DSO ENTITY
DSOs FOR EUROPE

European Network of Transmission System Operators for Electricity
entsoe

MÉTHODOLOGIE D'ÉCHELLE DE CLASSIFICATION DES CYBER-ATTAQUES

Proposition des GRT, avec l'assistance du REGRT pour l'électricité et en coopération avec l'entité des GRD de l'UE, pour une méthodologie d'échelle de classification des cyberattaques conformément à l'article 37 (8) du règlement délégué (UE) 2024/1366 de la Commission du 11 mars 2024 complétant le règlement (UE) 2019/943 du Parlement européen et du Conseil par l'établissement d'un code de réseau sur les règles sectorielles relatives aux aspects de cybersécurité des flux transfrontaliers d'électricité.

Table des matières

TITRE 1 Dispositions générales 4
Article premier Objet et champ d'application 4
Article 2 Définitions 4
Article 3 Principes de classification des cyberattaques 5
TITRE 2 Identification d'une cyberattaque à signaler 6
Article 4 Estimation de la cause première 6
Article 5 Détermination de l'impact potentiel de la cyberattaque 6
Article 6 Estimation de la gravité de la cyberattaque 6
Article 7 Classification de la gravité des cyberattaques 8
TITRE 3 Dispositions finales 9
Article 8 Calendrier de mise en œuvre 9
Article 9 Langue 9
Annexe I 10

LES GRT, AVEC L'AIDE DU REGRT POUR L'ÉLECTRICITÉ ET EN COOPÉRATION AVEC L'ENTITÉ DES GRD DE L'UE, EN TENANT COMPTE DES ÉLÉMENTS SUIVANTS :

Considérant que

(1) Le présent document expose la méthodologie d'identification et de classification des cyberattaques devant faire l'objet d'un signalement (ci-après dénommée "méthodologie de l'échelle de classification des cyberattaques") conformément à l'article 37, paragraphe 8, du règlement délégué (UE) 2024/1366 de la Commission du 11 mars 2024 complétant le règlement (UE) 2019/943 du Parlement européen et du Conseil par l'établissement d'un code de réseau sur les règles sectorielles relatives aux aspects de cybersécurité des flux transfrontaliers d'électricité (ci-après dénommé "règlement du NCCS").

(2) La méthodologie de l'échelle de classification des cyberattaques tient compte des principes généraux et des objectifs énoncés dans la :
   a) Règlement du NCCS;
   b) Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 relative à des mesures pour un niveau commun élevé de cybersécurité dans l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (ci-après dénommée "directive NIS 2") ;
   c) Règlement (UE) 2019/941 du Parlement européen et du Conseil du 5 juin 2019 relatif à la préparation aux risques dans le secteur de l'électricité et abrogeant la directive 2005/89/CE (ci-après dénommé "règlement sur la préparation aux risques") ; et
   d) Règlement (UE) 2019/943 du Parlement européen et du Conseil du 5 juin 2019 sur le marché intérieur de l'électricité (refonte) (ci-après dénommé "règlement électricité").

(3) Conformément à l'article 37, paragraphe 8, du règlement du NCCS, les GRT, avec l'aide du REGRT pour l'électricité et en coopération avec l'entité des GRD de l'UE, élaborent une méthodologie d'échelle de classification des cyberattaques d'ici le 13 juin 2025.

Aux fins de la présente méthodologie, le terme "criticité" figurant à l'article 38, paragraphe 4, du règlement sur le NCCS est considéré comme équivalent au terme "gravité" figurant à l'article 37, paragraphe 8, du règlement sur le NCCS.

(4) Afin d'identifier les cyberattaques et d'assurer le respect des exigences de déclaration prévues à l'article 38, paragraphe 4, du règlement SOCN, et en l'absence d'une définition claire du terme "malveillant" dans le cadre du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 relatif à la résilience opérationnelle numérique du secteur financier (ci-après dénommé "règlement 2022/2554"), la distinction entre "cause première malveillante" et "cause première non malveillante" est établie. Cette distinction fournit des indications essentielles aux entités pour déterminer si un événement peut être qualifié de "cyberattaque" au sens de l'article 3, paragraphe 14, du règlement (CE) n° 2022/2554.

