COMMISSION
EUROPÉENNE

Bruxelles, le 18.10.2022
COM(2022) 551 final

2022/0338 (NLE)

Proposition de

RECOMMANDATION DU CONSEIL

relative à une approche coordonnée de l'Union pour renforcer la résilience des infrastructures critiques

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

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Justification et objectifs de la proposition

La sécurité est un objectif fondamental de l'UE. Si la protection des citoyens incombe en premier lieu aux États membres, l'action collective au niveau de l'Union européenne contribue considérablement à la sécurité de l'UE dans son ensemble. La coordination permet de renforcer la résilience, la vigilance et notre réponse collective. Dans le cadre de la stratégie de l'UE pour l'union de la sécurité, des mesures importantes ont été prises, d'une part, pour renforcer les facultés et les capacités de prévention, de détection et de réaction rapide à de nombreuses menaces pour la sécurité, et, d'autre part, pour permettre une synergie entre les acteurs des secteurs public et privé en les ralliant à un effort commun.

Pour être en mesure de faire face à un paysage de menaces en constante évolution, l'UE doit faire preuve d'une vigilance et d'une capacité d'adaptation constantes. La guerre d'agression livrée par la Russie à l'Ukraine a engendré de nouveaux risques, qui se combinent souvent pour former une menace hybride. L'un d'entre eux est le risque de perturbation des services essentiels fournis par les entités exploitant des infrastructures critiques en Europe. Ce risque est devenu encore plus évident avec le sabotage apparent des gazoducs Nord Stream et d'autres incidents récents. La société dépend fortement des infrastructures tant physiques que numériques, et l'interruption de services essentiels, que ce soit à la suite d'attaques physiques conventionnelles, de cyberattaques ou d'une combinaison des deux, peut avoir de graves conséquences sur le bien-être des citoyens, nos économies et la confiance placée dans nos systèmes démocratiques.

Garantir le bon fonctionnement du marché intérieur est un autre objectif fondamental de l'UE, y compris lorsqu'il en va des services essentiels fournis par les entités exploitant des infrastructures critiques. C'est pourquoi l'UE a déjà pris un certain nombre de mesures pour réduire les vulnérabilités et accroître la résilience des entités critiques face aux cyberrisques comme aux risques autres.

Il est urgent d'agir pour renforcer la capacité de l'UE à faire face à d'éventuelles attaques contre des infrastructures critiques, principalement sur son sol, mais aussi, le cas échéant, dans son voisinage direct.

La recommandation du Conseil ici proposée vise à intensifier le soutien de l'UE au renforcement de la résilience des infrastructures critiques et à garantir une coordination de la préparation et de la réaction au niveau de l'UE. Son objectif est de maximiser et d'accélérer les travaux visant à protéger les actifs, installations et systèmes nécessaires au fonctionnement de l'économie et à la fourniture de services essentiels au marché intérieur, dont dépendent les citoyens, ainsi que d'atténuer les effets de toute attaque en permettant un rétablissement le plus rapide possible. S'il est vrai que toutes ces infrastructures devraient être protégées, les secteurs de l'énergie, des infrastructures numériques, des transports et de l'espace revêtent actuellement la plus haute priorité, en raison de leur caractère particulièrement horizontal pour la société et l'économie et au vu des évaluations actuelles des risques.

L'UE a un rôle particulier à jouer en ce qui concerne les infrastructures qui franchissent des frontières terrestres ou maritimes et touchent aux intérêts de plusieurs États membres, ou dont l'objet est de fournir des services essentiels sur une base transfrontière. Les infrastructures critiques d'importance pour plusieurs États membres peuvent toutefois se situer dans un seul État membre, voire en dehors du territoire de ces États membres; c'est, par exemple, le cas des câbles ou des gazoducs sous-marins. Il est dans l'intérêt de tous les États membres et de

l'UE dans son ensemble d'identifier clairement les infrastructures critiques et les entités qui les exploitent, ainsi que les risques auxquelles elles sont exposées, et de s'engager collectivement à protéger ces infrastructures et entités.

Le Parlement européen et le Conseil sont déjà parvenus à un accord politique sur la nécessité d'approfondir le cadre législatif de l'UE afin de contribuer à renforcer la résilience des entités exploitant des infrastructures critiques. À l'été 2022, des accords ont ainsi été trouvés sur la directive sur la résilience des infrastructures critiques («directive CER»)[1] et sur la directive révisée sur la sécurité des réseaux et des systèmes d'information («directive SRI 2»)[2]. Ces deux directives permettront une intensification majeure des capacités par rapport au cadre législatif existant, constitué de la directive 2008/114/CE 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 («directive ICE»)[3] et de la directive (UE) 2016/1148 du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union («directive SRI»)[4]. La nouvelle législation devrait entrer en vigueur fin 2022 ou début 2023, et les États membres devraient accorder la priorité à sa transposition et à sa mise en application, dans le respect du droit de l'Union.

Cela étant, compte tenu de l'urgence potentielle de faire face aux menaces découlant de la guerre d'agression livrée par la Russie à l'Ukraine, les mesures prévues par la nouvelle législation devraient, lorsque cela est possible et approprié, être mises en œuvre dès aujourd'hui. Intensifier la coopération mutuelle dès à présent contribuerait également à créer l'élan nécessaire à une mise en œuvre efficace de la nouvelle législation lorsque celle-ci sera pleinement en vigueur.

L'idée serait d'aller déjà au-delà des cadres actuels, en ce qui concerne tant la profondeur d'action que l'étendue des secteurs couverts. La nouvelle directive CER propose un nouveau cadre de coopération et imposera aux États membres et aux entités critiques des obligations visant à renforcer la résilience physique et non cyber, face aux menaces naturelles et d'origine humaine, de ces entités qui fournissent des services essentiels au marché intérieur, dans onze secteurs donnés[5]. La directive SRI 2 donnera aux obligations en matière de cybersécurité une large couverture sectorielle. À ce titre, les États membres seront notamment tenus d'inclure, s'il y a lieu, les câbles sous-marins dans leur stratégie de cybersécurité.

La législation confère à la Commission un rôle important de coordination. La directive CER prévoit que la Commission joue un rôle de soutien et de facilitation, à exercer avec le soutien et la participation du groupe sur la résilience des entités critiques (CERG) que cette directive institue, et la charge de compléter les activités des États membres en élaborant des bonnes pratiques, des documents d'orientation et des méthodes. En ce qui concerne la cybersécurité, le Conseil, dans les conclusions sur la posture cyber de l'Union européenne qu'il a adoptées à l'été 2022, a déjà invité la Commission, le haut représentant et le groupe de coopération SRI à travailler à des évaluations des risques et des scénarios du point de vue de la cybersécurité. Une telle coordination peut inspirer l'approche à adopter pour d'autres infrastructures critiques essentielles.

---

1 COM(2020) 829 final.
2 COM(2020) 823 final.
3 JO L 345 du 23.12.2008.
4 JO L 194 du 19.7.2016.
5 Énergie, transports, infrastructures numériques, banques, infrastructures des marchés financiers, santé, eau potable, eaux usées, administration publique, espace et alimentation.

Le 5 octobre 2022, la présidente von der Leyen a présenté un plan en cinq points, proposant une approche coordonnée des nécessaires travaux à venir. Ses principaux éléments étaient les suivants: améliorer la préparation; collaborer avec les États membres en vue de soumettre leurs infrastructures critiques à des tests de résistance, en commençant par le secteur de l'énergie, pour continuer avec d'autres secteurs à haut risque; accroître la capacité de réaction, notamment dans le cadre du mécanisme de protection civile de l'Union; utiliser au mieux nos capacités de surveillance satellitaire pour détecter les menaces potentielles; et renforcer la coopération avec l'OTAN et les principaux partenaires en matière de résilience des infrastructures critiques. Le plan en cinq points soulignait tout l'intérêt d'anticiper la législation faisant déjà l'objet d'un accord politique.

La recommandation du Conseil ici proposée salue cette approche pour structurer le soutien aux États membres et coordonner leurs efforts de sensibilisation aux risques, de préparation et de réaction aux menaces actuelles. À cet égard, des réunions d'experts sont convoquées, afin de discuter de la résilience des entités exploitant des infrastructures critiques en anticipation de l'entrée en vigueur de la directive CER et du CERG institué par celle-ci.

