CYBER-ATTACK CLASSIFICATION SCALE METHODOLOGY

Proposal of the TSOs, with the assistance of the ENTSO for Electricity, in cooperation with the EU DSO entity, for a cyber-attack classification scale methodology in accordance with Article 37 (8) of the Commission Regulation (EU) 2024/1366 of 11 March 2024 establishing a network code for cybersecurity aspects of cross-border electricity flows

Table of Contents

TSOS, WITH THE ASSISTANCE OF ENTSO FOR ELECTRICITY AND IN COOPERATION WITH THE EU DSO ENTITY, TAKING INTO ACCOUNT THE FOLLOWING:

Whereas

(1) This document sets out the methodology for identifying and classifying reportable cyber-attacks (hereafter referred to as 'Cyber-Attack Classification Scale Methodology') in accordance with Article 37 (8) of Commission Regulation (EU) 2024/1366 establishing a network code for cybersecurity aspects of cross-border electricity flows (hereinafter referred to as ‘NCCS Regulation’).

(2) The Cyber-Attack Classification Scale Methodology takes into account the general principles and goals set out in the:

a) NCCS Regulation;

b) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (hereafter referred to as ‘NIS 2 Directive’);

c) Regulation (EU) 2019/941 of the European Parliament and of Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/ (hereafter referred to as ‘Risk Preparedness Regulation’);

d) as well as Regulation (EU) 2019/943 of the European Parliament and of Council of 13 June 2024 on the internal market for electricity (recast) (hereafter referred to as the ‘Electricity Regulation’).

(3) According to Article 37(8) of the NCCS Regulation, the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity shall develop a Cyber-Attack Classification Scale Methodology by 13 June 2025.

(4) For the purpose of identifying cyber-attacks and ensuring compliance with the reporting requirements under Article 38(4) of the NCCS Regulation and in the absence of a clear definition of "malicious" under the Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (hereinafter referred to as ‘Regulation 2022/2554’), the distinction between "malicious root cause" and "not malicious root cause" is established. The distinction provides essential guidance for Entities in determining whether an incident qualifies as a ‘cyber-attack’ as defined in Article 3(14) of Regulation 2022/2554.

Furthermore, it is crucial in determining the reportability of an incident, ensuring that incidents with “not malicious root cause” are excluded from the regulatory definition of a ‘cyber-attack’. The distinction is solely intended for the purpose of affirming the interpretation of the definition of a ‘cyber-attack’ and shall not be extended outside the scope of this methodology.

SUBMIT THE FOLLOWING PROPOSAL FOR THE CYBER-ATTACK CLASSIFICATION SCALE METHODOLOGY TO ALL NCCS-NCAs

TITLE 1
General provisions

Article 1
Subject matter and scope

(1) This Cyber-Attack Classification Scale Methodology provides the rules for classifying the gravity of a cyber-attack according to five levels, the two highest levels being ‘high’ and ‘critical’.

(2) It sets out criteria for affected high-impact or critical-impact entities, to assess whether a cyber-attack at entity level is considered reportable according to Article 38(4) of the NCCS Regulation.

Article 2
Definitions

(1) For the purposes of this Cyber-attack Classification Scale Methodology, the terms and definitions in Article 3 of the NCCS Regulation, Article 6 of the NIS 2 Directive, Article 2 of the Risk Preparedness Regulation and Article 2 of the Electricity Regulation shall apply.

(2) In addition, the following definitions shall apply:

(a) ‘attacker’ means the threat actor who attempts to perform or perpetuate a cyber-attack.

(b) ‘estimation’ means the opinion of the affected entity based on internal and external information and findings gathered and available at a given time. The estimation reflects a subjective point of view of the Entity and is estimated for the sole purpose of scaling the cyber-attack and shall not be interpreted as binding or infringing any agency of any national authority or jurisdiction.

(c) ‘tactics’ means the reason for an attacker to perform an action, the goal they want to achieve in a certain stage of an attack.

(3) In this Cyber-Attack Classification Scale Methodology, unless the context clearly indicates otherwise, the singular also includes the plural and vice versa.

Article 3
Principles for cyber-attack classification

(1) This Cyber-Attack Classification Scale Methodology serves to assess the gravity of a cyber-attack according to five levels specified in Article 7 and Annex I.

(2) This Cyber-Attack Classification Scale Methodology sets out the rules for classification of the gravity of a cyber-attack in accordance with the following parameters:

a. the potential impact considering the assets and perimeters exposed pursuant to Article 5 that are determined in accordance with Article 26(4), point (c) of NCCS Regulation; and

b. the root cause estimation of the cyber-attack pursuant to Article 4; and

c. the severity of the cyber-attack pursuant to Article 6.