En outre, elle est cruciale pour déterminer si une cyberattaque doit être déclarée, en veillant à ce que les événements dont la cause première n'est pas malveillante soient exclus de la définition réglementaire

d'une "cyberattaque". Cette distinction a pour seul but d'affirmer l'interprétation de la définition d'une "cyber-attaque" et ne doit pas être étendue en dehors du champ d'application de cette méthodologie.

(5) Conformément à l'article 19 du règlement sur les NCCS, le rapport d'évaluation des risques à l'échelle de l'Union dresse une liste des processus à fort impact et des processus à impact critique à l'échelle de l'Union.

Au niveau de l'entité, cette liste à l'échelle de l'Union sert de base pour classer tous les actifs qui soutiennent les processus à fort impact et à impact critique à l'échelle de l'Union dans les périmètres à fort impact ou à impact critique, conformément aux critères définis à l'article 26, paragraphe 4, point c), du règlement relatif au système national de certification.
Cette classification est basée sur les processus à fort impact et à impact critique identifiés à l'échelle de l'Union qui pourraient potentiellement affecter les flux transfrontaliers d'électricité si l'actif est compromis conformément à l'article 26, paragraphe 4, point a) i), du règlement sur le SOCN.

SOUMETTRE LA PROPOSITION SUIVANTE CONCERNANT LA MÉTHODOLOGIE DE L'ÉCHELLE DE CLASSIFICATION DES CYBER-ATTAQUES À TOUTES LES ANC-CNCS

TITRE 1
Dispositions générales

Article premier
Objet et champ d'application

(1) La méthodologie de l'échelle de classification des cyberattaques fournit les règles permettant de classer la gravité d'une cyberattaque selon cinq niveaux, les deux niveaux les plus élevés étant "élevé" et "critique".

(2) Il définit les critères applicables aux entités touchées à fort impact ou à impact critique, identifiées conformément à l'article 24 du règlement du NCCS, pour déterminer si une cyberattaque au niveau de l'entité est considérée comme devant être déclarée conformément à l'article 38, paragraphe 4, du règlement du NCCS.

Article 2
Définitions

(1) Aux fins de la présente méthodologie de l'échelle de classification des cyberattaques, les termes et définitions de l'article 3 du règlement NCCS, de l'article 6 de la directive NIS 2, de l'article 2 du règlement relatif à la préparation aux risques et de l'article 2 du règlement relatif à l'électricité s'appliquent.

(2) En outre, les définitions suivantes s'appliquent :

(a) attaquant" : l'acteur de la menace qui tente d'exécuter ou de perpétrer une cyberattaque.

(b) estimation" : l'opinion de l'entité touchée, fondée sur des informations et des constatations internes et externes recueillies et disponibles à un moment donné. L'estimation reflète un point de vue subjectif de l'entité et est estimée dans le seul but de dimensionner la cyberattaque ; elle ne doit pas être interprétée comme liant ou enfreignant un organisme d'une autorité ou d'une juridiction nationale.

(c) Le terme "tactique" désigne la raison pour laquelle un attaquant effectue une action, l'objectif qu'il souhaite atteindre à un certain stade d'une attaque.

(3) Dans la présente méthodologie de l'échelle de classification des cyberattaques, sauf si le contexte indique clairement le contraire, le singulier comprend également le pluriel et vice versa.

Article 3
Principes de classification des cyberattaques

(1) La présente méthodologie de l'échelle de classification des cyberattaques permet d'évaluer la gravité d'une cyberattaque selon cinq niveaux spécifiés à l'article 7 et à l'annexe I de la présente méthodologie.

(2) La présente méthodologie de l'échelle de classification des cyberattaques définit les règles de classification de la gravité d'une cyberattaque en fonction des paramètres suivants :

a. l'impact potentiel compte tenu des biens et des périmètres exposés en vertu de l'article 5 qui sont déterminés conformément à l'article 26, paragraphe 4, point c), du règlement du NCCS; et

b. l'estimation des causes profondes de la cyberattaque conformément à l'article 4 de la présente méthodologie ; et

c. la gravité de la cyberattaque conformément à l'article 6 de la présente méthodologie.

