RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CRE COMMISSION DE RÉGULATION DE L'ÉNERGIE

DÉLIBÉRATION N°2026-125

Délibération de la Commission de régulation de l'énergie du 17 juin 2026 portant approbation de la méthodologie d'échelle de classification des cyberattaques conformément à l'article 37 du règlement délégué (UE) 2024/1366

Participaient à la séance : Emmanuelle WARGON, présidente, Victor ALONSO, Anthony CELLIER, Nadia FAURE et Didier REBISCHUNG, commissaires.

1. Contexte et compétence de la CRE

Le point e) du paragraphe 2 de l'article 59 du règlement (UE) 2019/943[1] prévoit que « [l]*a Commission est habilitée à adopter des actes délégués* […] *dans les domaines suivants :* […] *règles sectorielles concernant les aspects liés à la cybersécurité des flux transfrontaliers d'électricité* ».

Le 4 décembre 2020, la Commission de régulation de l'énergie (CRE) a mis en place un groupe de travail, avec l'agence nationale de la sécurité des systèmes d'information (ANSSI), regroupant les acteurs du système énergétique français notamment pour porter leurs messages au niveau européen et obtenir tout l'appui à la compréhension nécessaire, à la participation, à l'élaboration, puis à la mise en œuvre, de ce règlement délégué.

Le règlement délégué (UE) 2024/1366[2] (ci-après « NCCS ») est entré en vigueur le 13 juin 2024. Il établit un code de réseau sur des règles sectorielles concernant les aspects liés à la cybersécurité des flux transfrontaliers d'électricité.

Le paragraphe 1 de l'article 4 du NCCS prévoit :

- d'une part, que chaque État membre désigne une autorité gouvernementale ou réglementaire nationale chargée d'exécuter les tâches qui lui sont assignées par le NCCS et,
- d'autre part, que, jusqu'à cette désignation, l'autorité de régulation désignée par chaque État membre conformément à l'article 57, paragraphe 1, de la directive (UE) 2019/944[3] exécute les tâches de l'autorité compétente.

Le paragraphe 3 de de l'article 4 du NCCS prévoit de plus que l'État membre peut autoriser l'autorité compétente à déléguer les tâches qui lui sont assignées par le NCCS. En France, à défaut de la désignation d'une autorité gouvernementale ou réglementaire nationale ou d'autorisation de délégation, la CRE est tenue d'exécuter l'ensemble des tâches dévolues à l'autorité compétente.

Le 25 avril 2025, conformément au paragraphe 7 de l'article 47 du NCCS, l'agence pour la coopération des régulateurs de l'énergie (ACER) a publié des lignes directrices[4] permettant aux entités à fort impact ou à impact critique d'échanger des informations dans le cadre de l'application du NCCS (ci-après « Lignes directrices de l'ACER »). Ces Lignes directrices de l'ACER encadrent, pour toutes les entités identifiées ou non, notamment les échanges de données dans le cadre du NCCS, leur marquage et son implication, ou leur anonymisation et leur agrégation, devant permettre ainsi leur protection.

---

[1] Règlement (UE) 2019/943 du Parlement européen et du Conseil du 5 juin 2019 sur le marché intérieur de l'électricité

[2] Règlement délégué (UE) 2024/1366 de la Commission du 11 mars 2024 complétant le règlement (UE) 2019/943 du Parlement européen et du Conseil en établissant un code de réseau sur des règles sectorielles concernant les aspects liés à la cybersécurité des flux transfrontaliers d'électricité

[3] Directive (UE) 2019/944 du Parlement européen et du Conseil du 5 juin 2019 concernant des règles communes pour le marché intérieur de l'électricité

[4] *Guidelines for the entities on information exchange mechanisms* (ACER – 25 avril 2025)

Le paragraphe 8 de l'article 37 du NCCS prévoit que les gestionnaires des réseaux de transport élaborent une méthodologie d'échelle de classification des cyberattaques pour le 13 juin 2025.

Le paragraphe 1 de l'article 8 du NCCS prévoit que les gestionnaires des réseaux de transport soumettent leur projet d'une méthodologie pour approbation aux autorités compétentes. Le paragraphe 5 du même article prévoit que les autorités compétentes se prononcent sur ces projets dans un délais de six mois à compter de leur réception par l'autorité compétente concernée ou, le cas échéant, par la dernière autorité compétente concernée.