En matière de résilience des entités exploitant des infrastructures critiques, il sera essentiel de renforcer la coopération avec les principaux partenaires ainsi qu'avec les pays tiers voisins et d'autres pays tiers concernés, en particulier dans le cadre du dialogue structuré UE-OTAN sur la résilience.

La présente recommandation se concentre sur le renforcement de la capacité de l'Union à anticiper les nouvelles menaces découlant de la guerre d'agression livrée par la Russie à l'Ukraine, à les prévenir et à répondre. Les recommandations formulées ont ainsi pour principale finalité de parer aux risques et aux menaces pour la sécurité des infrastructures critiques. Il convient néanmoins de souligner que des événements récents ont aussi montré qu'il était urgent de prêter davantage attention aux effets du changement climatique sur les infrastructures et services critiques, par exemple au risque que peut représenter un approvisionnement en eau, soumis aux fluctuations saisonnières et imprévisible, qui serait insuffisant pour refroidir les centrales nucléaires, faire tourner les centrales hydroélectriques et permettre la navigation intérieure, ou au risque de dommages matériels aux infrastructures de transport, susceptibles de perturber fortement des services essentiels. Ces problèmes continueront d'être traités dans le cadre de la législation pertinente et de manière coordonnée.

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

La présente proposition de recommandation du Conseil est pleinement conforme au cadre juridique actuel et futur sur la résilience des entités exploitant des infrastructures critiques, à savoir la directive ICE et la directive CER, dans la mesure où elle vise notamment à faciliter la coopération entre les États membres dans ce domaine et à soutenir la mise en œuvre de mesures concrètes pour renforcer la résilience des entités exploitant des infrastructures critiques dans l'UE face aux menaces imminentes auxquelles elles sont actuellement exposées.

En outre, elle anticipe et complète la directive CER en invitant déjà les États membres à accorder la priorité à la transposition en temps voulu de la directive CER, en prévoyant une coopération dans le cadre des réunions d'experts convoquées au titre du plan en cinq points annoncé par la Commission et en prévoyant une coordination en vue d'une approche commune pour la réalisation des tests de résistance sur les infrastructures critiques de l'UE.

La proposition est également conforme à la directive SRI et à la future directive SRI 2, qui abrogera la directive SRI, en appelant à démarrer rapidement les travaux de transposition et de mise en œuvre. Elle reflète aussi l'appel conjoint de Nevers de mars 2022 et les conclusions

du Conseil de mai 2022 sur la posture cyber de l'UE en ce qui concerne la demande adressée par les États membres à la Commission de procéder à des évaluations des risques et à élaborer des scénarios de risque.

La proposition est en outre conforme à la politique de l'UE en matière de protection civile, dans le cadre de laquelle, en cas de perturbation massive du fonctionnement d'infrastructures/entités critiques, les États membres et les pays tiers peuvent demander de l'aide par l'intermédiaire du centre de coordination de la réaction d'urgence (ERCC) dans le cadre du mécanisme de protection civile de l'Union (MPCU). En cas d'activation du MPCU, l'ERCC a la faculté de coordonner et de cofinancer le déploiement, dans le pays touché, des équipements, du matériel et de l'expertise essentiels disponibles dans les États membres (en partie dans le cadre de la réserve européenne de protection civile) et dans le cadre de rescEU. L'assistance qui peut être fournie sur demande comprend, par exemple, du combustible, des générateurs, des infrastructures électriques, des capacités d'hébergement, des capacités d'épuration des eaux usées et des capacités médicales d'urgence.

La proposition est également conforme à l'acquis de l'UE en matière de sécurité de l'approvisionnement énergétique.

Le secteur de l'énergie nucléaire n'est pas spécifiquement inclus dans la recommandation du Conseil proposée, sauf en ce qui concerne des infrastructures liées (par exemple, les lignes de transmission vers les centrales nucléaires) susceptibles d'avoir une incidence sur la sécurité de l'approvisionnement. Les éléments strictement nucléaires relèvent de la réglementation pertinente en matière nucléaire, et notamment du traité Euratom et/ou du droit national[6]. Les enseignements tirés de l'accident de Fukushima ont conduit au renforcement de la législation européenne en matière de sûreté nucléaire; depuis lors, les autorités nationales sont tenues de procéder à des examens périodiques de la sûreté de chaque installation afin de garantir le respect permanent des exigences de sûreté les plus élevées et d'identifier les améliorations supplémentaires à apporter en matière de sûreté, et des examens thématiques par les pairs conduits au niveau de l'UE ont lieu tous les six ans.

La stratégie de sûreté maritime de l'UE[7] et le plan d'action lié[8] soulignent la nature changeante des menaces dans le domaine maritime et appellent à un engagement renouvelé à protéger les infrastructures maritimes critiques, y compris sous-marines, et en particulier les infrastructures maritimes des secteurs des transports, de l'énergie et des communications. Il s'agit notamment de renforcer la surveillance maritime grâce à une meilleure interopérabilité et une rationalisation des échanges d'informations.

La proposition est également conforme aux autres législations sectorielles pertinentes. Sa mise en œuvre devrait dès lors être cohérente avec les mesures spécifiques qui réglementent ou pourraient réglementer à l'avenir certains aspects de la résilience des entités actives dans les secteurs concernés, tels que les transports. Les autres initiatives pertinentes incluent le plan d'urgence pour les transports[9], ainsi que le plan d'urgence visant à garantir l'approvisionnement et la sécurité alimentaires en période de crise[10] et le mécanisme européen de préparation et de réaction aux crises de sécurité alimentaire, qui lui est lié. Plus généralement, la recommandation devrait naturellement être mise en œuvre dans le plein

6 Considérant 9 de la directive 2008/114/CE du Conseil (directive ICE).
7 11205/14.
8 10494/18.
9 COM(2022) 211 final.
10 COM(2021) 689 final.

respect de toutes les règles applicables du droit de l'Union, notamment celles énoncées dans les directives ICE et SRI.

La proposition est également conforme à la boussole stratégique en matière de sécurité et de défense, qui soulignait la nécessité de renforcer considérablement la résilience et la capacité à contrer les menaces hybrides et les cyberattaques, de même que la nécessité de renforcer la résilience des pays partenaires et de coopérer avec l'OTAN. Elle est également conforme au cadre pour une réponse coordonnée de l'UE aux menaces et campagnes hybrides touchant l'UE, ses États membres et ses partenaires[11].

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 (TFUE), qui prévoit le rapprochement des législations en vue de l'amélioration du marché intérieur, ainsi que sur l'article 292 du TFUE. Ce choix se justifie par le fait que la recommandation du Conseil proposée vise principalement à anticiper les mesures prévues dans les nouvelles directives CER et SRI 2, qui sont toutes deux également fondées sur l'article 114 du TFUE. Selon la logique consistant à utiliser cet article comme base juridique de ces directives, une action de l'UE visant à garantir le bon fonctionnement du marché intérieur est nécessaire au regard, notamment, de la nature et de la portée transfrontières des services concernés et des conséquences potentielles de perturbations les affectant, ainsi que des mesures nationales actuelles et émergentes visant à renforcer la résilience des entités exploitant les infrastructures critiques utilisées pour fournir des services essentiels au marché intérieur.

• Subsidiarité (en cas de compétence non exclusive)

En matière de résilience des entités exploitant des infrastructures critiques, il est nécessaire de proposer une voie à suivre au niveau européen compte tenu de la nature interdépendante et transfrontière du fonctionnement des infrastructures critiques et des services essentiels fournis, ainsi que de la nécessité, pour garantir une résilience suffisante des entités concernées dans le contexte géopolitique actuel, d'une approche européenne davantage commune et coordonnée. Si nombre des défis communs, tels que le sabotage apparent des gazoducs North Stream, sont d'abord et avant tout traités au moyen de mesures nationales ou par les entités exploitant des infrastructures critiques, le soutien de l'UE, y compris, s'il y a lieu, par l'intermédiaire de ses agences compétentes, est nécessaire pour accroître la résilience, améliorer la vigilance et renforcer la réponse collective de l'Union.

• 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, puisqu'elles respectent les prérogatives et les obligations des États membres en vertu du droit national.

[11] Conseil de l'Union européenne, 10016/22, 21 juin 2022.