TITRE 2
Identification d'une cyberattaque à signaler

Article 4
Estimation de la cause première

(1) Les entités doivent fournir une estimation de la cause première de l'événement, en tenant compte du fait que

- **Une cause racine malveillante** signifie que l'origine de l'événement est une intention humaine de causer délibérément un préjudice ou un dommage.
- **Une cause première non malveillante** signifie que l'origine de l'événement est dépourvue de toute intention humaine de causer délibérément un préjudice ou un dommage.
- **Une cause première incertaine** signifie que l'origine n'est pas claire ou ne peut pas encore être catégorisée.

(2) L'événement est considéré comme une cyberattaque par l'entité lorsqu'il est estimé avoir une cause première malveillante ou incertaine.

(3) Si la cause première est jugée incertaine, l'entité doit continuer à l'évaluer.

(4) Dans le cas où une cause première "non malveillante" est évaluée sans aucun doute, l'entité ne doit pas considérer l'événement comme devant être signalé conformément à l'article 38, paragraphe 4, du règlement sur les NCCS.

Article 5
Détermination de l'impact potentiel de la cyberattaque

(1) L'entité doit déterminer l'impact potentiel de la cyberattaque de la manière suivante :

a) **Impact potentiel faible :** Tout bien touché par la cyberattaque n'appartient ni à un périmètre à fort impact ni à un périmètre à impact critique et ne peut atteindre directement aucun bien situé dans un périmètre à fort impact ou à impact critique.

b) **Impact potentiel élevé** :

i. Au moins un bien touché par la cyberattaque appartient au périmètre à fort impact et aucun d'entre eux n'appartient au périmètre à impact critique ; ou

ii. au moins un bien touché par la cyberattaque peut atteindre directement un bien appartenant au périmètre à fort impact et non au périmètre à impact critique.

c) **Impact potentiel critique** :

i. Au moins un bien touché par la cyberattaque appartient au périmètre d'impact critique ; ou

ii. au moins un bien touché par la cyberattaque peut atteindre directement un bien appartenant au périmètre d'impact critique.

Article 6
Estimation de la gravité de la cyberattaque

(1) L'entité doit estimer la gravité de la cyberattaque :

a) Une cyberattaque **de faible gravité** signifie que l'attaquant tente d'accéder à un ou plusieurs biens ;

b) Une cyberattaque de **gravité élevée** signifie que l'attaquant a au moins un accès limité à un ou plusieurs biens ;
c) Une cyberattaque d'une **gravité critique** signifie que plus d'un actif est touché par un mouvement latéral, ou que l'attaquant est en mesure d'interrompre le processus ou de mener des actions sur un ou plusieurs actifs afin de déstabiliser l'entité.

Pour réaliser cette estimation, les entités peuvent utiliser le paragraphe (2).

(2) L'entité peut évaluer la position de l'attaquant dans le cadre des tactiques pour le SCI et l'entreprise MITRE ATT&CK[1] , sur la base du scénario le plus défavorable et de sa prévision de la situation à venir :

a) **Faible gravité** : détection d'une tentative de reconnaissance, de développement des ressources, d'accès initial.
b) **Gravité élevée :** détection d'une tentative d'exécution, de persistance, d'escalade des privilèges, d'évasion de la défense, d'accès aux informations d'identification, de découverte.
c) **Gravité critique :** détection d'une tentative de mouvement latéral, de collecte, de commandement et de contrôle, d'exfiltration, d'inhibition de la fonction de réaction, d'altération du contrôle des processus ou d'impact.

[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
Classification de la gravité des cyberattaques

(1) L'entité doit évaluer la gravité de la cyberattaque en combinant les éléments suivants :

(a) le résultat de la détermination de l'impact potentiel de la cyberattaque conformément à l'article 5 de la présente méthodologie ; et

(b) le résultat de l'estimation de la gravité de la cyberattaque conformément à l'article 6 de la présente méthodologie.

(2) Le niveau de gravité est considéré comme :

(a) "critique" si l'impact potentiel est jugé "critique" et que la gravité est estimée "critique" ; ou

(b) "élevé" si :

i. l'impact potentiel est jugé "critique" et la gravité est estimée "élevée" ; ou,

ii. l'impact potentiel est jugé "élevé" et la gravité est estimée "critique" ou "élevée" ; ou

(c) "important", "moyen" et "à suivre" selon les critères énoncés à l'annexe I de la présente méthodologie.

