Conseil de
l'Union européenne

Bruxelles, le 9 décembre 2022
(OR. en)

15623/22

Dossier interinstitutionnel:
2022/0338(NLE)

PROCIV 149	**ATO 102**
ENV 1248	**CSC 561**
JAI 1617	**ECOFIN 1279**
SAN 650	**CSCI 189**
COSI 315	**DATAPROTECT 346**
CHIMIE 100	**MI 912**
ENFOPOL 619	**CODEC 1916**
RECH 645	**COPS 581**
CT 220	**JAIEX 103**
DENLEG 93	**COPEN 430**
COTER 297	**IND 533**
RELEX 1657	**POLMIL 297**
ENER 654	**IPCR 116**
HYBRID 116	**DIGIT 231**
TRANS 768	**DISINFO 102**
CYBER 397	**CSDP/PSDC 848**
TELECOM 512	**MARE 71**
ESPACE 125	**POLMAR 78**

RÉSULTATS DES TRAVAUX

Origine:	Secrétariat général du Conseil
Destinataire:	délégations
Nº doc. préc.:	13713/22, 15454/22
Objet:	RECOMMANDATION DU CONSEIL relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques

Les délégations trouveront en annexe la recommandation du Conseil relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques, adoptée par le Conseil lors de sa 3920e session, tenue le 8 décembre 2022.

ANNEXE

RECOMMANDATION (UE) 2022/… DU CONSEIL

du …

relative à une approche coordonnée à l'échelle 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 son article 114, et son article 292, première et deuxième phrases,

vu la proposition de la Commission européenne,

considérant ce qui suit:

(1) Dans le but de garantir le bon fonctionnement du marché intérieur, il est dans l'intérêt de tous les États membres et de l'Union dans son ensemble de recenser clairement et de protéger les infrastructures critiques pertinentes qui fournissent des services essentiels sur ce marché, en particulier dans des secteurs clés, tels que l'énergie, les infrastructures numériques, les transports et l'espace, ainsi que les infrastructures critiques ayant une dimension transfrontière notable[1], dont les perturbations pourraient avoir une incidence considérable sur d'autres États membres.

[1] Les États membres devraient évaluer cette pertinence conformément à leurs pratiques nationales et peuvent le faire en se fondant, entre autres facteurs, sur une évaluation des risques, ainsi que sur l'incidence et la nature de l'événement.

(2) La présente recommandation, qui constitue un acte non contraignant, témoigne de la volonté politique des États membres de coopérer et de leur engagement en faveur des mesures recommandées, soulignés dans un plan en cinq points présenté par la présidente de la Commission européenne, dans le plein respect de la compétence des États membres. La présente recommandation ne porte pas atteinte à la protection des intérêts essentiels relatifs à la sécurité nationale, à la sécurité publique ou à la défense des États membres, et on ne devrait attendre d'aucun État membre qu'il partage des informations préjudiciables à ces intérêts.

(3) Si c'est aux États membres et à leurs opérateurs d'infrastructures critiques qu'incombe au premier chef la responsabilité d'assurer la sécurité et la fourniture des services essentiels par les infrastructures critiques, une coordination accrue au niveau de l'Union s'impose, en particulier au regard des menaces évolutives susceptibles de toucher plusieurs États membres en même temps, telles que la guerre d'agression de la Russie contre l'Ukraine et les campagnes hybrides menées contre les États membres, ou de porter atteinte à la résilience et au bon fonctionnement de l'économie, du marché intérieur et de l'ensemble de la société de l'Union. Il convient d'accorder une attention particulière aux infrastructures critiques situées en dehors du territoire des États membres, telles que les infrastructures critiques sous-marines ou les infrastructures énergétiques en mer.

(4) Dans ses conclusions des 20 et 21 octobre 2022, le Conseil européen a fermement condamné les actes de sabotage commis contre des infrastructures critiques, tels que ceux visant les gazoducs Nord Stream, soulignant que l'Union répondrait de manière unie et déterminée à toute perturbation délibérée d'infrastructures critiques ou à toute autre action hybride.

