Conseil de
l'Union européenne

Bruxelles, le 7 septembre 2023
(OR. en)

12485/23

Dossier interinstitutionnel:
2023/0318(NLE)

PROCIV 57	**ATO 48**
ENV 925	**CSC 408**
JAI 1084	**ECOFIN 839**
SAN 494	**CSCI 149**
COSI 140	**DATAPROTECT 216**
CHIMIE 85	**MI 698**
ENFOPOL 356	**CODEC 1500**
RECH 380	**COPS 418**
CT 133	**JAIEX 46**
DENLEG 38	**COPEN 292**
COTER 153	**IND 441**
RELEX 987	**POLMIL 221**
ENER 467	**IPCR 55**
HYBRID 53	**DIGIT 160**
TRANS 329	**DISINFO 62**
CYBER 203	**CSDP/PSDC 608**
TELECOM 251	**MARE 18**
ESPACE 45	**POLMAR 47**

NOTE DE TRANSMISSION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	6 septembre 2023
Destinataire:	Madame Thérèse BLANCHET, secrétaire générale du Conseil de l'Union européenne
N° doc. Cion:	COM(2023) 526 final
Objet:	Proposition de RECOMMANDATION DU CONSEIL relative à un schéma directeur visant à coordonner au niveau de l'Union la réponse en cas de perturbations des infrastructures critiques ayant une dimension transfrontière notable

Les délégations trouveront ci-joint le document COM(2023) 526 final.

p.j.: COM(2023) 526 final

COMMISSION
EUROPÉENNE

Bruxelles, le 6.9.2023
COM(2023) 526 final

2023/0318 (NLE)

Proposition de

RECOMMANDATION DU CONSEIL

relative à un schéma directeur visant à coordonner au niveau de l'Union la réponse en cas de perturbations des infrastructures critiques ayant une dimension transfrontière notable

(Texte présentant de l'intérêt pour l'EEE)

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Justification et objectifs de la proposition

Dans le contexte géopolitique actuel, caractérisé par une instabilité croissante, résultant notamment de la guerre d'agression menée par la Russie contre l'Ukraine et de la complexité grandissante des menaces pesant sur la sécurité, ainsi que par les effets du changement climatique, tels que l'augmentation des événements climatiques inhabituels ou les pénuries d'eau, l'Union doit rester vigilante et s'adapter en permanence. Les citoyens, les entreprises et les autorités de l'Union dépendent d'infrastructures critiques[1] en raison des services essentiels fournis par les entités exploitant ces infrastructures. Ces services sont cruciaux pour le maintien de fonctions sociétales ou d'activités économiques vitales, de la santé publique et de la sûreté publique, ou de l'environnement, et doivent être fournis sans entrave dans le marché intérieur. Par conséquent, en raison de l'importance de ces services essentiels pour le marché intérieur et, par conséquent, de la nécessité de rendre les infrastructures critiques plus résilientes et, plus généralement, de garantir la résilience des entités critiques qui fournissent ces services, l'Union doit prendre des mesures pour renforcer cette résilience et atténuer toute perturbation de la fourniture de ces services essentiels. De telles perturbations pourraient sinon avoir de graves conséquences pour les citoyens de l'Union, nos économies et la confiance dans nos systèmes démocratiques et nuire au bon fonctionnement du marché intérieur, en particulier dans un contexte d'interdépendances croissantes entre les secteurs et par-delà les frontières.

L'Union a déjà pris un certain nombre de mesures pour renforcer la protection des infrastructures critiques, notamment en ce qui concerne les infrastructures transfrontières, et la résilience des entités critiques, afin de prévenir ou d'atténuer les effets des perturbations des services essentiels qu'elles fournissent dans le marché intérieur.

La directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes[2] (ci-après la «directive ICE») a été le premier instrument juridique à établir une procédure à l'échelle de l'UE pour le recensement et la désignation des infrastructures critiques européennes et une approche commune pour évaluer la nécessité d'améliorer la protection de ces infrastructures contre les menaces d'origine humaine – tant intentionnelles qu'accidentelles – ainsi que contre les catastrophes naturelles. Toutefois, elle se concentrait uniquement sur les secteurs de l'énergie et des transports et sur la protection des infrastructures critiques et ne prévoyait pas de mesures plus larges pour renforcer la résilience des entités exploitant ces infrastructures.

En raison de la nature de plus en plus interconnectée et transfrontière des opérations au sein du marché intérieur, il était nécessaire de couvrir plus que deux secteurs et d'aller au-delà de mesures de protection d'actifs individuels. C'est pourquoi la directive (UE) 2022/2557 sur la résilience des entités critiques[3] (ci-après la «directive CER») a été adoptée en 2022, en même

---

[1] Le terme «infrastructure critique» désigne un bien, une installation, un équipement, un réseau ou un système, ou une partie d'un bien, d'une installation, d'un équipement, d'un réseau ou d'un système, qui est nécessaire à la fourniture d'un service essentiel [article 2, point 4), de la directive (UE) 2022/2557 sur la résilience des entités critiques].

[2] Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection (JO L 345 du 23.12.2008, p. 75).

[3] Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil (JO L 333 du 27.12.2022, p. 164).

temps que la directive (UE) 2022/2555 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union[4] (ci-après la «directive SRI 2»). L'objectif est de garantir un niveau global de résilience physique et numérique des entités critiques. La directive CER est entrée en vigueur le 16 janvier 2023 et vise à aider les États membres à renforcer la résilience globale des entités critiques, tout en renforçant la coordination au niveau de l'Union. Elle remplacera la directive ICE à compter du 18 octobre 2024, date à laquelle les États membres devront prendre les mesures nécessaires pour s'y conformer. La directive CER s'applique à onze secteurs[5]. Elle met l'accent non plus sur la protection des infrastructures critiques, mais sur le concept plus large de résilience des entités critiques exploitant ces infrastructures critiques, qui couvre la période avant, pendant et après un incident. La directive SRI 2 est également entrée en vigueur le 16 janvier 2023 et modernise le cadre juridique existant afin de s'adapter à la numérisation accrue et à l'évolution du panorama des cybermenaces. Elle étend également le champ d'application des règles de cybersécurité à de nouveaux secteurs et entités et améliore les capacités de résilience et de réponse aux incidents des entités publiques et privées, des autorités compétentes et de l'Union dans son ensemble.