Enfin, s'agissant de la préparation et de la réaction aux menaces physiques sur les infrastructures critiques, la proposition permet une approche potentiellement différenciée selon les réalités internes diverses des 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. Une recommandation du Conseil constitue un instrument approprié en l'espèce, compte tenu également du contexte législatif actuel, tel qu'expliqué ci-dessus. En tant qu'acte juridique, bien que de nature non contraignante, une recommandation du Conseil témoigne de l'engagement des États membres en faveur des mesures prévues et fournit une base politique solide pour la coopération dans les domaines concernés, tout en respectant pleinement l'autorité des États membres.

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

- **Consultation des parties intéressées**

Les avis exprimés par les experts des États membres lors de la réunion du 12 octobre 2022 ont été pris en considération dans l'élaboration de la présente proposition. Un large consensus s'est dégagé quant à l'utilité d'une coordination accrue au niveau de l'Union en ce qui concerne la préparation et la réaction dans le contexte actuel de menace, et quant à l'utilité d'anticiper certains éléments de la directive CER avant son adoption formelle. Les États membres se sont déclarés disposés à partager leurs expériences et leurs bonnes pratiques en matière de mesures et de méthodes pour renforcer la résilience des entités exploitant des infrastructures critiques. Ils se sont également déclarés ouverts à une approche coordonnée pour soumettre les entités exploitant des infrastructures critiques à des tests de résistance conduits à titre volontaire et sur la base de principes communs. Ils ont indiqué que les entités exploitant des infrastructures critiques dans les secteurs de l'énergie, des infrastructures numériques et des transports, notamment celles qui intéressent plusieurs États membres, devraient être considérées comme une priorité aux fins de la présente recommandation. Ils se sont également félicités de l'intention de la Commission de convoquer de nouvelles réunions de leurs experts dans les semaines à venir.

- **Explication détaillée de certaines dispositions de la proposition**

La proposition de recommandation du Conseil prévoit ce qui suit:

– Son chapitre I définit l'objectif de la proposition et son champ d'application et indique les mesures prioritaires recommandées.

– Son chapitre II se concentre sur les mesures qui devraient être prises pour améliorer la préparation, tant au niveau de l'Union qu'au niveau des États membres.

– Son chapitre III traite du renforcement de la réaction, tant au niveau de l'UE qu'au niveau des États membres.

– Son chapitre IV traite de la coopération internationale et des mesures qui devraient être prises pour renforcer la résilience des entités exploitant des infrastructures critiques.

2022/0338 (NLE)

Proposition de

RECOMMANDATION DU CONSEIL

relative à une approche coordonnée de l'Union pour renforcer la résilience des infrastructures critiques

(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) L'Union a un rôle particulier à jouer en ce qui concerne les infrastructures transfrontières qui touchent aux intérêts de plusieurs États membres, ou qui sont exploitées par des entités pour la fourniture de services essentiels sur une base transfrontière. Cette prestation de services et ces infrastructures critiques qui concernent plusieurs États membres peuvent toutefois se situer dans un seul État membre ou en dehors du territoire des États membres; c'est, par exemple, le cas des câbles sous-marins ou des conduites sous-marines. Il est dans l'intérêt de tous les États membres et de l'Union dans son ensemble d'identifier clairement les infrastructures et entités en question, ainsi que les menaces auxquelles elles sont exposées, et de s'engager collectivement à protéger ces infrastructures et entités.

(2) La directive 2008/114/CE du Conseil[12] régit actuellement la protection des infrastructures critiques dans deux secteurs. Cette directive établit une procédure de recensement et de désignation des infrastructures critiques européennes, ainsi qu'une approche commune pour évaluer la nécessité d'améliorer leur protection, afin de contribuer à la protection des personnes. Elle couvre les secteurs de l'énergie et des transports. Afin d'améliorer la résilience des entités critiques, des services essentiels qu'elles fournissent et des infrastructures critiques sur lesquelles elles s'appuient, une nouvelle directive sur la résilience des entités critiques (ci-après la «directive CER»)[13], qui remplacera la directive 2018/114/CE et couvrira un plus grand nombre de secteurs, dont les infrastructures numériques, est en voie d'adoption par le législateur de l'Union.

(3) Une autre directive, la directive (UE) 2016/1148 du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des

[12] 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).

[13] COM(2020) 829 final.

réseaux et des systèmes d'information dans l'Union[14], se concentre en outre sur les menaces liées au cyberespace. Cette directive sera remplacée par une nouvelle directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (ci-après la «directive SRI 2»)[15], qui est également en voie d'adoption par le législateur de l'Union.

(4) Dans un contexte d'évolution rapide du paysage des menaces, marqué notamment par le sabotage apparent des infrastructures gazières Nord Stream 1 et 2, les entités exploitant des infrastructures critiques sont confrontées à des défis particuliers qui éprouvent leur résilience face aux actes hostiles et aux autres menaces d'origine humaine, tandis que les défis liés à des facteurs naturels et au changement climatique se multiplient et peuvent se conjuguer à des actes hostiles. Il est dès lors nécessaire qu'elles prennent, avec le soutien des États membres, des mesures appropriées pour renforcer leur résilience. Il conviendrait que ces mesures et ce soutien aillent au-delà des mesures prévues par les directives 2008/114/CE et (UE) 2016/1148 et soient mis en œuvre avant même l'adoption, l'entrée en vigueur et la transposition des nouvelles directives CER et SRI 2.

(5) Dans l'attente de l'adoption, de l'entrée en vigueur et de la transposition de ces nouvelles directives, l'Union et les États membres sont encouragés à utiliser tous les instruments à leur disposition, conformément au droit de l'Union, pour aller de l'avant et contribuer au renforcement de la résilience physique et de la cyberrésilience des entités concernées et des infrastructures critiques qu'elles exploitent afin de fournir des services essentiels au marché intérieur, c'est-à-dire des services indispensables à la préservation de fonctions sociétales et d'activités économiques vitales, de la santé et de la sécurité publiques, ou de l'environnement. À cet égard, la notion de résilience devrait s'entendre comme désignant la capacité d'une entité à prévenir des événements qui perturbent ou sont susceptibles de perturber sensiblement la fourniture des services essentiels en question, et à s'en protéger, à y réagir, à y résister, à les atténuer, à les absorber, à s'y adapter et à s'en remettre.

(6) Afin de garantir une approche à la fois efficace et aussi cohérente que possible avec la nouvelle directive CER, les mesures contenues dans la présente recommandation devraient concerner toute infrastructure qu'un État membre a désignée comme infrastructure critique – ce qui inclut aussi bien les infrastructures critiques nationales que les infrastructures critiques européennes –, et ce, que l'entité exploitant l'infrastructure critique ait déjà été désignée ou non comme entité critique en vertu de cette nouvelle directive. Aux fins de la présente recommandation, le terme «infrastructure critique» devrait s'entendre dans ce sens.

(7) Au vu des menaces existantes, des mesures de renforcement de la résilience devraient être prises en priorité dans les secteurs clés de l'énergie, des infrastructures numériques, des transports et de l'espace, et elles devraient principalement viser à renforcer la résilience des entités exploitant les infrastructures critiques face aux risques d'origine humaine. En ce qui concerne les infrastructures critiques nationales, compte tenu des conséquences possibles en cas de matérialisation des risques, la priorité devrait être donnée aux infrastructures revêtant une dimension transfrontière.

---

[14] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).

[15] COM(2020) 823 final.

(8) Ainsi, les mesures prévues par la présente recommandation visent principalement à compléter les nouvelles directives CER et SRI 2, fondées sur l'article 114 du traité sur le fonctionnement de l'Union européenne (TFUE), en anticipant et en complétant les mesures qu'elles prévoiront. Par conséquent, et compte tenu de la nature et de l'importance transfrontières des services essentiels et des infrastructures critiques concernés, ainsi que des différences qui existent ou se font jour entre les législations nationales, et qui faussent le marché intérieur, il convient de fonder la présente recommandation non seulement sur l'article 292 du TFUE, mais aussi sur l'article 114 du TFUE.