Le 23 juin 2025, RTE a saisi la CRE d'un projet d'une méthodologie d'échelle de classification des cyberattaques (ci-après « le Projet »). Le 28 novembre 2025, l'ensemble des gestionnaires de réseau de transport européens concernés par le Projet avaient saisi leur autorité compétente du Projet. Ainsi, les autorités compétentes avaient six mois à partir de cette date pour approuver le Projet ou demander à leur gestionnaire de réseau de transport de l'amender, conformément à l'article 8 du NCCS susmentionné.

La présente délibération a pour objet d'approuver le Projet annexé.

2. Contenu du Projet

Le paragraphe 4 de l'article 38 du NCCS prévoit que les informations liées à une cyberattaque sont considérées comme devant faire l'objet d'une déclaration lorsque l'évaluation de la cyberattaque par l'entité concernée conclut à une gravité allant de « élevée » à « critique » selon la méthode/échelle de classification des cyberattaques établie conformément à l'article 37, paragraphe 8, du NCCS.

Le Projet décrit le processus, dont le contenu est détaillé ci-après, au cours duquel un événement est classé ou non comme une cyberattaque puis, le cas échant, la gravité de celle-ci est définie et enfin, suivant le degré de gravité, la nécessité ou non de la signaler.

Selon le Projet, un événement est considéré comme une cyberattaque s'il n'est pas établi que sa cause n'est pas malveillante. Ainsi les événements de cause indéterminée ou malveillante sont considérés comme une cyberattaque. Ceux de cause non-malveillante certaine ne sont pas qualifiés de cyberattaque et ne doivent donc pas être signalés.

La gravité d'une cyberattaque est la combinaison de son impact potentiel et de sa sévérité, chacun évalué sur une échelle de trois niveaux (faible, élevé et critique). L'impact potentiel est déterminé en fonction de la criticité du périmètre des biens auxquels la cyberattaque porte atteinte. La sévérité quant à elle est fonction du degré de pénétration de la cyberattaque. La gravité est déterminée conformément au tableau ci-dessous.

Gravité de la cyberattaque		Impact potentiel		
		Faible	Élevé	Critique
Sévérité	Faible	À suivre	Moyenne	Importante
	Élevée	Moyenne	Élevée	Élevée
	Critique	Importante	Élevée	Critique

Tableau 1 – Détermination de la gravité d'une cyberattaque suivant son impact potentiel et sa sévérité (source : annexe I du Projet)

Si la sévérité et l'impact potentiel sont élevés ou critiques, la cyberattaque doit être signalée.

Le paragraphe 1 de l'article 37 prévoit qu'une fois une cyberattaque signalée au centre de réponse aux incidents de sécurité informatique (CSIRT[5]) et à son autorité compétente nationale, cette dernière doit anonymiser l'information et en informer les entités et les autorités ayant à en connaître dans les vingt-quatre heures.

3. Analyse de la CRE

3.1. Sur le Projet

La CRE considère que le Projet est clair et simple. Il permet un traitement efficace et rapide des événements, notamment leur tri, avant le cas échéant leur signalement.

La CRE recommande que les entités désignées entités à fort impact ou à impact critique provisoires désignées conformément à l'article 48 du NCCS appliquent volontairement le Projet en vue de signaler les cyberattaques qu'elles viendraient à subir, dans l'attente de la nomination définitive des entités à fort impact ou à impact critique conformément à l'article 24 du même code.

La CRE recommande que les informations échangées le soient suivant les Lignes directrices de l'ACER.

Le sous-groupe *ad hoc* du groupe de travail sur la cybersécurité de la CRE avec le soutien de l'ANSSI se réunira pour établir les modalités de cette mise en œuvre transitoire.

3.2. Sur l'autorité compétente

La CRE constate l'absence de désignation d'une autorité compétente en France ainsi que l'absence de décision permettant à l'autorité compétente de déléguer ses tâches.

La CRE n'a à ce jour pas la capacité de traiter dans les délais impartis les signalements de cyberattaque.

Compte tenu des enjeux de sécurité ou de continuité d'alimentation, la CRE recommande que, sans délai, une autorité compétente en mesure de traiter les signalements dans les délais impartis soit désignée ou que la CRE puisse déléguer cette tâche à une autorité capable de les traiter de façon adéquate.