La directive CER comprend des dispositions relatives à la notification des incidents par l'entité critique à l'autorité nationale compétente, à la notification des autres États membres (potentiellement) touchés par l'autorité nationale compétente et à la notification de la Commission si l'incident touche six États membres ou plus. La directive CER prévoit certaines obligations de notification des incidents lorsque l'incident a ou pourrait avoir des conséquences importantes sur les entités critiques et sur la continuité de la fourniture de services essentiels à ou dans un ou plusieurs autres États membres[6].

Comme l'illustre le sabotage des gazoducs Nord Stream en septembre 2022, le contexte de sécurité dans lequel les infrastructures critiques sont exploitées a considérablement changé et une action supplémentaire urgente est nécessaire au niveau de l'Union afin de renforcer la résilience des infrastructures critiques, non seulement en ce qui concerne la préparation, mais aussi pour apporter une réponse coordonnée.

Dans ce contexte, une recommandation du Conseil relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques[7] (ci-après la «recommandation sur la résilience des infrastructures critiques») a été adoptée le 8 décembre 2022 à la suite d'une proposition de la Commission. Cette recommandation souligne, entre autres, la nécessité d'assurer, au niveau de l'Union, une réponse coordonnée et efficace face aux risques actuels et futurs pesant sur la fourniture de services essentiels. Plus spécifiquement, le Conseil a invité la Commission à élaborer un «schéma directeur sur une réponse coordonnée en cas de perturbations des infrastructures critiques ayant une dimension transfrontière notable». La recommandation indique que ce schéma directeur devrait être

[4] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (JO L 333 du 27.12.2022, p. 80).

[5] Énergie, transports, secteur bancaire, infrastructures des marchés financiers, infrastructures numériques, administration publique, espace, santé, eau potable, eaux résiduaires, et production, transformation et distribution de denrées alimentaires.

[6] Conformément à l'article 15, paragraphes 1 et 3, de la directive CER.

[7] Recommandation du Conseil du 8 décembre 2022 relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques (2023/C 20/01) (JO C 20 du 20.1.2023, p. 1).

cohérent avec le protocole de l'Union de lutte contre les menaces hybrides[8], tenir compte de la recommandation 2017/1584 de la Commission sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs[9] (ci-après le «plan d'action pour la cybersécurité») et respecter le dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR)[10].

Dans ce contexte, la présente proposition de recommandation supplémentaire du Conseil contient un tel schéma directeur. La proposition vise à compléter le cadre juridique actuel en décrivant la réponse coordonnée au niveau de l'Union en cas de perturbations d'infrastructures critiques ayant une dimension transfrontière notable, tout en utilisant les dispositifs existants au niveau de l'Union. Concrètement, la proposition décrit le champ d'application et les objectifs du schéma directeur et les acteurs, les processus et les outils existants qui pourraient être utilisés pour réagir, de manière coordonnée au niveau de l'Union, à un incident perturbant une infrastructure critique ayant un effet transfrontière notable, et décrit les modalités de la coopération entre les États membres et les institutions, organes et organismes de l'Union dans de telles situations.

- **Cohérence avec les dispositions existantes dans le domaine d'action**

La présente proposition de recommandation du Conseil est conforme et complète le cadre juridique actuel sur la protection des infrastructures critiques et la résilience des entités critiques – respectivement la directive ICE et la directive CER, ainsi que la recommandation sur la résilience des infrastructures critiques – dans la mesure où elle vise à assurer, de manière complémentaire, la coordination entre les États membres et entre ceux-ci et les institutions, organes et organismes de l'Union en ce qui concerne la réponse à apporter aux incidents qui provoquent des perturbations d'infrastructures critiques ayant une dimension transfrontière notable et de la fourniture de services essentiels. La proposition utilise les structures et mécanismes existants au niveau de l'Union, y compris ceux établis par la directive CER, à savoir la coopération entre les autorités compétentes et le groupe sur la résilience des entités critiques, qui a été établi par la directive CER afin de soutenir la Commission et de faciliter la coopération entre les États membres et l'échange d'informations sur les questions relatives à la directive CER.

La présente proposition de recommandation du Conseil est également conforme et complémentaire au cadre de l'Union en matière de cybersécurité établi par la directive SRI 2.

La présente proposition vise à soumettre, dans le domaine de la résilience des entités critiques et de la protection des infrastructures critiques, un schéma directeur pour les infrastructures critiques similaire au plan d'action pour la cybersécurité.

La partie I, point 4 b), de l'annexe explique également les interconnexions avec le plan d'action pour la cybersécurité, qui s'applique aux incidents de cybersécurité majeurs qui provoquent des perturbations dépassant les capacités d'action du seul État membre concerné ou qui frappent plusieurs États membres ou institutions de l'Union en s'accompagnant de répercussions techniques ou politiques si vastes et significatives qu'ils requièrent une coordination et une réaction rapides au niveau politique de l'Union. Le terme «incident» est

[8] Document de travail conjoint des services, Protocole opérationnel de l'Union européenne de lutte contre les menaces hybrides [SWD(2023) 116 final].

[9] Recommandation (UE) 2017/1584 de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs (JO L 239 du 19.9.2017, p. 36).

[10] Décision d'exécution (UE) 2018/1993 du Conseil du 11 décembre 2018 concernant le dispositif intégré de l'Union européenne pour une réaction au niveau politique dans les situations de crise (JO L 320 du 17.12.2018, p. 28).

défini dans la directive SRI 2 comme étant «un événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles» (ci-après «cyberincident»).

Les autorités compétentes au titre de la directive CER et de la directive SRI 2 ont l'obligation de coopérer et d'échanger des informations sur les incidents et incidents en matière de cybersécurité affectant les entités critiques, y compris en ce qui concerne les mesures pertinentes adoptées. Dans une situation où un incident majeur affectant une infrastructure critique et un incident de cybersécurité majeur concernent la même entité, il devrait y avoir une coordination des réponses éventuelles entre les acteurs concernés.