(9) La mise en œuvre de la présente recommandation ne devrait pas être interprétée comme ayant une incidence sur les exigences actuelles et futures du droit de l'Union concernant certains aspects de la résilience des entités concernées et elle devrait être cohérente avec celles-ci. Ces exigences sont énoncées dans des instruments de portée générale tels que les directives 2008/114/CE et (UE) 2016/1148 et les nouvelles directives CER et SRI 2 appelées à les remplacer, mais aussi dans certains instruments sectoriels, par exemple dans le secteur des transports, où la Commission a notamment pris une initiative concernant un plan d'urgence pour les transports[16]. Conformément au principe de coopération loyale, la présente recommandation devrait être mise en œuvre dans un esprit de plein respect mutuel et de pleine assistance mutuelle.

(10) Le 5 octobre 2022, la Commission a annoncé un plan en cinq points, proposant une approche coordonnée pour relever les défis qui nous attendent. Il s'agit notamment de travailler sur la préparation en s'appuyant sur la nouvelle directive CER, en anticipation de son adoption et de son entrée en vigueur, et de travailler avec les États membres en vue de soumettre les entités exploitant des infrastructures critiques à des tests de résistance basés sur des principes communs, en commençant par le secteur de l'énergie. La présente recommandation, qui contribuera à ce plan, salue l'approche proposée et indique comment la transposer en actes.

(11) Face à l'évolution rapide du paysage des menaces et dans le contexte de risques actuel, caractérisé par la prédominance des risques d'origine humaine, en particulier pour les infrastructures critiques d'importance transfrontière, il est essentiel de disposer d'un tableau précis, à jour et complet des risques les plus importants auxquels sont confrontées les entités exploitant des infrastructures critiques. Les États membres devraient dès lors prendre les mesures nécessaires pour évaluer ces risques ou actualiser leurs évaluations de ces risques. Si la présente recommandation met l'accent sur les risques liés à la sécurité, il convient en outre de poursuivre les efforts visant à lutter contre le changement climatique et les risques environnementaux, en particulier lorsque des événements naturels peuvent encore aggraver les risques d'origine humaine.

(12) Compte tenu de ce paysage de menaces, les États membres devraient être invités à prendre dès que possible, pour renforcer la résilience des infrastructures critiques, les mesures appropriées, y compris celles allant au-delà desdites évaluations des risques, qui seront ultérieurement requises en vertu de la nouvelle directive CER.

(13) Dans le cadre de la mise en œuvre du plan en cinq points annoncé par la Commission, il est nécessaire de coordonner les travaux en réunissant des experts nationaux en anticipation de la création, par la nouvelle directive CER, du groupe sur la résilience des entités critiques, afin de permettre la coopération entre les États membres et

[16] COM(2022) 211 final.

l'échange d'informations concernant la résilience des entités exploitant des infrastructures critiques. Cela devrait inclure la coopération et l'échange d'informations dans le cadre d'activités telles que le recensement des entités et des infrastructures critiques, l'élaboration et la promotion d'un ensemble de principes communs pour réaliser les tests de résistance et en tirer des enseignements communs, et l'identification des vulnérabilités et des moyens mobilisables. Ces processus devraient également conforter la résilience des entités exploitant des infrastructures critiques face aux risques climatiques et environnementaux. Ils permettraient aussi d'établir des priorités communes pour l'organisation des tests de résistance, mettant l'accent sur les secteurs de l'énergie, des infrastructures numériques, des transports et de l'espace. La Commission a déjà entrepris de réunir ces experts et de faciliter leurs travaux, et elle entend poursuivre dans cette voie. Une fois la nouvelle directive CER entrée en vigueur, et le groupe sur la résilience des entités critiques en place, ce travail d'anticipation devrait être poursuivi par ce groupe conformément aux missions que lui assigne la directive CER.

(14) L'exercice des tests de résistance devrait être complété par la production d'un schéma directeur (*blueprint*) sur les incidents et les crises pouvant affecter les infrastructures critiques, qui définisse et décrive les objectifs et les modalités de la coopération entre les États membres et les institutions, organes et organismes de l'UE dans la réponse apportée aux incidents touchant des infrastructures critiques, en particulier lorsque ceux-ci entraînent des perturbations majeures de la fourniture de services essentiels pour le marché intérieur. Ce schéma directeur devrait s'appuyer sur le dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR) en vue de coordonner cette réponse, il devrait fonctionner en cohérence et en complémentarité avec le plan d'action sur les cyberincidents majeurs et il devrait aussi prévoir un accord sur les messages clés de communication à adresser au public, étant donné le rôle important que joue la communication de crise dans l'atténuation des effets négatifs des incidents et des crises affectant les infrastructures critiques.

(15) Pour que la réponse apportée aux menaces actuelles et anticipées soit coordonnée et efficace, la Commission apportera un soutien supplémentaire aux États membres en vue de renforcer la résilience face à ces menaces, notamment en leur fournissant des informations pertinentes sous la forme de notes d'information, de manuels et de lignes directrices, en encourageant le lancement de projets de recherche et d'innovation financés par l'Union, en prenant les mesures d'anticipation nécessaires et en optimisant l'utilisation des moyens de surveillance de l'Union. Le SEAE, en particulier par l'intermédiaire du Centre de situation et du renseignement de l'UE, devrait fournir des évaluations des menaces.

(16) Les agences de l'Union compétentes dans les secteurs concernés et les autres organismes compétents devraient également apporter un soutien sur les questions de résilience, dans la mesure où leurs mandats respectifs, tels qu'ils sont définis dans les instruments pertinents du droit de l'Union, le permettent. En particulier, l'Agence de l'Union européenne pour la cybersécurité (ENISA) pourrait apporter son aide sur les questions de cybersécurité, l'Agence européenne pour la sécurité maritime (AESM) pourrait mettre l'expertise de son service de surveillance maritime au service des États membres sur les questions de sûreté et de sécurité maritimes et l'Agence de l'Union européenne pour la coopération des services répressifs (EUROPOL) pourrait contribuer à la collecte d'informations et aux enquêtes dans le cadre d'actions répressives transnationales, tandis que l'Agence de l'Union européenne pour le programme spatial (EUSPA) et le Centre satellitaire de l'Union européenne (CSUE)

pourraient fournir une assistance dans le cadre d'opérations menées au titre du programme spatial de l'Union.

(17) Si la responsabilité première d'assurer la sécurité des infrastructures critiques et des entités concernées incombe aux États membres, une coordination accrue au niveau de l'Union est particulièrement appropriée au regard notamment des menaces susceptibles d'impacter plusieurs États membres à la fois, telles que la guerre d'agression menée par la Russie contre l'Ukraine, ou de porter atteinte à la résilience et au bon fonctionnement de l'économie, du marché unique et des sociétés de l'Union.

(18) La présente recommandation ne prévoit pas la fourniture d'informations dont la divulgation serait contraire aux intérêts essentiels des États membres en matière de sécurité nationale, de sécurité publique ou de défense.

(19) Étant donné l'interdépendance croissante des infrastructures physiques et numériques, les actes de cybermalveillance ciblant des domaines critiques peuvent perturber ou endommager des infrastructures physiques, tandis que le sabotage d'infrastructures physiques peut rendre des services numériques inaccessibles. Compte tenu de la menace accrue que représentent les attaques hybrides sophistiquées, les États membres devraient aussi prendre ces considérations en compte lors de la mise en œuvre de la présente recommandation. Compte tenu des liens qui existent entre la cybersécurité et la sécurité physique des opérateurs, il importe que les préparatifs nécessaires à la transposition et à l'application de la nouvelle directive SRI 2 débutent dès que possible et que ceux relatifs à la nouvelle directive CER avancent aussi en parallèle.

(20) Outre l'amélioration de la préparation, il importe également de renforcer les moyens permettant de répondre rapidement et efficacement à une matérialisation des risques qui pèsent sur la fourniture de services essentiels par des entités exploitant des infrastructures critiques. La présente recommandation devrait dès lors prévoir les mesures à prendre tant au niveau des États membres qu'au niveau de l'Union, y compris le renforcement de la coopération et de l'échange d'informations dans le cadre du mécanisme de protection civile de l'Union et l'utilisation des moyens pertinents du programme spatial de l'Union.