(5) Compte tenu de l'évolution rapide du paysage des menaces, des mesures visant à renforcer la résilience devraient être prises en priorité dans des secteurs clés, tels que l'énergie, les infrastructures numériques, les transports et l'espace, et dans d'autres secteurs pertinents définis par les États membres. Ces mesures devraient être axées sur le renforcement de la résilience des infrastructures critiques, compte tenu des risques pertinents, en particulier des effets en cascade, des perturbations des chaînes d'approvisionnement, des dépendances, des effets du changement climatique, des fournisseurs et partenaires peu fiables et des menaces et campagnes hybrides, y compris des activités de manipulation de l'information et d'ingérence menées depuis l'étranger. En ce qui concerne les infrastructures critiques nationales, compte tenu des conséquences possibles, il convient d'accorder la priorité aux infrastructures critiques ayant une dimension transfrontière notable. Les États membres sont encouragés à prévoir d'urgence, le cas échéant, de telles mesures de renforcement de la résilience, tout en maintenant l'approche définie dans le cadre juridique en évolution.

(6) La protection des infrastructures critiques européennes dans les secteurs de l'énergie et des transports est actuellement régie par la directive 2008/114/CE du Conseil[2], et la sécurité des réseaux et des systèmes d'information dans l'Union, axée sur les cybermenaces, est régie par la directive (UE) 2016/1148 du Parlement européen et du Conseil[3]. Afin d'assurer un niveau commun plus élevé de résilience et de protection des infrastructures critiques, en matière de cybersécurité et en ce qui concerne le marché financier, le cadre juridique existant est actuellement modifié et complété par l'adoption de nouvelles règles applicables aux entités critiques ("directive CER"), de règles renforcées destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union ("directive SRI 2") et de nouvelles règles applicables à la résilience opérationnelle numérique du secteur financier ("DORA").

(7) Les États membres devraient, conformément au droit de l'Union et au droit national, utiliser tous les instruments à leur disposition pour progresser et contribuer au renforcement de la résilience physique et de la cyberrésilience. À cet égard, par infrastructures critiques, il convient d'entendre 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 et les entités critiques à recenser en vertu de la directive CER ou, le cas échéant, les entités relevant de la directive SRI 2. Le concept de résilience devrait 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 remettre.

[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) 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).

(8) Des experts nationaux devraient se réunir pour coordonner les travaux afin de parvenir à un niveau commun plus élevé de résilience et de protection des infrastructures critiques devant être introduit au moyen des nouvelles règles applicables aux entités critiques. Ces travaux coordonnés permettraient une coopération entre les États membres ainsi que le partage d'informations concernant des activités telles que l'élaboration de méthodes visant à recenser les services essentiels fournis par les infrastructures critiques. La Commission a déjà commencé à réunir ces experts et à faciliter leurs travaux, et elle entend poursuivre dans cette voie. Une fois la directive CER entrée en vigueur et un groupe sur la résilience des entités critiques mis en place au titre de cette directive, ce travail d'anticipation devrait être poursuivi par ledit groupe, conformément à ses tâches.

(9) Compte tenu de l'évolution du paysage des menaces, il convient de développer les possibilités d'effectuer des tests de résistance des infrastructures critiques au niveau national, étant donné que de tels tests pourraient être utiles pour renforcer la résilience des infrastructures critiques. Au regard de l'importance particulière que revêt le secteur de l'énergie et des répercussions de ses éventuelles perturbations à l'échelle de l'Union, ledit secteur pourrait tirer le plus grand profit de la réalisation de tests de résistance sur la base de principes arrêtés d'un commun accord. Ces tests relèvent de la compétence des États membres, et ces derniers devraient encourager et aider les opérateurs des infrastructures critiques à effectuer de tels tests lorsqu'ils sont jugés bénéfiques et conformes à leurs cadres juridiques nationaux.

(10) Afin d'assurer une réaction coordonnée et efficace face aux menaces actuelles et anticipées, la Commission est encouragée à apporter un soutien supplémentaire aux États membres, notamment en leur fournissant des informations pertinentes sous la forme de documents d'information et de manuels et lignes directrices non contraignants. Le Service européen pour l'action extérieure (SEAE), en particulier par l'intermédiaire du Centre de situation et du renseignement de l'UE et de sa cellule de fusion contre les menaces hybrides, avec le soutien de la direction "Renseignement" de l'état-major de l'Union européenne (EMUE) dans le cadre de la capacité unique d'analyse du renseignement (SIAC), devrait fournir des évaluations des menaces. La Commission est également invitée, en coopération avec les États membres, à encourager le lancement de projets de recherche et d'innovation financés par l'Union.