La présente proposition est cohérente avec le protocole de l'Union de lutte contre les menaces hybrides, ce dernier étant applicable en cas d'incident hybride. La partie I, point 4 a), de l'annexe explique les interconnexions avec le protocole de l'Union, y compris en précisent quel instrument s'applique en cas d'incident majeur affectant une infrastructure critique qui revêt une dimension hybride.

La proposition est également cohérente par rapport à d'autres mécanismes existants de gestion des crises à l'échelon de l'Union, tels que le dispositif IPCR du Conseil, le processus interne de coordination des crises de la Commission (ARGUS)[11] et le mécanisme de protection civile de l'Union[12] (ci-après le «MPCU») soutenu par son centre de coordination de la réaction d'urgence (ERCC) et le mécanisme de réaction aux crises du Service européen pour l'action extérieure.

La proposition est également cohérente avec les autres législations sectorielles pertinentes, et notamment avec les mesures spécifiques qu'elles contiennent et qui réglementent certains aspects de la réponse aux perturbations apportées par les entités opérant dans les secteurs concernés.

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

• Base juridique

La proposition est fondée sur l'article 114 du traité sur le fonctionnement de l'Union européenne (ci-après le «TFUE»), qui implique le rapprochement des législations en vue de l'amélioration du marché intérieur, ainsi que sur l'article 292 TFUE, qui établit les règles pertinentes concernant l'adoption de recommandations.

Le choix de l'article 114 TFUE comme base juridique matérielle se justifie par le fait que la proposition de recommandation du Conseil vise à garantir une réponse coordonnée en cas de perturbations d'infrastructures critiques ayant une dimension transfrontière notable. De telles perturbations concernent plusieurs États membres et risquent d'avoir des conséquences sur le fonctionnement du marché intérieur en raison des dépendances mutuelles croissantes entre les infrastructures et les secteurs dans une économie de l'Union de plus en plus interdépendante. Une meilleure réponse aux perturbations évitera, à son tour, de perturber le fonctionnement du marché intérieur, étant donné que ces infrastructures critiques et les services essentiels

[11] Communication de la Commission au Parlement européen, au Conseil, Comité économique et social européen et au Comité des régions - Dispositions de la Commission relatives au système général d'alerte rapide «ARGUS» [COM(2005) 662 final].

[12] Règlement (UE) 2021/836 du Parlement européen et du Conseil du 20 mai 2021 modifiant la décision n° 1313/2013/UE relative au mécanisme de protection civile de l'Union (JO L 185 du 26.5.2021, p. 1).

qu'elles fournissent sont cruciaux pour le maintien de fonctions sociétales ou d'activités économiques vitales, de la santé publique et de la sûreté publique, ou de l'environnement.

La proposition viendrait compléter les directives ICE et CER, qui sont également fondées sur l'article 114 TFUE. La recommandation sur la résilience des infrastructures critiques est, comme la recommandation à présent proposée, également fondée sur les articles 114 et 292 TFUE.

- **Subsidiarité (en cas de compétence non exclusive)**

Alors que la réponse aux perturbations des infrastructures critiques ou des services fournis par les entités critiques exploitant ces infrastructures critiques relève avant tout de la responsabilité des États membres, l'Union joue un rôle important en cas de perturbation d'une infrastructure critique ayant une dimension transfrontière notable, étant donné qu'une telle perturbation peut avoir une incidence sur plusieurs pans de l'activité économique au sein du marché unique, voire sur tous les pans de celle-ci, ainsi que sur la sécurité et les relations internationales de l'Union. Afin de garantir le bon fonctionnement du marché intérieur, la coordination, au niveau de l'Union, en cas de perturbation d'une infrastructure critique ayant une dimension transfrontière notable est non seulement appropriée, mais aussi nécessaire, étant donné qu'une telle réponse coordonnée au niveau de l'Union soutiendra la réaction des États membres à la perturbation grâce à une connaissance situationnelle partagée, à une communication publique coordonnée et à l'atténuation des conséquences de la perturbation sur le marché intérieur.

- **Proportionnalité**

La présente proposition est conforme au principe de subsidiarité énoncé à l'article 5, paragraphe 4, du traité sur l'Union européenne (TUE).

Ni le contenu ni la forme de cette recommandation du Conseil telle qu'elle est proposée n'excèdent ce qui est nécessaire pour atteindre ses objectifs. Les actions proposées sont proportionnées aux objectifs poursuivis, qui visent à garantir une réponse coordonnée au niveau de l'Union en cas de perturbation des infrastructures critiques ou des services fournis par les entités critiques exploitant ces infrastructures critiques et revêtant une dimension transfrontière notable. Cette proposition de réponse coordonnée est proportionnée aux prérogatives et obligations des États membres au titre du droit national. Les incidents qui perturbent des infrastructures critiques ou la fourniture de services essentiels par des entités critiques n'atteignent souvent pas le seuil établi pour un incident majeur affectant une infrastructure critique et peuvent être traités efficacement au niveau national. Par conséquent, le recours au mécanisme prévu par la présente proposition est limité aux perturbations majeures qui ont une dimension transfrontière notable concernant plusieurs États membres.

- **Choix de l'instrument**

Pour atteindre les objectifs susmentionnés, le TFUE prévoit, notamment en son article 292, l'adoption de recommandations par le Conseil, sur la base d'une proposition de la Commission. Conformément à l'article 288 du TFUE, les recommandations ne lient pas. Une recommandation du Conseil est un instrument approprié dans ce cas, car elle marque l'engagement des États membres en faveur des mesures qui y figurent et fournit une base solide pour la coopération dans le domaine de la réponse coordonnée en cas de perturbations importantes d'infrastructures critiques. De cette manière, la recommandation proposée viendrait compléter le cadre juridique contraignant (en particulier la directive CER) ainsi que la recommandation sur la résilience des infrastructures critiques adoptée précédemment, qui

préconise de telles mesures complémentaires, tout en respectant pleinement les responsabilités des États membres dans le domaine en question.

3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

• Consultation des parties intéressées

Dans le cadre de l'élaboration de la présente proposition, les États membres, les institutions et les agences de l'Union ont été consultés. En outre, les avis exprimés par les experts des États membres lors de l'atelier du 24 avril 2023 et envoyés par écrit à la suite de cet atelier ont été pris en considération.