(21) À la suite de l'invitation formulée par le Conseil dans ses conclusions sur la posture cyber de l'Union européenne[17], la Commission, le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité (ci-après le «haut représentant») et le groupe de coopération institué par la directive (UE) 2016/1148 (ci-après le «groupe de coopération SRI»), en coordination avec les organismes et agences civils et militaires compétents et les réseaux établis, y compris UE-CyCLONe, ont entrepris d'évaluer les risques et d'élaborer des scénarios de risque du point de vue de la cybersécurité, pour les situations de menace ou d'attaque éventuelle contre des États membres ou des pays partenaires. Cet exercice se concentre sur les secteurs critiques tels que l'énergie, les infrastructures numériques, les transports et l'espace.

(22) L'appel ministériel conjoint de Nevers[18] et les conclusions du Conseil sur la posture cyber de l'Union européenne appelaient également à renforcer la résilience des infrastructures et réseaux de communication de l'Union sur la base d'une évaluation des risques, et adressaient à cet effet des recommandations aux États membres et à la

[17] Posture cyber: le Conseil approuve des conclusions – Consilium (europa.eu)

[18] https://www.regeringen.se/494477/contentassets/e5f13bec9b1140038eed9a3d0646f8cf/joint-call-to-reinforce-the-eus-cybersecurity-capabilities.pdf

Commission. Cette évaluation des risques est actuellement conduite par le groupe de coopération SRI, avec le soutien de la Commission et de l'ENISA et en coopération avec l'Organe des régulateurs européens des communications électroniques (ORECE). L'évaluation des risques et l'analyse des lacunes examinent les risques de cyberattaques dans les différents sous-secteurs des infrastructures de communication (infrastructures de téléphonie fixe et mobile, satellites, câbles sous-marins, routage internet, etc.) et constitueront ainsi une base pour les travaux conduits au titre de la présente recommandation. Cette évaluation des risques sera une source d'informations pour les travaux en cours d'évaluation intersectorielle des cyberrisques et d'élaboration de scénarios demandés par le Conseil dans ses conclusions du 23 mai 2022.

(23) Ces deux exercices seront cohérents et coordonnés avec l'exercice d'élaboration de scénarios axés sur la protection civile dans le contexte d'un large éventail de catastrophes naturelles ou d'origine humaine, incluant les événements de cybersécurité et leur impact dans la vie réelle, actuellement mené par la Commission et les États membres au titre de la décision nº 1313/2013/UE du Parlement européen et du Conseil[19]. Dans un souci d'efficience, d'efficacité et de cohérence, il conviendrait de mettre en œuvre la présente recommandation en tenant compte des résultats de ces exercices.

(24) La boîte à outils de l'UE pour la cybersécurité des réseaux 5G[20] prévoit des mesures et des plans d'atténuation pertinents pour renforcer la sécurité des réseaux 5G. Étant donné la dépendance de nombreux services essentiels à l'égard des réseaux 5G et la nature interconnectée des écosystèmes numériques, il est essentiel que tous les États membres mettent en œuvre d'urgence les mesures recommandées dans la boîte à outils et, en particulier, appliquent les restrictions pertinentes aux fournisseurs à haut risque pour les actifs essentiels définis comme critiques et sensibles dans l'évaluation coordonnée des risques au niveau de l'UE.

(25) Afin de renforcer immédiatement la préparation et les capacités de réaction à des cyberincidents majeurs, la Commission a mis en place un programme à court terme pour soutenir les États membres, aux fins duquel un financement supplémentaire a été alloué à l'ENISA. Les services fournis comprendront des mesures de préparation, telles que des tests de pénétration des entités critiques afin d'en identifier les vulnérabilités. Les possibilités d'aide aux États membres en cas d'incident majeur touchant des entités critiques seront également renforcées. Il s'agit d'une première étape conforme aux conclusions du Conseil sur la posture cyber, qui invitaient la Commission à présenter une proposition relative à un fonds d'intervention d'urgence en matière de cybersécurité. Les États membres devraient tirer pleinement parti de ces possibilités, dans le respect des exigences applicables.

(26) Le réseau mondial de câbles sous-marins par lesquels transitent les données et les communications électroniques est essentiel à la connectivité mondiale et intra-UE. En raison de la longueur considérable de ces câbles et de leur installation sur les fonds marins, la surveillance visuelle sous-marine de la plupart des sections de câbles est extrêmement difficile. La compétence partagée et d'autres questions juridictionnelles concernant ces câbles plaident tout particulièrement pour une coopération européenne

---

19 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).

20 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf

et internationale en matière de protection et de restauration des infrastructures. C'est pourquoi il est nécessaire de compléter les évaluations de risques en cours et prévues pour les infrastructures numériques et physiques sur lesquels reposent les services numériques par des évaluations de risques et des options de mesures d'atténuation particulières pour les câbles sous-marins. La Commission réalisera donc des études à cet effet et communiquera ses conclusions aux États membres.

(27) Les secteurs de l'énergie et des transports, identifiés comme prioritaires dans la présente recommandation, peuvent également être impactés par les risques liés aux infrastructures numériques. Par exemple, les technologies énergétiques intégrant des composants numériques peuvent être touchées. La sécurité des filières associées est importante pour la continuité des services essentiels et pour le contrôle stratégique des infrastructures critiques exploitées par les entités du secteur de l'énergie. Il conviendrait d'en tenir compte lors de l'adoption de mesures visant à renforcer la résilience des entités exploitant des infrastructures critiques conformément à la présente recommandation.

(28) Compte tenu de l'importance croissante des infrastructures spatiales et des services spatiaux pour les activités de sécurité, il est essentiel de garantir la résilience et la protection des actifs et services spatiaux de l'Union en son sein, mais aussi, dans le cadre de la présente recommandation, d'utiliser de manière plus structurée les données et services fournis par les systèmes et programmes spatiaux pour surveiller et protéger les infrastructures critiques dans d'autres secteurs. La stratégie spatiale de l'UE pour la sécurité et la défense qui sera présentée prochainement proposera des mesures appropriées à cet égard, qui devraient être prises en compte lors de la mise en œuvre de la présente recommandation.

(29) Il est également nécessaire de coopérer au niveau international pour parer efficacement aux risques éprouvant la résilience des entités exploitant des infrastructures critiques, que ce soit dans l'Union, dans des pays tiers ou dans les eaux internationales. Les États membres devraient, par conséquent, être invités à coopérer avec la Commission et le haut représentant, afin que des mesures soient prises à cet effet, étant entendu que ces mesures ne devraient être prises que conformément aux missions et aux responsabilités de chacun en vertu du droit de l'Union, notamment les dispositions des traités de l'UE relatives aux relations extérieures.

(30) Comme elle l'a indiqué dans sa communication intitulée «Contribution de la Commission à la défense européenne»[21], à l'appui de la «Boussole stratégique en matière de sécurité et de défense – Pour une Union européenne qui protège ses citoyens, ses valeurs et ses intérêts, et qui contribue à la paix et à la sécurité internationales»[22], la Commission évaluera, en coopération avec le haut représentant et les États membres, les exigences de base sectorielles en matière de résilience face aux menaces hybrides, en identifiant les lacunes et les besoins ainsi que les mesures à prendre pour y répondre d'ici à 2023. En contribuant à renforcer le partage d'informations et la coordination des actions, cette initiative devrait éclairer les travaux menés au titre de la présente recommandation en vue de renforcer encore la résilience, notamment, des infrastructures critiques.

(31) La stratégie de sûreté maritime de l'UE de 2014 et le plan d'action corollaire préconisaient une protection accrue des infrastructures maritimes critiques, y compris

21 COM(2022) 60 final.

22 Conseil de l'Union européenne, 7371/22, 21 mars 2022.

sous-marines, et en particulier des infrastructures maritimes des secteurs des transports, de l'énergie et des communications. Il s'agissait notamment de renforcer la surveillance maritime grâce à une meilleure interopérabilité et à une rationalisation des échanges d'informations (obligatoires et volontaires). Cette stratégie et ce plan d'action sont en cours d'actualisation, et leur version actualisée prévoira des mesures renforcées pour protéger les infrastructures maritimes critiques. Ces mesures devraient éclairer et compléter le contenu de la présente recommandation.