La CRE note que, s'agissant des signalements de cyberattaques, le CSIRT à périmètre national[6] doit, comme l'autorité compétente, se voir communiquer les informations relatives aux déclarations des cyberattaques. La CRE recommande que la réception des informations relatives à une cyberattaque relève de la compétence du CSIRT notamment du fait de sa compétence avérée et pour éviter tout doublon.

[5] Centre chargé de la gestion des risques et des incidents, rôle dévolu au *French Computer Emergency Response Team* (CERT-FR) en France au sein de l'ANSSI

[6] Computer Security Incident Response Team ou « équipe de réponse aux incidents de sécurité informatique »

Décision de la CRE

Le paragraphe 8 de l'article 37 du règlement délégué (UE) 2024/1366 du 11 mars 2024 (ci-après « NCCS ») prévoit que les gestionnaires des réseaux de transport élaborent une méthodologie d'échelle de classification des cyberattaques pour le 13 juin 2025.

Le paragraphe 1 de l'article 8 du NCCS prévoit que les gestionnaires des réseaux de transport soumettent leurs projets d'une méthodologies pour approbation aux autorités compétentes. Le paragraphe 5 du même article prévoit que les autorités compétentes se prononcent sur ces projets dans un délai de six mois à compter de leur réception par l'autorité compétente concernée ou, le cas échéant, par la dernière autorité compétente concernée.

Le paragraphe 1 de l'article 4 du NCCS prévoit que, jusqu'à la désignation par l'État membre d'une autorité gouvernementale ou réglementaire nationale chargée d'exécuter les tâches qui lui sont assignées par le NCCS, l'autorité de régulation désignée par chaque État membre conformément à l'article 57, paragraphe 1, de la directive (UE) 2019/944 exécute les tâches de l'autorité compétente.

Le 23 juin 2025, RTE a saisi la Commission de régulation de l'énergie (CRE) d'un projet d'une méthodologie d'échelle de classification des cyberattaques. Le 28 novembre 2025, l'ensemble des gestionnaires de réseau de transport européens concernés par le Projet avaient saisi leur autorité compétente du Projet. Ainsi, les autorités compétentes avaient six mois à partir de cette date pour approuver le Projet ou demander à leur gestionnaire de réseau de transport de l'amender, conformément à l'article 8 du NCCS susmentionné.

La CRE approuve la méthodologie d'échelle de classification des cyberattaques permettant un traitement efficace et rapide des événements, notamment leur tri.

La CRE recommande que les entités désignées entités à fort impact ou à impact critique provisoires désignées conformément à l'article 48 du NCCS appliquent volontairement cette méthodologie en vue de signaler les cyberattaques qu'elles viendraient à subir, dans l'attente de la nomination définitive des entités à fort impact ou à impact critique conformément à l'article 24 du même code. Les modalités de mise en œuvre seront, pour cette phase transitoire, établies dans le sous-groupe *ad hoc* de son groupe de travail sur la cybersécurité avec le soutien de l'ANSSI.

La CRE recommande que les informations soient échangées dans le cadre des signalements suivant les lignes directrices de l'ACER du 25 avril 2025 permettant aux entités à fort impact ou à impact critique d'échanger des informations dans le cadre de l'application du NCCS.

La CRE recommande que, sans délai, une autorité compétente en mesure de traiter les signalements dans les délais impartis soit désignée ou que la CRE puisse déléguer cette tâche à une autorité capable de les traiter de façon adéquate.

La CRE recommande que le traitement des signalements de cyberattaques incombe (soit directement, soit par délégation) au centre de réponse aux incidents de sécurité informatique (rôle aujourd'hui dévolu au *French Computer Emergency Response Team* (CERT-FR) en France au sein de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)) notamment du fait de sa compétence avérée et pour éviter tout doublon.

La présente délibération sera publiée sur le site internet de la CRE. Elle sera transmise à la ministre chargée de l'énergie, à l'ANSSI et aux entités à fort impact ou à impact critique provisoires.

Délibéré à Paris, le 17 juin 2026.
Pour la Commission de régulation de l'énergie,
La présidente,
Emmanuelle WARGON

Annexe

Projet d'une méthodologie d'échelle de classification des cyberattaques dont RTE a saisi la CRE le 23 juin 2025