Un large consensus s'est dégagé sur l'utilité d'assurer une coordination accrue de la réponse au niveau de l'Union aux perturbations des infrastructures critiques ayant une dimension transfrontière notable dans le contexte actuel de menace, tout en respectant la compétence des États membres dans ce domaine ainsi que la confidentialité des informations sensibles. Un consensus s'est également dégagé sur la nécessité d'éviter la duplication des instruments et de faire bon usage des mécanismes existants au niveau de l'Union pour la coordination, l'échange d'informations et la réponse.

Si certains États membres ont exprimé un avis positif en ce qui concerne le champ d'application plus large du schéma directeur pour les infrastructures critiques, d'autres ont estimé que le seuil de six États membres ou plus prévu par la directive CER pour le recensement des entités critiques d'importance européenne particulière était suffisant et qu'il n'était pas nécessaire d'inclure un second type d'incident dans le champ d'application. Quelques États membres ont souligné à quel point il importait d'associer, le cas échéant, les opérateurs d'infrastructures critiques fournissant des services essentiels, compte tenu de leur expertise et de l'importance de tenir compte de la dimension virtuelle («cyber»).

• Explication détaillée de certaines dispositions de la proposition

La proposition de recommandation du Conseil se compose d'une partie principale et d'une annexe.

La partie principale est constituée de 11 points, comme suit:

Le point 1) expose la nécessité d'une coopération renforcée en ce qui concerne la réponse aux incidents majeurs affectant des infrastructures critiques conformément au schéma directeur pour les infrastructures critiques prévu par la présente proposition de recommandation, y compris les parties pertinentes de son annexe.

Le point 2) précise le champ d'application du schéma directeur pour les infrastructures critiques, qui fait référence à deux types de cas dans lesquels des incidents perturbateurs déclencheraient l'application de ce schéma directeur: soit l'incident a un effet perturbateur important sur la fourniture de services essentiels à ou dans six États membres ou plus, soit il a un effet perturbateur important dans deux États membres ou plus et les acteurs concernés qui y sont mentionnés s'accordent sur la nécessité d'une coordination au niveau de l'Union en raison des conséquences significatives de l'incident.

Le point 3) concerne la détermination des acteurs pertinents qui doivent être associés au schéma directeur pour les infrastructures critiques et les niveaux auxquels ce schéma directeur s'appliquera (opérationnel, stratégique/politique). Ces éléments sont expliqués plus en détail dans l'annexe de la recommandation.

Le point 4) recommande d'appliquer le schéma directeur pour les infrastructures critiques de manière cohérente par rapport aux autres instruments pertinents, ainsi que décrit dans l'annexe.

Le point 5) recommande aux États membres de réagir efficacement, au niveau national, aux perturbations importantes d'infrastructures critiques.

Le point 6) recommande que les acteurs concernés désignent ou mettent en place des points de contact afin de faciliter l'utilisation du schéma directeur pour les infrastructures critiques. Dans la mesure du possible, ces points de contact devraient être les mêmes que les points de contact uniques prévus par la directive CER.

Le point 7) fait référence au flux d'informations en cas d'incident majeur affectant une infrastructure critique.

Le point 8) expose dans le détail comment l'échange d'informations devrait avoir lieu.

Le point 9) recommande de tester le fonctionnement du schéma directeur pour les infrastructures critiques au moyen d'exercices.

Le point 10) recommande que les enseignements tirés soient examinés au sein du groupe sur la résilience des entités critiques, qui devrait préparer un rapport comprenant des recommandations. Il convient que ce rapport soit adopté par la Commission.

Le point 11) recommande aux États membres de débattre du rapport au sein du Conseil.

L'annexe décrit les objectifs, les principes, les principaux acteurs, l'interaction avec les mécanismes de réaction aux crises existants et le fonctionnement du schéma directeur pour les infrastructures critiques avec ses deux modes de coopération: l'échange d'informations et la réponse.

2023/0318 (NLE)

Proposition de

RECOMMANDATION DU CONSEIL

relative à un schéma directeur visant à coordonner au niveau de l'Union la réponse en cas de perturbations des infrastructures critiques ayant une dimension transfrontière notable

(Texte présentant de l'intérêt pour l'EEE)

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment ses articles 114 et 292,

vu la proposition de la Commission européenne,

considérant ce qui suit:

(1) Il est fondamental, pour assurer le bon fonctionnement du marché intérieur et de la société dans son ensemble, de pouvoir compter sur des infrastructures critiques résilientes et des entités critiques résilientes, cruciales pour le maintien de fonctions sociétales ou d'activités économiques vitales, de la santé publique et de la sûreté publique, ou de l'environnement.

(2) Compte tenu de l'évolution actuelle du paysage des risques et à la lumière des interdépendances croissantes entre les infrastructures et les secteurs et, plus généralement, des interconnexions par-delà les secteurs et les frontières, il est nécessaire d'assurer et de renforcer, de manière globale et coordonnée, la protection des infrastructures critiques et la résilience des entités critiques exploitant ces infrastructures.

(3) Un incident qui perturbe des infrastructures critiques et, de ce fait, empêche ou perturbe gravement la fourniture de services essentiels peut avoir des répercussions transfrontières importantes et avoir des conséquences négatives sur le marché intérieur. Afin de garantir une approche ciblée, proportionnée et efficace, il convient de prendre des mesures pour faire face, en particulier, aux incidents majeurs affectant des infrastructures critiques, comme indiqué dans la présente recommandation, en couvrant, par exemple, les situations dans lesquelles les perturbations causées par l'incident sont de longue durée ou peuvent avoir des effets en cascade considérables dans le même secteur ou dans d'autres secteurs ou dans d'autres États membres.

(4) Une réaction coordonnée aux incidents majeurs affectant des infrastructures critiques est essentielle pour éviter des perturbations majeures du marché intérieur et assurer le rétablissement de la fourniture de ces services essentiels dans les meilleurs délais, étant donné que de tels incidents peuvent avoir de graves conséquences sur l'économie et les citoyens de l'Union. Une réponse rapide et efficace au niveau de l'Union à de tels incidents nécessite une coopération rapide et efficace entre tous les acteurs concernés ainsi qu'une action coordonnée soutenue au niveau de l'Union. Une telle

réponse est donc tributaire de l'existence de procédures et de mécanismes de coopération préalablement établis et, dans la mesure du possible, bien éprouvés, dans le cadre desquels des responsabilités et des rôles précis sont assignés aux principaux acteurs aux niveaux national et européen.