(32) Les États membres devraient exploiter tout le potentiel du programme de recherche de l'Union en matière de sécurité, notamment en mettant à profit la priorité spécifique qu'il accorde aux infrastructures critiques, en particulier dans le cadre des programmes financés par le Fonds pour la sécurité intérieure, ainsi que des autres possibilités de financement qui peuvent exister au niveau de l'Union, notamment le Fonds européen de développement régional, pour autant que les mesures concernées satisfassent à ses critères d'éligibilité. REPowerEU peut également offrir des possibilités de financement de la résilience. Tout recours aux possibilités de financement offertes par l'Union doit se faire dans le respect des exigences légales applicables.

A ADOPTÉ LA PRÉSENTE RECOMMANDATION:

CHAPITRE I: OBJECTIF, CHAMP D'APPLICATION ET HIÉRARCHISATION DES PRIORITÉS

(1) La présente recommandation invite les États membres à prendre d'urgence des mesures effectives et à coopérer de manière loyale, efficace, solidaire et coordonnée entre eux et avec la Commission et les autres autorités publiques concernées, ainsi qu'avec les entités concernées, pour renforcer la résilience des infrastructures critiques qui servent à fournir des services essentiels au sein du marché intérieur.

(2) Les mesures décrites dans la présente recommandation concernent toute infrastructure désignée par un État membre comme étant une infrastructure critique, y compris comme étant une infrastructure critique européenne.

(3) Lors de la mise en œuvre de la présente recommandation, la priorité devrait être de renforcer la résilience des entités opérant dans les secteurs de l'énergie, des infrastructures numériques, des transports et de l'espace, et la résilience des infrastructures critiques que ces entités exploitent et qui ont une importance transfrontière, face aux risques d'origine humaine.

CHAPITRE II RENFORCEMENT DE LA PRÉPARATION

Mesures à prendre au niveau des États membres

(4) Les États membres sont invités à effectuer ou à actualiser leur évaluation des risques concernant la résilience des entités exploitant des infrastructures critiques européennes désignées, conformément à la directive 2008/114/CE, dans les secteurs des transports et de l'énergie, et à coopérer les uns avec les autres sur ces évaluations de risques et sur les mesures de renforcement de la résilience qui en découlent, en tant que de besoin et conformément à ladite directive.

(5) En outre, et afin de permettre aux entités exploitant des infrastructures critiques d'atteindre un niveau élevé de résilience, les États membres devraient accélérer leurs préparatifs pour transposer et appliquer dès que possible la nouvelle directive CER:

(a) en accélérant l'adoption ou la mise à jour de stratégies nationales visant à renforcer la résilience des entités exploitant des infrastructures critiques, en vue de répondre à la menace actuelle. Les principaux éléments de ces stratégies devraient être communiqués à la Commission;

(b) en effectuant ou en actualisant l'évaluation des risques au regard du caractère évolutif des menaces actuelles, en ce qui concerne la résilience des entités qui exploitent des infrastructures critiques dans des secteurs pertinents autres que l'énergie, les infrastructures numériques, les transports et l'espace et, si possible, dans les secteurs relevant de la nouvelle directive CER, à savoir les banques, les infrastructures des marchés financiers, les infrastructures numériques, la santé, l'eau potable, les eaux usées, l'administration publique, l'espace, et la production, la transformation et la distribution de denrées alimentaires, compte tenu de la nature potentiellement hybride des menaces en question, y compris des effets en cascade et des effets du changement climatique;

(c) en informant la Commission des types de risques identifiés par secteur et sous-secteur et des résultats des évaluations de risques, ce qui pourrait être fait au moyen d'un modèle de déclaration commun mis au point par la Commission en coopération avec les États membres;

(d) en accélérant le processus d'identification et de désignation des entités critiques, la priorité allant aux entités critiques:

(e) qui utilisent des infrastructures critiques qui connectent physiquement deux États membres ou plus;

(f) qui font partie de structures d'entreprise connectées ou liées à des entités critiques situées dans d'autres États membres;

(g) qui ont été identifiées comme telles dans un État membre et fournissent des services essentiels dans ou à six États membres ou plus, et qui revêtent donc une importance européenne particulière, et en en informant la Commission;

(h) en coopérant mutuellement, en particulier en ce qui concerne les entités critiques et les services essentiels et infrastructures critiques d'importance transfrontière, notamment en se consultant mutuellement aux fins du point 5 d) et en s'informant mutuellement de tout incident aux effets transfrontières perturbateurs significatifs ou potentiellement significatifs, tout en tenant la Commission dûment informée;

(i) en renforçant leur soutien aux entités critiques désignées afin d'en améliorer la résilience, ce qui peut inclure la mise à disposition de documents d'orientation et de méthodes, l'organisation d'exercices visant à tester leur résilience, la fourniture de conseils et la formation de leur personnel, et en leur permettant de vérifier les antécédents des personnes qui jouent un rôle sensible, conformément à la législation de l'Union et à la législation nationale, dans le cadre des mesures qu'elles prennent pour gérer la sécurité au niveau de leur personnel;

(j) accélérer la désignation ou la création, au sein de l'autorité compétente, d'un point de contact unique chargé d'exercer une fonction de liaison avec les points de contact uniques des autres États membres aux fins de la coopération transfrontière en matière de résilience des entités exploitant des infrastructures critiques.

(6) Les États membres sont encouragés à soumettre les entités exploitant des infrastructures critiques à des tests de résistance. En particulier, ils sont invités à accélérer leur préparation, ainsi que celle des entités concernées, dans le secteur de

l'énergie et à réaliser dans ce secteur des tests de résistance, si possible selon des principes définis d'un commun accord au niveau de l'Union, tout en veillant à communiquer efficacement avec ces entités. Des tests de résistance pourraient être envisagés ultérieurement, en fonction des besoins, dans d'autres secteurs prioritaires, à savoir les infrastructures numériques, les transports et l'espace, en tenant dûment compte des inspections menées dans les sous-secteurs aérien et maritime conformément au droit de l'Union, et en tenant compte des dispositions pertinentes de la législation sectorielle.

(7) Les États membres sont invités à coopérer avec les pays tiers concernés, lorsque cela est opportun et conformément au droit de l'Union, en matière de résilience des entités exploitant des infrastructures critiques qui revêtent une importance transfrontière.

(8) Pour renforcer la résilience des entités exploitant des infrastructures critiques dans l'Union, y compris, par exemple, le long des réseaux transeuropéens, face à tout l'éventail des menaces importantes, les États membres sont invités à utiliser, dans le respect des exigences applicables, les possibilités de financement qui peuvent exister au niveau de l'Union et au niveau national, notamment dans le cadre des programmes financés par le Fonds pour la sécurité intérieure et le Fonds européen de développement régional, sous réserve du respect des critères d'éligibilité respectifs, et dans le cadre du mécanisme pour l'interconnexion en Europe, notamment des dispositions sur l'adaptation au changement climatique. Les financements du mécanisme de protection civile de l'Union peuvent aussi être utilisés à cette fin, conformément aux exigences applicables, en particulier pour des projets portant sur l'évaluation des risques, les plans ou études d'investissement, le renforcement des capacités ou l'amélioration de la base de connaissances. REPowerEU peut également offrir des possibilités de financement de la résilience.

(9) En ce qui concerne les infrastructures de communication et de réseaux dans l'Union, le groupe de coopération SRI devrait, dans le respect de l'article 11 de la directive (UE) 2016/1148, puis de l'article 14 de la directive SRI 2, accélérer ses travaux en cours sur une évaluation ciblée des risques, et présenter ses premières recommandations début 2023. Il devrait mener ces travaux en veillant à leur cohérence et à leur complémentarité avec ceux de son groupe de travail ad hoc sur la sécurité de la chaîne d'approvisionnement des technologies de l'information et de la communication, et les travaux d'autres groupes concernés, comme le groupe sur la résilience des entités critiques prévu par la nouvelle directive CER et le forum de supervision prévu par le nouveau règlement sur la résilience opérationnelle numérique du secteur financier (DORA)[23].

(10) Le groupe de coopération SRI, qui doit exercer ses tâches conformément à l'article 11 de la directive (UE) 2016/1148 puis à l'article 14 de la directive SRI 2, est invité à travailler en priorité, avec le soutien de la Commission et de l'ENISA, sur la sécurité du secteur des infrastructures numériques et du secteur spatial, notamment en définissant des orientations stratégiques et des méthodes et mesures de gestion des risques en matière de cybersécurité, selon une approche «tous risques», pour les câbles de communication sous-marins, en prévision de l'entrée en vigueur de la directive SRI 2, et sur la définition, à l'intention des opérateurs du secteur spatial, d'orientations pour les mesures de gestion des risques en matière de cybersécurité,

[23] COM(2020) 595 final.

afin d'accroître la résilience des infrastructures terrestres dont dépendent les services spatiaux.