TITLE 2

Identification of a reportable cyber-attack

Article 4
Estimation of the root cause

(1) Entities shall provide an estimation of the root cause of the event:

- **A malicious root cause** means that the origin of the event is any human intention to deliberately cause harm or damage and it is clearly determined.
- **A not malicious root cause** means that the origin of the event is without any human intention to deliberately cause harm or damage.
- **An uncertain root cause** means that the origin is not clear or cannot yet be categorised.

(2) The event shall be considered a cyber-attack by the entity when it is estimated to have a malicious or an uncertain root cause.

(3) In case the root cause is estimated as uncertain, the entity shall continue to evaluate the root cause.

(4) In the case where a "not malicious" root cause is assessed without any doubt, the entity shall not consider the event as reportable according to article 38 (4) of the NCCS Regulation.

Article 5
Determination of the potential impact of the cyber-attack

(1) The entity shall determine the potential impact of the cyber-attack as follows:

- **Low potential impact:** Any asset affected by the cyber-attack belongs to neither high-impact nor critical-impact perimeter and cannot directly reach any assets in a high-impact or critical-impact perimeter.
- **High potential impact:**
  - (a) At least one asset affected by the cyber-attack belongs to the high-impact perimeter and none of them belongs to the critical-impact perimeter, or
  - (b) At least one asset affected can directly reach one asset belonging to the high-Impact perimeter and not the critical-impact perimeter.
- **Critical potential impact:** At least one asset affected by the cyber-attack belongs to the critical-impact perimeter or can directly reach an asset belonging to the critical-impact perimeter.

Article 6
Estimation of the severity of the cyber-attack

(1) The entity shall estimate the severity of the cyber-attack:

- A cyber-attack with **low severity** means that the attacker is trying to get access to one or more assets.
- A cyber-attack with a **high severity** means that the attacker has at least limited access to one or more assets which could lead to a critical severity;
- A cyber-attack with a **critical severity** means that more than one asset is impacted by lateral movement, or the attacker appears to be able to interrupt the process or perpetuate actions on one or multiple assets to destabilise the entity;

In order to perform this estimation, entities may use paragraph (2).

(2) The entity can evaluate the position of the attacker within the tactics for the ICS and Enterprise MITRE ATT&CK framework[1], based on the worst-case scenario and their forecast of the upcoming situation:

(1) **Low severity**: detection of an attempt to perform Reconnaissance, obtain Resource Development, gain Initial access:

(a) *the attackers are trying to gather information they can use to plan future operations, or*
(b) *the attackers are trying to establish resources they can use to support operations, or*
(c) *the attackers are trying to get into one of the perimeters of the Entity.*

(2) **High severity:** detection of an attempt to perform Execution, Persistence, Privilege escalation, Defense evasion, Credential access, Discovery:

(a) *the attackers are trying to run a malicious code or*
(b) *the attackers are trying to maintain their foothold, or*
(c) *the attackers are trying to gain higher-level permissions, or*
(d) *the attackers are trying to avoid being detected, or*
(e) *the attackers are trying to steal account names and passwords, or*
(f) *the attackers are trying to figure out the perimeter.*

(3) **Critical severity:** detection of an attempt to perform Lateral Movement, Collection, Command and control, Exfiltration, Inhibit Response Function, Impair Process Control, or Impact:

(a) *the attackers are trying to move through the perimeter, or*
(b) *the attackers are trying to gather data of interest to their goal, or*
(c) *the attackers are trying to communicate with compromised systems to control them, or*
(d) *the attackers are trying to steal data, or*
(e) *the attackers are trying to prevent safety, protection, or other functions from responding in the way they are expected, or*
(f) *the attackers are trying to interfere with control processes, or*
(g) *the attackers are trying to manipulate, interrupt, or destroy a system and data.*

[1] MITRE | ATT&CK Enterprise Tactics (https://attack.mitre.org/tactics/enterprise/)
MITRE | ATT&CK ICS Tactics (https://attack.mitre.org/tactics/ics/)

Article 7
Cyber-attack gravity classification

(1) The entity shall assess the gravity of the cyber-attack by combining:

(a) the result of the determination of the potential impact of the cyber-attack pursuant to Article 5, and

(b) the result of the estimation of the severity of the cyber-attack pursuant to Article 6.

(2) The level of gravity shall be considered as:

(a) “critical” if the potential impact is determined to “critical” and the severity is estimated as “critical”; or

(b) “high” if:

i. the potential impact is determined to “critical”, and the severity is estimated as “high”; or,

ii. the potential impact is determined to “high”, and the severity is estimated as “critical” or “high”; or

(c) “important”, “medium” and “to follow” according to the criteria set out in Annex I.