(5) Bien qu'il incombe en premier lieu aux États membres et aux entités qui exploitent des infrastructures critiques et fournissent des services essentiels de réagir aux incidents majeurs affectant des infrastructures critiques, une coordination accrue au niveau de l'Union est appropriée en cas de perturbations ayant une dimension transfrontière notable. Une réponse rapide et efficace dépend non seulement du déploiement de mécanismes nationaux par les États membres, mais aussi d'une action coordonnée soutenue au niveau de l'Union, y compris d'une coopération appropriée mise en œuvre de manière rapide et efficace.

(6) La protection des infrastructures critiques européennes est actuellement régie par la directive 2008/114/CE du Conseil[1], qui ne couvre que deux secteurs, à savoir les transports et l'énergie. Ladite directive établit une procédure de recensement et de classement des infrastructures critiques européennes ainsi qu'une approche commune pour évaluer la nécessité d'améliorer leur protection. Elle constitue le pilier central du programme européen de protection des infrastructures critiques[2] (ci-après l'«EPCIP»), adopté par la Commission en 2006, qui a établi, au niveau européen, un cadre «tous risques» pour la protection des infrastructures critiques.

(7) Afin d'aller au-delà de la protection des infrastructures critiques et de garantir, plus largement, la résilience des entités critiques exploitant de telles infrastructures qui fournissent des services essentiels dans le marché intérieur, la directive (UE) 2022/2557 du Parlement européen et du Conseil[3] remplacera la directive 2008/114/CE à partir du 18 octobre 2024. La directive (UE) 2022/2557 couvre onze secteurs et prévoit des obligations d'amélioration de la résilience pour les États membres et les entités critiques, une coopération entre les États membres et avec la Commission, ainsi qu'un soutien de la Commission aux autorités nationales et aux entités critiques et un soutien des États membres aux entités critiques.

(8) À la suite du sabotage des gazoducs Nord Stream, il est nécessaire d'adopter davantage de mesures de renforcement de la résilience des infrastructures critiques au niveau de l'Union. Par conséquent, sur la base d'une proposition de la Commission, le Conseil a adopté une recommandation relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques (la «recommandation 2023/C 20/01»)[4], qui vise à améliorer la préparation, la réaction et la coopération internationale dans ce domaine. Cette recommandation a notamment souligné la nécessité d'assurer, au niveau de l'Union, une réponse coordonnée et efficace face aux risques pesant sur la fourniture de services essentiels.

---

[1] Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection (JO L 345 du 23.12.2008, p. 75).

[2] COM(2006) 786 final du 12 décembre 2006 – Communication de la Commission sur un programme européen de protection des infrastructures critiques.

[3] Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil (JO L 333 du 27.12.2022, p. 164).

[4] Recommandation du Conseil du 8 décembre 2022 relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques (2023/C 20/01) (JO C 20 du 20.1.2023, p. 1).

(9) Il est donc est nécessaire de compléter le cadre juridique existant par une recommandation supplémentaire du Conseil définissant un schéma directeur sur une réponse coordonnée en cas de perturbations des infrastructures critiques ayant une dimension transfrontière notable (ci-après le «schéma directeur pour les infrastructures critiques»), tout en utilisant les dispositifs existants au niveau de l'Union.

(10) La présente recommandation devrait être alignée sur la recommandation 2023/C 20/01 afin de garantir la cohérence et d'éviter les doubles emplois. Par conséquent, la présente recommandation ne devrait pas, en tant que telle, couvrir les autres éléments du cycle de gestion de crise, à savoir la prévention, la préparation et le relèvement.

(11) La présente recommandation devrait compléter la directive (UE) 2022/2557, notamment en ce qui concerne la réponse coordonnée, et devrait être mise en œuvre tout en assurant la cohérence avec ladite directive et toute autre règle applicable du droit de l'Union. Par conséquent, la présente recommandation devrait également s'appuyer sur les notions, outils et processus de ladite directive, tels que le groupe sur la résilience des entités critiques, agissant dans les limites de ses tâches telles que définies dans ladite directive, et les points de contact, et les utiliser, dans la mesure du possible. En outre, la notion d'«infrastructure critique» utilisée dans la présente recommandation devrait s'entendre de la même manière que celle énoncée au considérant 7 de la recommandation 2023/C 20/01, c'est-à-dire comme englobant les infrastructures critiques pertinentes recensées par un État membre au niveau national ou désignées comme infrastructures critiques européennes en vertu de la directive 2008/114/CE ainsi que les entités critiques à recenser au titre de la directive (UE) 2022/2557. Afin d'assurer la cohérence avec la directive (UE) 2022/2557, les notions utilisées dans la présente recommandation devraient donc être interprétées comme ayant la même signification que dans ladite directive. Par exemple, le concept de résilience, tel qu'il est défini à l'article 2, point 2), de ladite directive, devrait aussi s'entendre comme faisant référence à la capacité d'une infrastructure critique à prévenir des événements qui perturbent de manière notable ou sont susceptibles de perturber de manière notable la fourniture de services essentiels sur le marché intérieur, c'est-à-dire de services indispensables pour maintenir les fonctions sociétales et économiques vitales, la sûreté et la sécurité publiques, la santé de la population ou l'environnement, ainsi qu'à s'en protéger, à y réagir, à y résister, à les atténuer, à les absorber, à s'y adapter ou à s'en rétablir

(12) En outre, la notion d'«effet perturbateur important» devrait être interprétée à la lumière des critères prévus à l'article 7, paragraphe 1, de la directive (UE) 2022/2557, qui font référence: i) au nombre d'utilisateurs tributaires du service essentiel fourni par l'entité concernée; ii) à la mesure dans laquelle les autres secteurs et sous-secteurs figurant à l'annexe de la directive dépendent du service essentiel en question; iii) à l'impact que des incidents pourraient avoir, du point de vue de l'ampleur et de la durée, sur les activités économiques et sociétales, l'environnement, la sûreté et la sécurité publiques, ou la santé de la population; iv) à la part de marché de l'entité sur le marché du ou des services essentiels concernés; v) à la zone géographique susceptible d'être affectée par un incident, y compris toute conséquence transfrontière, compte tenu de la vulnérabilité associée au degré d'isolement de certains types de zones géographiques, telles que les régions insulaires, les régions éloignées ou les zones montagneuses; et vi) à l'importance que revêt l'entité pour le maintien d'un niveau suffisant de service essentiel, compte tenu de la disponibilité de solutions de rechange pour la fourniture de ce service essentiel.