(11) Les États membres devraient pleinement profiter des services de préparation en matière de cybersécurité offerts par le programme de soutien à court terme que la Commission met en œuvre avec l'ENISA, notamment des tests de pénétration destinés à détecter les vulnérabilités, et ils sont encouragés, dans ce contexte, à donner la priorité aux entités qui exploitent des infrastructures critiques dans les secteurs de l'énergie, des infrastructures numériques et des transports.

(12) Les États membres devraient d'urgence finir de mettre en œuvre les mesures recommandées dans la boîte à outils de l'UE sur la cybersécurité des réseaux 5G[24]. Les États membres qui n'ont pas encore imposé de restrictions visant les fournisseurs à haut risque devraient le faire sans plus tarder, tout retard risquant d'accroître la vulnérabilité des réseaux dans l'Union. Ils devraient aussi renforcer la protection physique et immatérielle des parties critiques et sensibles des réseaux 5G, y compris au moyen de contrôles d'accès stricts. En outre, les États membres devraient, en coopération avec la Commission, examiner la nécessité de mesures complémentaires, incluant l'imposition de règles légalement contraignantes au niveau de l'Union, afin de garantir un niveau uniforme de sécurité et de résilience des réseaux 5G.

(13) Les États membres devraient mettre en œuvre dès que possible le code de réseau pour le volet cybersécurité des flux d'électricité transfrontières, en s'appuyant sur l'expérience acquise avec la mise en œuvre de la directive SRI et sur les orientations définies en la matière par le groupe de coopération SRI, en particulier dans son document «Reference document on security measures for Operators of Essential Services».

(14) Les États membres devraient développer l'utilisation de Galileo et/ou de Copernicus à des fins de surveillance et partager leurs informations au sein des groupes d'experts convoqués conformément au point 15. Il conviendrait de mettre à profit les moyens qu'offre le système de communications gouvernementales par satellite (GOVSATCOM) créé dans le cadre du programme spatial de l'Union pour surveiller les infrastructures critiques et aider à faire face aux crises.

Mesures à prendre au niveau de l'Union

(15) La Commission entend renforcer la coopération entre les experts des États membres afin de contribuer au renforcement de la résilience physique, autre que cyber, des entités qui exploitent des infrastructures critiques, notamment:

(a) en préparant la mise au point et la promotion d'outils communs, comprenant des méthodes et des scénarios de risques, pour aider les États membres à renforcer cette résilience;

(b) en soutenant la définition de principes communs pour la réalisation par les États membres des tests de résistance visés au point 6, qui commenceront par des tests sur les risques d'origine humaine dans le secteur de l'énergie, puis dans d'autres secteurs clés comme les infrastructures numériques, les transports et l'espace; en se penchant sur d'autres risques et aléas majeurs; et, le cas échéant, en apportant son soutien et ses conseils sur la conduite de ces tests de résistance.

[24] 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf

(c) en fournissant une plateforme sécurisée permettant de rassembler, d'analyser et de partager les bonnes pratiques, les enseignements tirés des expériences nationales et d'autres informations relatives à cette forme de résilience, notamment sur la réalisation de ces tests de résistance et la traduction de leurs résultats en protocoles et en plans d'urgence.

Les travaux de ces experts devraient accorder une attention particulière aux dépendances transsectorielles et aux entités exploitant des infrastructures critiques d'importance transfrontière, et ils devraient être poursuivis par le groupe sur la résilience des entités critiques, dès qu'il aura vu le jour.

(16) Les États membres devraient participer pleinement à la coopération renforcée mentionnée au point 15, notamment en nommant des points de contact disposant de l'expertise nécessaire et en partageant leur expérience des méthodes utilisées pour les tests de résistance, ainsi que les protocoles et les plans d'urgence élaborés sur cette base. Cet échange d'informations devra préserver la confidentialité des informations concernées ainsi que la sécurité et les intérêts commerciaux des entités critiques, tout en respectant la sécurité des États membres. Il n'implique pas la fourniture d'informations dont la divulgation est contraire aux intérêts essentiels des États membres en matière de sécurité nationale, de sécurité publique ou de défense.

(17) La Commission épaulera les États membres en leur fournissant des manuels et des lignes directrices, par exemple un manuel sur la protection des infrastructures critiques et des espaces publics contre les systèmes d'aéronefs sans pilote, ainsi que des outils d'évaluation des risques. Le SEAE est invité à organiser, en particulier par l'intermédiaire du Centre de situation et du renseignement de l'UE (INTCEN) et de sa cellule de fusion contre les menaces hybrides (HFC), des séances d'information sur les menaces qui pèsent sur les infrastructures critiques de l'UE, afin d'améliorer l'appréciation qu'on peut porter sur une situation donnée.

(18) La Commission soutiendra la diffusion des résultats des projets sur la résilience des entités exploitant des infrastructures critiques financés par les programmes de recherche et d'innovation de l'Union. Elle a l'intention d'augmenter les financements consacrés à cette résilience dans le cadre du budget alloué à Horizon Europe au titre du cadre financier pluriannuel 2021-2027. Cela devrait permettre de faire face aux défis actuels et à venir dans ce domaine, tels que l'adaptation des infrastructures critiques au changement climatique, sans nuire au financement des autres projets de recherche et d'innovation en matière de sécurité civile dépendant d'Horizon Europe. La Commission intensifiera également ses efforts pour diffuser les résultats des projets de recherche pertinents financés par l'Union.

(19) Le groupe de coopération SRI est invité à intensifier, en coopération avec la Commission et le haut représentant, et dans le respect des missions et responsabilités assignées à chacun par le droit de l'Union, les travaux menés avec les réseaux et les organismes civils et militaires concernés en vue d'évaluer les risques et d'élaborer des scénarios de risques en matière de cybersécurité, en mettant l'accent, dans un premier temps, sur l'énergie, les communications, les transports et les infrastructures spatiales, ainsi que sur les interdépendances entre secteurs et entre États membres. Cet exercice devrait tenir compte des risques corollaires pour les infrastructures physiques dont dépendent ces secteurs. Les évaluations des risques et les scénarios de risques devraient avoir lieu régulièrement, s'appuyer sur les évaluations des risques existantes ou prévues dans ces secteurs, en les complétant et en évitant de les répéter, et éclairer les discussions sur la manière de renforcer la résilience globale des

entités exploitant des infrastructures critiques et de remédier aux vulnérabilités constatées.

(20) La Commission va accélérer ses activités d'aide à la préparation des États membres et à la réponse aux incidents de cybersécurité majeurs; elle va notamment:

(a) réaliser, en complément des évaluations de risques pertinentes dans le contexte de la sécurité des réseaux et de l'information, une étude complète dressant l'état des lieux de l'infrastructure de câbles sous-marins qui relie les États membres entre eux, et l'Europe au reste du monde, avec une cartographie de cette infrastructure, indiquant ses capacités et ses doublons, ses vulnérabilités, les risques en termes de disponibilité des services et les possibilités d'atténuation des risques. Les résultats devraient être communiqués aux États membres;

(b) soutenir la préparation des États membres et la capacité de réponse des institutions, organes et agences de l'UE (EUIBA) à des incidents de cybersécurité majeurs.

(21) La Commission intensifiera ses travaux sur des mesures d'anticipation à visée prospective, notamment dans le cadre du MPCU, en collaborant avec les États membres au titre des articles 6 et 10 de la décision nº 1313/2013/UE, et sous la forme d'une planification d'urgence destinée à soutenir la préparation opérationnelle du centre de coordination de la réaction d'urgence.