(3) Chaque fois que l'un des paramètres suivants change, l'entité répète les étapes pour évaluer la gravité de la cyberattaque conformément au TITRE 2 :

(a) un changement dans l'estimation de la cause première conformément à l'article 4 de la présente méthodologie ; ou

(b) une modification de la détermination de l'impact potentiel conformément à l'article 5 de la présente méthodologie ; ou

(c) un changement dans l'estimation de la gravité conformément à l'article 6.1 de la présente méthodologie.

TITRE 3
Dispositions finales

Article 8
Calendrier de mise en œuvre

(1) Cette méthodologie sera mise en œuvre conformément au calendrier fixé dans le règlement sur les NCCS.

(2) Les entités visées à l'article 24, paragraphe 6, du règlement du NCCS doivent utiliser cette méthodologie pour déterminer si une cyberattaque doit être déclarée en vertu du règlement du NCCS.

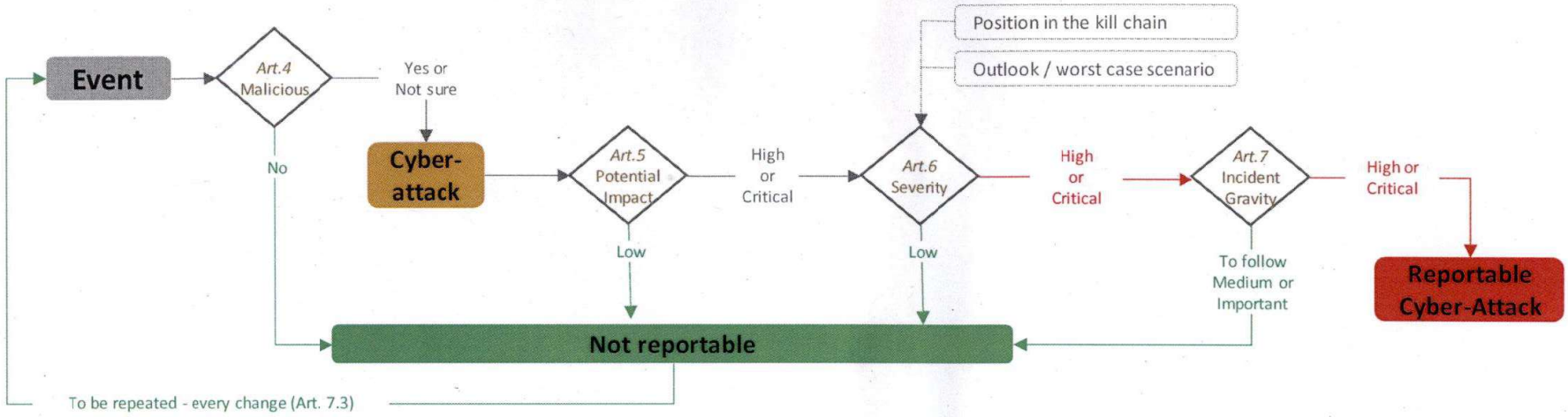
Article 9
Langue

La langue de référence de la présente proposition de méthodologie d'échelle de classification des cyberattaques est l'anglais. Pour éviter toute ambiguïté, lorsque les autorités nationales compétentes l'exigent pour le règlement du NCCS, les GRT et les GRD de l'État membre concerné traduisent, en coopération, la présente proposition de méthodologie d'échelle de classification des cyberattaques dans leur(s) langue(s) nationale(s).

En cas d'incohérences entre la version anglaise publiée par les GRT, avec l'assistance du REGRT-E, et en coopération avec l'entité des GRD de l'UE, conformément à l'article 8, paragraphe 9, du règlement du NCCS et toute version traduite dans une autre langue, les GRT et GRD concernés fournissent, conformément à la législation nationale, aux autorités nationales compétentes pour le règlement du NCCS une traduction mise à jour de la proposition de méthodologie de l'échelle de classification des cyber-attaques.

Annexe I

Severity of the Attack	Potential Impact: Low PI	Potential Impact: High PI	Potential Impact: Critical PI
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	Potential Impact: High PI	Potential Impact: 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