(13) Dans un souci d'efficience et d'efficacité, le schéma directeur pour les infrastructures critiques devrait être pleinement cohérent et interopérable avec le protocole opérationnel révisé de l'Union de lutte contre les menaces hybrides[5] et tenir compte du plan d'action pour une réaction coordonnée aux incidents et crises transfrontières de cybersécurité majeurs établi par la recommandation (UE) 2017/1584 de la Commission[6] (ci-après le «plan d'action pour la cybersécurité») et du mandat du réseau européen d'organisations de liaison en cas de crises de cybersécurité (ci-après «UE-CyCLONe») défini dans la directive (UE) 2022/2555 du Parlement européen et du Conseil[7], et éviter la duplication des structures et des activités. Il devrait en outre respecter pleinement le dispositif intégré pour une réaction au niveau politique dans les situations de crise[8] (ci-après l'«IPCR») du Conseil pour coordonner la réponse apportée.

(14) La présente recommandation s'appuie sur les mécanismes existants de gestion de crise à l'échelon de l'Union, tels que le dispositif IPCR du Conseil, le processus interne de coordination des crises de la Commission (ARGUS)[9] et le mécanisme de protection civile de l'Union (le «MPCU»)[10], soutenu par le centre de coordination de la réaction d'urgence («ERCC»)[11], le mécanisme de réaction aux crises du Service européen pour l'action extérieure («SEAE») et l'instrument du marché unique pour les situations d'urgence[12], qui peuvent tous jouer un rôle en cas de perturbation majeure des opérations d'infrastructures critiques, et est, de manière plus générale, cohérente et complémentaire par rapport à ces mécanismes.

(15) Au moment de répondre à un incident majeur affectant une infrastructure critique, les outils ou mécanismes au niveau de l'Union mentionnés ci-dessus peuvent être utilisés, conformément aux règles et procédures qui leur sont applicables, que la présente recommandation devrait compléter sans toutefois y apporter d'altération. Par exemple, le dispositif intégré IPCR du Conseil demeure le principal outil de coordination de la réponse au niveau politique de l'Union entre les États membres. La coordination interne au sein de la Commission s'inscrit dans le cadre du processus intersectoriel ARGUS pour la coordination en cas de crise. Si la crise comporte des implications

---

5 Document de travail conjoint des services, Protocole opérationnel de l'Union européenne de lutte contre les menaces hybrides [SWD(2023) 116 final].

6 Recommandation (UE) 2017/1584 de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs (JO L 239 du 19.9.2017, p. 36).

7 Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (JO L 333 du 27.12.2022, p. 80).

8 Décision d'exécution (UE) 2018/1993 du Conseil du 11 décembre 2018 concernant le dispositif intégré de l'Union européenne pour une réaction au niveau politique dans les situations de crise (JO L 320 du 17.12.2018, p. 28).

9 Communication de la Commission au Parlement européen, au Conseil, Comité économique et social européen et au Comité des régions - Dispositions de la Commission relatives au système général d'alerte rapide «ARGUS» [COM(2005) 662 final].

10 Décision nº 1313/2013/UE du Parlement européen et du Conseil du 17 décembre 2013 relative au mécanisme de protection civile de l'Union (JO L 347 du 20.12.2013, p. 924).

11 La décision nº 1313/2013/UE relative au mécanisme de protection civile de l'Union (MPCU) établit un cadre «tous risques» définissant un dispositif de prévention, de préparation et de réponse visant à gérer toutes sortes de catastrophes naturelles et d'origine humaine ou de catastrophes imminentes à l'intérieur comme à l'extérieur de l'UE.

12 Règlement …/… du Parlement européen et du Conseil établissant un instrument du marché unique pour les situations d'urgence et abrogeant le règlement (CE) nº 2679/98 du Conseil [COM(2022) 459 final].

liées à la politique extérieure ou à la politique de sécurité et de défense commune (PSDC), le mécanisme de réaction aux crises du Service européen pour l'action extérieure (SEAE) peut être utilisé. Conformément à la décision nº 1313/2013/UE relative au mécanisme de protection civile de l'Union (ci-après le «MPCU»), les réponses opérationnelles mises en œuvre au titre du MPCU en cas de catastrophes naturelles et d'origine humaine, réelles ou imminentes, à l'intérieur comme à l'extérieur de l'UE (y compris celles affectant des infrastructures critiques) sont organisées par l'ERCC, la plateforme unique de la Commission, opérationnelle 24 heures sur 24, 7 jours sur 7, qui gère les réponses aux crises. Dans de tels cas, l'ERCC peut assurer une alerte précoce, une notification et une analyse et faciliter le partage d'informations, et, en cas d'activation du MPCU par un État membre, déployer une assistance opérationnelle et des experts dans les zones touchées. Elle peut également faciliter la coordination sectorielle et intersectorielle tant au niveau de l'UE qu'entre l'UE et les autorités nationales compétentes, y compris celles chargées de la protection civile et de la résilience des infrastructures critiques.

(16) Bien qu'il convienne d'envisager les processus prévus dans la présente recommandation, le cas échéant, en relation avec ces autres outils ou mécanismes une fois qu'ils sont utilisés, la présente recommandation devrait également décrire les mesures susceptibles d'être prises au niveau de l'Union en ce qui concerne la connaissance situationnelle partagée, la coordination de la communication publique et l'efficacité de la réponse en dehors de ces mécanismes de coordination de crise de l'Union dans le cas où ils ne seraient pas utilisés.