En particulier, la Commission s'engage:

(a) à poursuivre les travaux entrepris dans le cadre du centre de coordination de la réaction d'urgence sur l'anticipation et la planification transsectorielle des mesures de prévention, de préparation et de réaction, afin d'anticiper les perturbations de la fourniture de services essentiels par les entités exploitant des infrastructures critiques et de s'y préparer;

(b) à accroître les investissements dans des approches préventives et dans la préparation de la population à de telles perturbations, en mettant particulièrement l'accent sur les agents et explosifs chimiques, biologiques, radiologiques et nucléaires ou sur d'autres menaces émergentes d'origine humaine;

(c) à renforcer l'échange de connaissances et de bonnes pratiques dans ces domaines et à améliorer la conception et le déroulement des activités de développement des capacités, telles que les cours de formation et les exercices organisés avec les entités exploitant des infrastructures critiques, en utilisant les structures et l'expertise existantes, comme le réseau européen de connaissances en matière de protection civile.

(22) La Commission encouragera l'utilisation des moyens de surveillance de l'UE (Copernicus et Galileo) pour aider les États membres à surveiller leurs infrastructures critiques et, le cas échéant, leur voisinage immédiat, et pour soutenir d'autres options de surveillance prévues dans le programme spatial de l'Union.

(23) S'il y a lieu, et conformément à leurs mandats respectifs, les agences et autres organes de l'Union concernés sont invités à apporter leur soutien sur les questions relatives à la résilience des entités exploitant des infrastructures critiques; sont notamment concernées, par exemple:

(a) EUROPOL, pour la collecte d'informations, l'analyse de la criminalité et le soutien aux enquêtes menées dans le cadre d'actions répressives transfrontières;

(b) l'AESM, pour les questions de sécurité et de sûreté du secteur maritime de l'Union, y compris les services de surveillance maritime pour les questions liées à la sûreté et à la sûreté maritimes;

(c) l'EUSPA, pour les activités relevant du programme spatial de l'Union;

(d) l'ENISA, pour les activités en rapport avec la cybersécurité.

CHAPITRE III RENFORCEMENT DE LA RÉACTION

Mesures à prendre au niveau des États membres

(24) Les États membres devraient:

(a) coordonner leur réaction et conserver une vision d'ensemble des réactions transsectorielles aux perturbations majeures de la fourniture de services essentiels par des entités exploitant des infrastructures critiques, dans le cadre du mécanisme de gestion de crise du Conseil (IPCR), pour les infrastructures critiques ayant une dimension transfrontière, dans le cadre du schéma directeur sur les incidents et crises de cybersécurité majeurs ou, en cas de campagnes hybrides, au sein du cadre pour une réponse coordonnée de l'UE aux campagnes hybrides;

(b) accroître les échanges d'informations dans le cadre du mécanisme de protection civile de l'Union, afin de favoriser le lancement d'alertes précoces et de coordonner leur réaction au sein de ce mécanisme en cas de perturbations majeures de cet ordre, de manière à réagir plus rapidement, avec l'appui de l'Union, lorsque cela est nécessaire;

(c) accroître leur capacité à réagir, grâce au mécanisme de protection civile de l'Union, à de telles perturbations majeures, en particulier si elles sont susceptibles d'avoir d'importantes implications transfrontières, voire paneuropéennes, et des implications transsectorielles;

(d) travailler avec la Commission à la poursuite du développement de capacités de réaction adaptées dans le cadre de la réserve européenne de protection civile (ECPP) et de rescEU;

(e) inviter les entités exploitant des infrastructures critiques et les autorités nationales compétentes à renforcer la capacité de ces entités à rétablir rapidement un service minimum, dans le cas de services essentiels;

(f) veiller à ce que, lorsqu'il est nécessaire de reconstruire des infrastructures critiques, les infrastructures reconstruites puissent résister à tout l'éventail des risques majeurs auxquels elles peuvent être exposées, y compris dans des scénarios climatiques défavorables.

(25) Les États membres sont invités à accélérer leurs travaux préparatoires en vue de la transposition et de l'application de la directive SRI 2, en commençant immédiatement à renforcer les capacités des centres nationaux de réponse aux incidents de sécurité informatique (CSIRT) au vu des nouvelles tâches confiées à ces centres et du nombre accru d'entités opérant dans de nouveaux secteurs, en actualisant rapidement leurs stratégies de cybersécurité et en adoptant dès que possible des plans nationaux de réponse aux incidents et aux crises en matière de cybersécurité.

Mesures à prendre au niveau de l'Union

(26) La réponse apportée aux perturbations majeures de la fourniture de services essentiels par des entités exploitant des infrastructures critiques devrait être coordonnée entre les experts des États membres, pour ce qui est de la résilience de ces entités et des réponses à ces perturbations qui seraient susceptibles de contribuer au fonctionnement du mécanisme de gestion de crise du Conseil (IPCR).

(27) La Commission coopérera étroitement avec les États membres pour continuer à développer des capacités de réaction d'urgence déployables, incluant des experts et des réserves rescEU dans le cadre du MPCU, en vue d'améliorer la capacité opérationnelle à faire face aux effets immédiats et indirects de perturbations majeures de la fourniture de services essentiels par les entités exploitant des infrastructures critiques.

(28) Compte tenu de l'évolution du paysage des risques, et en coopération avec les États membres, la Commission, dans le cadre du MPCU:

(a) analysera et testera en continu l'adéquation et l'état de préparation opérationnelle des capacités de réaction existantes;

(b) réexaminera régulièrement la nécessité éventuelle de développer de nouvelles capacités de réaction au niveau de l'UE par l'intermédiaire de rescEU;

(c) intensifiera encore la collaboration transsectorielle afin de garantir une réponse adéquate au niveau de l'UE, et organisera régulièrement des exercices pour tester cette collaboration;

(d) continuera de développer l'ERCC, en tant que plateforme transsectorielle de crise au niveau de l'UE pour la coordination du soutien aux États membres touchés.

(29) La Commission, en coopération avec le haut représentant, en concertation étroite avec les États membres, et avec le soutien des agences de l'Union concernées, élaborera un schéma directeur sur les incidents et les crises pouvant affecter les infrastructures critiques, qui définira et décrira les objectifs et les modalités de la coopération entre les États membres et les institutions, organes et organismes de l'UE dans le cadre de la réaction aux incidents touchant des infrastructures critiques, en particulier lorsque ceux-ci entraînent des perturbations majeures de la fourniture de services essentiels pour le marché intérieur. Ce schéma directeur devrait s'appuyer sur l'actuel dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR) pour coordonner la réponse apportée.

(30) La Commission collaborera avec les parties prenantes et les experts pour définir les mesures de rétablissement après incident qu'il serait possible de prendre en ce qui concerne les infrastructures de câbles sous-marins, mesures qu'elle présentera en même temps que l'étude visant à dresser un état des lieux visée au point 20 a), et pour poursuivre la définition des plans d'urgence et des scénarios de risques et les travaux menés sur la résilience de l'Union face aux catastrophes dans le cadre du mécanisme de protection civile de l'Union.

CHAPITRE IV: COOPÉRATION INTERNATIONALE

(31) S'il y a lieu, et dans le respect des missions et responsabilités qui leur sont respectivement assignées par le droit de l'Union, la Commission et le haut représentant aideront les pays partenaires à renforcer la résilience des entités qui exploitent des infrastructures critiques sur leur territoire.

(32) Dans le respect des missions et responsabilités qui leur sont respectivement assignées par le droit de l'Union, la Commission et le haut représentant renforceront la coordination avec l'OTAN en ce qui concerne la résilience des infrastructures critiques, dans le cadre du dialogue structuré UE-OTAN sur la résilience, et créeront une task force à cet effet.

(33) Les États membres sont invités à contribuer, en coopération avec la Commission et le haut représentant, à accélérer l'élaboration et la mise en œuvre de la boîte à outils hybride de l'UE, ainsi que des lignes directrices sur la mise en œuvre prévues dans les conclusions du Conseil sur un cadre pour une réponse coordonnée de l'UE aux campagnes hybrides[25], et à les utiliser ensuite pour donner pleinement effet à ce cadre, en particulier lorsqu'il s'agira de prévoir et d'élaborer des réponses globales et coordonnées de l'UE aux campagnes hybrides et aux menaces hybrides, notamment celles visant des entités qui exploitent des infrastructures critiques.

(34) La Commission envisagera, le cas échéant, et s'il y a lieu, une participation de représentants de pays tiers dans le cadre de la coopération et de l'échange d'informations entre experts des États membres sur la résilience des entités exploitant des infrastructures critiques.

[…]

Fait à Bruxelles, le

Par le Conseil
Le président

25 https://www.consilium.europa.eu/fr/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/