(11) Compte tenu de l'interdépendance croissante des infrastructures physiques et numériques, il se peut que des actes de cybermalveillance ciblant des domaines critiques aient pour conséquence de perturber ou d'endommager des infrastructures physiques ou que le sabotage d'infrastructures physiques rende des services numériques inaccessibles. Les États membres sont invités à accélérer les travaux préparatoires en vue de la transposition et de l'application du nouveau cadre juridique applicable aux entités critiques et du cadre juridique renforcé en matière de cybersécurité, en s'appuyant sur l'expérience acquise au sein du groupe de coopération institué par la directive (UE) 2016/1148 (ci-après dénommé "groupe de coopération SRI"), dès que possible, tout en gardant à l'esprit les délais de transposition et le fait que ces travaux préparatoires devraient progresser en parallèle et de manière cohérente.

(12) Il importe non seulement d'améliorer la préparation, mais également de renforcer les capacités permettant de réagir rapidement et efficacement face à une perturbation des services essentiels fournis par les infrastructures critiques. Dès lors, la présente recommandation contient des mesures tant au niveau de l'Union qu'au niveau national, y compris en soulignant le rôle de soutien et la valeur ajoutée qui peuvent découler de la mise en place d'une coopération et d'un échange d'informations accrus dans le cadre du mécanisme de protection civile de l'Union (MPCU) établi par la décision nº 1313/2013/UE du Parlement européen et du Conseil[4] et en utilisant des moyens pertinents du programme spatial de l'Union établi en vertu du règlement (UE) 2021/696 du Parlement européen et du Conseil[5].

(13) La Commission, le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité (ci-après dénommé "haut représentant") et le groupe de coopération SRI, en coopération avec les organes et organismes civils et militaires compétents et des réseaux en place, y compris le réseau européen d'organisations de liaison en cas de crises de cybersécurité (UE-CyCLONe), doivent procéder à une évaluation des risques et élaborer des scénarios de risques. En outre, dans le prolongement de l'appel ministériel conjoint de Nevers, une évaluation des risques est actuellement effectuée par le groupe de coopération SRI, avec le soutien de la Commission et de l'Agence de l'Union européenne pour la cybersécurité (ENISA) et en coopération avec l'Organe des régulateurs européens des communications électroniques (ORECE). Ces deux exercices seront cohérents et coordonnés avec l'exercice d'élaboration de scénarios dans le cadre du MPCU, englobant les événements de cybersécurité et leur impact dans la vie réelle, actuellement mis au point par la Commission et les États membres. Dans un souci d'efficience, d'efficacité et de cohérence et en vue de la bonne application de la présente recommandation, les résultats de ces exercices devraient être pris en compte au niveau national.

---

4 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).

5 Règlement (UE) 2021/696 du Parlement européen et du Conseil du 28 avril 2021 établissant le programme spatial de l'Union et l'Agence de l'Union européenne pour le programme spatial et abrogeant les règlements (UE) nº 912/2010, (UE) nº 1285/2013 et (UE) nº 377/2014 et la décision nº 541/2014/UE (JO L 170 du 12.5.2021, p. 69)..

(14) Afin de renforcer immédiatement la préparation et la capacité de réaction à un incident de cybersécurité majeur, la Commission a mis en place un programme à court terme pour soutenir les États membres, au moyen d'un financement supplémentaire alloué à l'ENISA. Les services proposés comprennent, entre autres, des actions de préparation, telles que des tests de pénétration des entités destinés à détecter les vulnérabilités. Le programme peut également renforcer les possibilités de soutien aux États membres en cas d'incident de cybersécurité majeur touchant des entités critiques. Il s'agit d'une première étape s'inscrivant dans le prolongement des conclusions du Conseil du 23 mai 2022 sur la mise en place d'une posture cyber de l'Union européenne (ci-après dénommées "conclusions du Conseil sur la posture cyber de l'UE"), dans lesquelles le Conseil a invité 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, et sont encouragés à poursuivre leurs travaux dans le domaine de la gestion des crises de cybersécurité au niveau de l'Union, notamment en assurant le suivi et en faisant le bilan de manière régulière des progrès réalisés dans la mise en œuvre de la feuille de route pour la gestion des crises de cybersécurité récemment élaborée au sein du Conseil. Cette feuille de route est un document évolutif, qui devrait être révisé et mis à jour, en tant que de besoin.

