity undertakings and to the important electricity undertakings;
ii) the average expenditure in cybersecurity hygiene for all the electricity undertakings which are not important or essential electricity undertakings;

[30] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=JOIN:2020:18:FIN

iii) the average prices of cybersecurity services, systems and products that mainly contribute to the enhancement and maintenance of the cybersecurity posture in the different cybersecurity electricity regions; it will allow to analyse the existence of similar costs associated with cybersecurity as well as to identify possible measures needed to foster efficiency in spending, particularly on critical areas where cybersecurity technological investments may be needed;
iv) the level of efficiency of spending on cybersecurity and observe the correlation between the level of spending and the maturity of the sector (prudence of cybersecurity expenditure).

8.3 Reporting

The main object of reporting shall be to consolidate knowledge and experiences in the boundaries of the network code, and analyse lessons learned and new trends in cybersecurity that may not directly be included in the network code at the time of the release, but that may need the attention of the policy makers, together with a revision of the network code. In this respect, the "Cross-Border Electricity Cybersecurity Risk Assessment Report" will be crucial for policy makers to identify past behaviours, trends and risks that may emerge, and to identify the need for improvements and changes to the current plans. The network code shall set provision for the regular (meaning, at least once every two years) publication of such a report.

The report shall be drafted by ENTSO-E and the EU-DSO Entity, with the contribution of all the stakeholders listed in Table 1. In preparing the draft, ENTSO-E and the EU-DSO Entity shall consult ENISA, ACER, NRAs and CS-NCAs who may aim to contribute.

The report shall include at least the following information:

- High level asset inventory lists putting emphasis on:
  - Legacy systems still in use and planned to be replaced;
  - Systems that implement the highest level of security;
  - Systems that contribute in operating the cross border electricity flows.
- current threats, with emphasis on emerging threats and risks for the electricity system;
- incidents for the previous period both at EU level and international level, providing a critical overview of how such incidents may have had an impact on electricity cross border flows, if replicated in the EU;
- overall status of implementation of the cybersecurity measures and the regional approaches;
- status of implementation of the critical information flows (at chapter 5);
- Identified and highlighted risks that may derive from poor supply chain management;
- any other information that may be useful to identify a partial failure of the network code or the need for a revision of the network code or any of its tools.

The report shall be subject to the rules on protection of exchange of information (see chapter 7). For this reason, the report may be released in a sanitised public version without those annexes that, for the nature of their confidentiality, may be released on "need-to-know basis". A full and confidential version shall be distributed on "need-to-know basis", only to NIS Coordination Group members, to ACER, to ENISA and to the European Commission. Before the release of the public sanitised version, the NIS Coordination Group shall provide its approval.
ENTSO-E and EU-DSO entity are responsible for the compilation and the release of the report in line with the rules defined above.

9 New systems, processes and procedures

The network code shall be elaborated in a way that is not detrimental to innovation. In particular, it shall not constitute a barrier to the access of new electricity undertakings to the electricity markets and the subsequent use of innovative solutions that contribute to the efficiency of the electricity system. As a fundamental principle, all new systems, processes and procedures shall be acquired/designed/configured/maintained embedding principles such as, but not limited to, security in-depth and security by design. Therefore, the network code shall promote the safe digitalisation of the electricity sector, discouraging and penalising any intervention that does not imply due consideration of aspects of security and cybersecurity.