(17) Afin de mieux coordonner la réponse en cas d'incidents majeurs affectant des infrastructures critiques, il convient de renforcer la coopération entre les États membres et les institutions, organes et organismes compétents de l'Union travaillant dans le cadre des dispositifs existants, conformément au cadre du schéma directeur pour les infrastructures critiques. Le schéma directeur pour les infrastructures critiques devrait par conséquent s'appliquer lorsque le seuil de six États membres ou plus prévu par la directive (UE) 2022/2557 pour le recensement des entités critiques d'importance européenne particulière est atteint, ainsi que lorsque des incidents concernant un plus petit nombre d'États membres ont lieu parce que de tels incidents pourraient avoir des conséquences considérables, en raison d'effets transfrontières en cascade, et que, dès lors, une coordination de la réponse au niveau de l'Union serait bénéfique.

(18) Bien qu'un cadre de coopération au niveau de l'Union pour une réponse coordonnée aux incidents majeurs affectant des infrastructures critiques soit jugé nécessaire, il ne devrait pas détourner les ressources des entités critiques et des autorités compétentes de la gestion des incidents, qui devrait être la priorité.

(19) Les acteurs concernés participant à la mise en œuvre du schéma directeur pour les infrastructures critiques devraient être clairement identifiés de manière à disposer d'une vue d'ensemble claire et complète des institutions, organes, organismes, agences et autorités susceptibles de réagir à un incident majeur affectant des infrastructures critiques.

(20) La réponse aux incidents affectant des infrastructures critiques, y compris majeurs, relève en premier lieu de la responsabilité des autorités compétentes des États membres. La présente recommandation ne devrait pas affecter la responsabilité qui incombe aux États membres en matière de sauvegarde de la sécurité nationale et de la défense ou leur pouvoir de garantir d'autres fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer la sécurité publique, l'intégrité

territoriale et le maintien de l'ordre public conformément au droit de l'Union. En outre, la présente recommandation ne devrait pas avoir d'incidence sur les processus nationaux, tels que la communication et les échanges des exploitants d'infrastructures critiques avec les autorités nationales compétentes. La présente recommandation devrait s'appliquer sans préjudice des accords bilatéraux ou multilatéraux pertinents conclus entre les États membres.

(21) La désignation ou la mise en place de points de contact par les acteurs concernés est essentielle pour une coopération efficace et en temps utile dans le cadre du schéma directeur pour les infrastructures critiques. Dans un souci de cohérence, les États membres devraient envisager la possibilité que les points de contact désignés ou mis en place dans ce cadre soient les mêmes que ceux qui doivent être désignés ou mis en place dans le cadre de la directive (UE) 2022/2557.

(22) Dans un souci d'efficacité, l'expérimentation et la mise en pratique du schéma directeur pour les infrastructures critiques, ainsi que l'établissement de rapports et l'examen des enseignements tirés après son application, devraient constituer un élément essentiel des efforts visant à maintenir un niveau élevé de préparation en cas d'incidents majeurs affectant des infrastructures critiques et à garantir la capacité d'apporter une réponse rapide et bien coordonnée, avec la participation des acteurs concernés.

(23) Compte tenu de la structure du mécanisme du Conseil pour la coordination des crises (IPCR) et, plus généralement, de l'activation potentielle des mécanismes de coordination de crise qui existent déjà au niveau de l'Union, le schéma directeur pour les infrastructures critiques devrait comprendre deux modes de coopération pour réagir à un incident majeur affectant une infrastructure critique. Le premier devrait consister en un échange d'informations associant tous les acteurs concernés, en une coordination de la communication publique et, si de tels mécanismes sont utilisés, en une coordination au moyen de mécanismes déjà existants, tels que le dispositif intégré IPCR au Conseil, le système de coordination ARGUS au sein de la Commission, soutenu par l'ERCC en tant que point de contact opérationnel 24 heures sur 24 et 7 jours sur 7, et le mécanisme de réaction aux crises du SEAE. Le second devrait prévoir des mesures d'intervention plus approfondies pour les incidents de grande ampleur. Cette coopération devrait impliquer un engagement aux niveaux opérationnel et stratégique/politique, reflétant les niveaux figurant dans la recommandation 2017/1584 et dans le protocole de l'Union de lutte contre les menaces hybrides, afin de coordonner les actions et de répondre de manière efficace et efficiente aux incidents majeurs affectant des infrastructures critiques. Sur la base des principes de proportionnalité, de subsidiarité, de confidentialité des informations et de complémentarité, et afin de garantir une coopération efficace, le schéma directeur pour les infrastructures critiques devrait décrire la manière dont les acteurs concernés élaborent une appréciation commune de la situation et prévoir une communication publique coordonnée et une réponse efficace.

(24) L'échange d'informations au titre de la présente recommandation devrait être effectué sans porter atteinte à la sécurité nationale ou à la sécurité et aux intérêts commerciaux des entités exploitant des infrastructures critiques. Dès lors, les informations sensibles devraient être consultées, échangées et traitées avec prudence, conformément aux règles applicables, et en accordant une attention particulière aux canaux de transmission et aux capacités de stockage utilisés,

A ADOPTÉ LA PRÉSENTE RECOMMANDATION:

(1) Les États membres, le Conseil, la Commission et, le cas échéant, le Service européen pour l'action extérieure (ci-après le «SEAE») et les organes, organismes et agences compétents de l'Union devraient coopérer entre eux dans le cadre du schéma directeur pour les infrastructures critiques prévu par la présente recommandation, afin d'atteindre les objectifs énoncés dans la partie I, section 1, de l'annexe, et, eu égard aux principes énoncés dans la partie I, section 2, de l'annexe, d'apporter une réponse coordonnée aux incidents majeurs affectant des infrastructures critiques.