(15) Les câbles de communication sous-marins mondiaux sont essentiels à la connectivité mondiale et intra-UE. En raison de la longueur considérable de tels 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 de compétence en lien avec de tels câbles constituent un argument spécifique en faveur de la coopération européenne et internationale en matière de protection et de restauration des infrastructures. C'est pourquoi il est nécessaire de compléter les évaluations des risques en cours et prévues concernant les infrastructures numériques et physiques sur lesquelles s'appuient les services numériques par des évaluations des risques et des options de mesures d'atténuation spécifiques concernant les câbles de communication sous-marins. Les États membres invitent la Commission à réaliser des études à cet effet et à communiquer ses conclusions aux États membres.

(16) Les secteurs de l'énergie et des transports peuvent également être touchés par des menaces liées aux infrastructures numériques, par exemple en lien avec les technologies énergétiques intégrant des composants numériques. La sécurité des chaînes d'approvisionnement associées est importante pour la continuité de la fourniture de services essentiels et pour le contrôle stratégique des infrastructures critiques dans le secteur de l'énergie. Il convient de tenir compte de ces aspects lors de l'adoption de mesures visant à renforcer la résilience des infrastructures critiques conformément à la présente recommandation.

(17) Compte tenu de l'importance croissante que revêtent les infrastructures spatiales, les moyens au sol liés au secteur spatial, y compris les installations de production, et les services spatiaux pour les activités en matière de sécurité, il est essentiel d'assurer la résilience et la protection du secteur spatial de l'Union et de ses moyens et services terrestres au sein de l'Union. Pour les mêmes raisons, il est également essentiel, dans le cadre de la présente recommandation, d'utiliser de manière plus structurée les données et services spatiaux, qui sont fournis par les systèmes et programmes spatiaux pour la surveillance et le suivi ainsi que pour la protection des infrastructures critiques dans d'autres secteurs. La future stratégie spatiale de l'UE pour la sécurité et la défense proposera des mesures appropriées à cet égard, qui devraient être prises en compte lors de la mise en œuvre de la présente recommandation.

(18) Il est également nécessaire de coopérer au niveau international afin de faire face efficacement aux risques pesant sur les infrastructures critiques, entre autres dans les eaux internationales. Dès lors, les États membres sont invités à coopérer avec la Commission et le haut représentant pour prendre des mesures en vue de mettre en œuvre une telle coopération, étant entendu que de telles mesures ne seront prises que dans le respect de leurs missions et responsabilités respectives en vertu du droit de l'Union, notamment des dispositions des traités relatives aux relations extérieures.

(19) Conformément à sa communication du 15 février 2022 intitulée "Contribution de la Commission à la défense européenne", 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, 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 recensant les lacunes et les besoins ainsi que les mesures à prendre pour y remédier d'ici 2023. En contribuant à renforcer le partage d'informations et la coordination des actions, cette initiative devrait venir alimenter les travaux menés au titre de la présente recommandation en vue de renforcer encore la résilience, notamment celle des infrastructures critiques.

(20) La stratégie de sûreté maritime de l'UE de 2014 et son plan d'action révisé préconisaient de renforcer la protection des infrastructures maritimes critiques, y compris sous-marines, et en particulier des infrastructures maritimes des secteurs des transports, de l'énergie et des communications, entre autres en améliorant l'appréciation de la situation maritime grâce à une plus grande interopérabilité et à un échange (obligatoire et volontaire) d'informations rationalisé. Cette stratégie et ce plan d'action sont en cours de mise à jour et comprendront des actions renforcées visant à protéger les infrastructures maritimes critiques. Ces actions devraient venir compléter la présente recommandation.