(3) Every time one of the following parameters change, the entity shall repeat the steps to assess the gravity of the cyber-attack pursuant to TITLE 2:

(a) a change in the estimation of the root cause pursuant to Article 4, or
(b) a change in the determination of the potential impact pursuant to Article 5, or
(c) a change in the estimation of the severity pursuant to Article 6.1.

TITLE 3
Final provisions

Article 8
Implementation timeline

(1) This methodology shall be implemented according to the timeline set out in the NCCS Regulation.

(2) Entities pursuant to Article 24(6) of the NCCS Regulation must use this methodology to discern whether a cyber-attack is reportable under the NCCS Regulation.

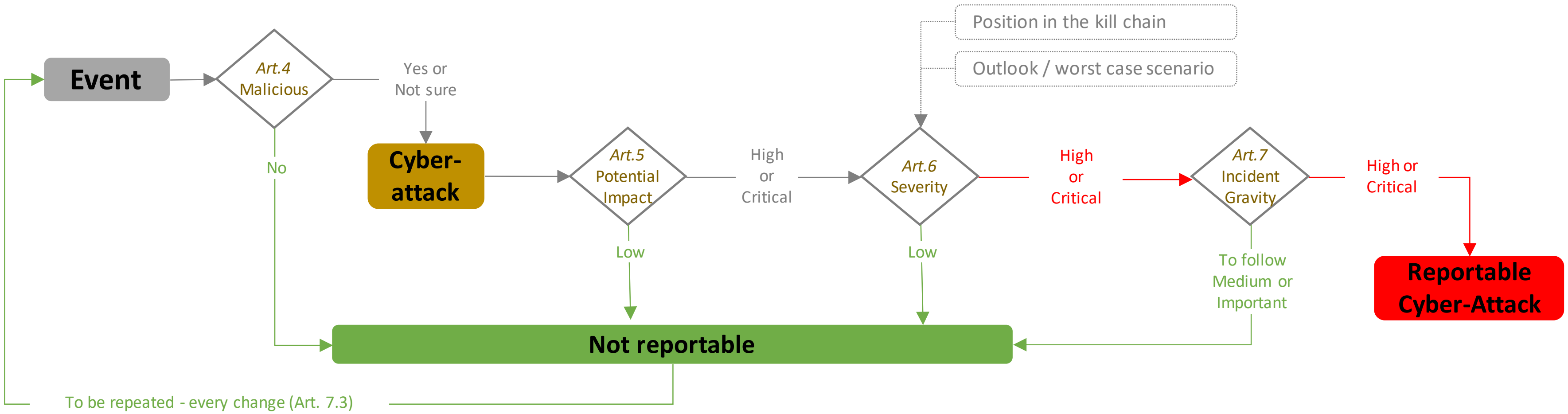
Article 9
Language

The reference language for this Cyber-attacks Classification Scale Methodology Proposal shall be English. For the avoidance of doubt, where required by relevant national competent authorities for the NCCS Regulation, the TSOs and DSOs of the relevant Member State, in cooperation, shall translate this Cyber-attacks Classification Scale Methodology Proposal into their national language(s).

In the event of inconsistencies between the English version published by TSOs, with assistance of ENTSO-E, and in cooperation with EU DSO Entity, pursuant to Article 8(9) of the NCCS Regulation and any translated version in another language, the relevant TSOs and DSOs shall, in accordance with national legislation, provide the relevant national competent authorities for the NCCS Regulation with an updated translation of the Cyber-attacks Classification Scale Methodology Proposal.

Annex I

		Potential Impact		
		Low PI	High PI	Critical PI
Severity of the Attack	Low Severity	To follow gravity	Medium gravity	Important gravity
	High Severity	Medium gravity	High gravity	High gravity
	Critical Severity	Important gravity	High gravity	Critical gravity



Tactics / Trying to
Reconnaissance Ressource Development Initial acces
Execution Persistence
Privilege escalation Defense Evasion
Credential access Discovery
Lateral Movement Collection
Command and control Exfiltration Inhibit Response Function Impair Process Control Impact

Severity of the Attack			Potential Impact		
			Low PI	High PI	Critical PI
	Low Severity	the attackers are trying to get access to one or more asset.	To follow gravity	Medium gravity	Important gravity
	High Severity	the attackers have at least limited access to one or more assets	Medium gravity	High gravity	High gravity
	Critical Severity	more than one assets are impacted by lateral movement, or [the attackers] appear to be able to interrupt the process or perpetuate actions on one or multiple assets to destabilize the entity	Important gravity	High gravity	Critical gravity