(2) Les États membres, le Conseil, la Commission et, le cas échéant, le SEAE et les organes, organismes et agences compétents de l'Union devraient appliquer le schéma directeur pour les infrastructures critiques dans les meilleurs délais chaque fois qu'un incident majeur affectant une infrastructure critique se produit, c'est-à-dire un incident affectant une infrastructure critique ayant l'un des effets suivants:

   (a) un effet perturbateur important sur la fourniture de services essentiels à ou dans six États membres ou plus, y compris lorsqu'il touche une entité critique d'importance européenne particulière au sens de l'article 17 de la directive (UE) 2022/2557 sur la résilience des entités critiques[13]; ou

   (b) un effet perturbateur important sur la fourniture de services essentiels dans deux États membres ou plus, lorsque l'État membre exerçant la présidence tournante du Conseil, en accord avec ces autres États membres et en consultation avec la Commission, estime qu'une coordination en temps utile des réponses au niveau de l'Union est requise, eu égard aux conséquences vastes et significatives de l'incident sur le plan technique ou politique.

(3) Les acteurs concernés du schéma directeur pour les infrastructures critiques, recensés aux niveaux opérationnel et stratégique/politique conformément à la partie I, section 3, de l'annexe, devraient s'efforcer d'interagir et de coopérer de manière complémentaire. Ils devraient assurer un échange d'informations adéquat et en temps utile, y compris la coordination de la communication publique, et la réponse coordonnée prévue dans la partie II de l'annexe.

(4) Le schéma directeur pour les infrastructures critiques devrait être appliqué en tenant compte des autres instruments pertinents et en cohérence avec ceux-ci, conformément à la partie I, section 4, de l'annexe. Si un incident affecte à la fois les aspects physiques et la cybersécurité des infrastructures critiques, il convient de garantir des synergies avec les processus pertinents mis en place dans le plan d'action pour la cybersécurité.

(5) Les États membres devraient veiller à répondre efficacement, au niveau national et dans le respect du droit de l'Union, aux perturbations des infrastructures critiques faisant suite à des incidents majeurs affectant des infrastructures critiques.

(6) Les États membres, le Conseil, le SEAE, l'Agence de l'Union européenne pour la coopération des services répressifs («Europol») et les autres agences compétentes de l'Union, ainsi que la Commission, devraient désigner ou mettre en place un point de contact pour les questions relatives au schéma directeur pour les infrastructures critiques. Ces points de contact devraient contribuer à l'application du schéma

[13] Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil (JO L 333 du 27.12.2022, p. 164).

directeur pour les infrastructures critiques en fournissant les informations nécessaires et faciliter la mise en œuvre des mesures de coordination adoptées pour répondre à un incident majeur affectant une infrastructure critique. Pour les États membres, dans la mesure du possible, ces points de contact devraient être les mêmes que ceux qui doivent être désignés ou mis en place au titre de l'article 9, paragraphe 2, de la directive (UE) 2022/2557. Pour la Commission, l'ERCC assure les contacts et les capacités opérationnels 24 heures sur 24, 7 jours sur 7, et coordonne, surveille et soutient en temps réel la réaction aux situations d'urgence au niveau de l'Union, tout en servant les États membres et la Commission en tant que plateforme opérationnelle pour la réaction aux crises promouvant une approche intersectorielle de la gestion des catastrophes.

(7) L'État membre exerçant la présidence tournante du Conseil, en accord avec les États membres touchés, devrait informer tous les acteurs concernés, par l'intermédiaire des points de contact visés au point 6), de l'incident majeur affectant une infrastructure critique et de l'application du schéma directeur pour les infrastructures critiques. L'échange d'informations concernant un incident majeur affectant une infrastructure critique devrait être effectué au moyen des canaux de communication appropriés, y compris, le cas échéant et s'il y a lieu, le dispositif intégré pour une réaction au niveau politique dans les situations de crise[14] («IPCR») et l'ERCC par l'intermédiaire du système commun de communication et d'information d'urgence («CECIS»), une application d'alerte et de notification en ligne permettant l'échange d'informations en temps réel.

(8) Si nécessaire, les canaux de transmission devraient inclure des canaux sécurisés afin de ne pas compromettre la sécurité nationale ou la sécurité et les intérêts commerciaux des entités concernées. L'échange d'informations décrit dans la partie II, section 1, de l'annexe de la présente recommandation devrait également être effectué sans compromettre la sécurité nationale ou la sécurité et les intérêts commerciaux des entités critiques et conformément au droit de l'Union, en particulier le règlement (UE) .../... du Parlement européen et du Conseil[15]. En particulier, les informations sensibles devraient être consultées, échangées et traitées avec prudence. Les outils agréés disponibles ainsi que les mesures de sécurité adéquates devraient être utilisés pour le traitement et l'échange d'informations classifiées.

(9) Les acteurs concernés devraient régulièrement mettre en pratique et tester le fonctionnement du schéma directeur pour les infrastructures critiques et leur réponse coordonnée à un incident majeur affectant une infrastructure critique au niveau national, régional et de l'Union, par exemple dans le cadre d'exercices. Ces tests et mises en pratique peuvent faire appel, le cas échéant, à des entités du secteur privé. Un exercice au niveau de l'Union intégrant les aspects physiques et liés au cyberespace devrait être réalisé au plus tard le [*date d'adoption de la présente recommandation + 12 mois*].

(10) Lorsque le schéma directeur pour les infrastructures critiques a été appliqué à la suite d'un incident majeur affectant une infrastructure critique, le groupe sur la résilience des entités critiques visé à l'article 19 de la directive (UE) 2022/2557 devrait examiner

[14] Décision d'exécution (UE) 2018/1993 du Conseil du 11 décembre 2018 concernant le dispositif intégré de l'Union européenne pour une réaction au niveau politique dans les situations de crise, ST/13422/2018/INIT, (JO L 320 du 17.12.2018, p. 28).

[15] Règlement (UE) .../... relatif à la sécurité de l'information dans les institutions, organes et organismes de l'Union [COM(2022) 119 final].

avec les acteurs concernés, en temps utile, les enseignements recensés susceptibles d'indiquer des lacunes et des domaines dans lesquels des améliorations sont nécessaires, et préparer ensuite un rapport contenant des recommandations visant à parvenir à de telles améliorations. Les acteurs associés à la mise en œuvre du schéma directeur pour les infrastructures critiques devraient contribuer à l'élaboration de ce rapport. Il convient que ce rapport soit adopté par la Commission.

(11) Les États membres devraient examiner le rapport visé au point 10) au sein des instances préparatoires compétentes du Conseil ou au sein du Conseil.

Fait à Bruxelles, le

Par le Conseil
Le président