(21) Le renforcement de la résilience des infrastructures critiques contribue aux efforts plus larges déployés pour lutter contre les menaces et campagnes hybrides à l'encontre de l'Union et de ses États membres. La présente recommandation s'inscrit dans le prolongement de la communication conjointe au Parlement européen et au Conseil intitulée "Cadre commun en matière de lutte contre les menaces hybrides – une réponse de l'Union européenne". L'action n° 1 de ce cadre commun, à savoir l'étude sur les risques hybrides, joue un rôle clé dans le recensement des vulnérabilités susceptibles d'affecter les structures et les réseaux nationaux et paneuropéens. En outre, la mise en œuvre des conclusions du Conseil du 21 juin 2022 sur un cadre pour une réponse coordonnée de l'UE aux campagnes hybrides permettra de mener une action coordonnée renforcée grâce à l'application de la boîte à outils hybride de l'UE dans tous les domaines touchés.

A ADOPTÉ LA PRÉSENTE RECOMMANDATION:

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

(1) La présente recommandation définit une série d'actions ciblées au niveau de l'Union et au niveau national pour soutenir et renforcer la résilience des infrastructures critiques, sur une base volontaire, en mettant l'accent sur les infrastructures critiques ayant une dimension transfrontière notable et relevant de secteurs clés identifiés, tels que l'énergie, les infrastructures numériques, les transports et l'espace. Ces actions ciblées portent sur le renforcement de la préparation et de la réaction, ainsi que sur la coopération internationale.

(2) Les informations partagées en vue d'atteindre les objectifs de la présente recommandation, qui sont confidentielles en application de la réglementation nationale ou de l'Union, ainsi que des règles applicables au secret des affaires, ne devraient faire l'objet d'un échange avec la Commission et d'autres autorités concernées que si cet échange est nécessaire à la bonne application de la présente recommandation. La présente recommandation ne porte pas atteinte à la protection des intérêts essentiels relatifs à la sécurité nationale, à la sécurité publique ou à la défense des États membres, et on ne devrait attendre d'aucun État membre qu'il partage des informations contraires à ces intérêts.

CHAPITRE II: RENFORCEMENT DE LA PRÉPARATION

Mesures à prendre au niveau des États membres

(3) Les États membres devraient envisager une approche "tous risques" lorsqu'ils mettent à jour leur évaluation des risques ou leurs analyses équivalentes existantes, au regard du caractère évolutif des menaces pesant actuellement sur leurs infrastructures critiques, notamment dans les secteurs clés identifiés et, si possible, dans tous les secteurs couverts par le nouveau cadre juridique applicable aux entités critiques qui est en préparation.

(4) Les États membres sont invités à accélérer leurs travaux préparatoires et à adopter des mesures de renforcement de la résilience, si possible, comme le prévoit le cadre juridique applicable aux entités critiques qui est en préparation, en mettant particulièrement l'accent sur la coopération et le partage d'informations pertinentes entre les États membres et avec la Commission, sur le recensement des entités critiques ayant une dimension transfrontière notable, ainsi que sur le renforcement du soutien aux entités critiques recensées, afin d'améliorer leur résilience.

(5) Les États membres devraient soutenir la formation des experts et les exercices ainsi que le partage des meilleures pratiques et des enseignements tirés de leurs expériences respectives. Ils devraient encourager les experts à participer aux plateformes de formation existantes, tant nationales qu'internationales, par exemple dans le cadre du MPCU.

(6) Les États membres devraient encourager les opérateurs des infrastructures critiques, au moins dans le secteur de l'énergie, à effectuer des tests de résistance, selon des principes définis d'un commun accord au niveau de l'Union, lorsque cela s'avère utile, et leur apporter un soutien à cet égard. Les tests de résistance devraient évaluer la résilience des infrastructures critiques face à des menaces antagonistes d'origine humaine. Par conséquent, les États membres devraient s'efforcer de recenser les infrastructures critiques qu'il convient de tester et de consulter les opérateurs d'infrastructures critiques concernés dès que possible, et au plus tard d'ici la fin du premier trimestre de 2023. De plus, les États membres devraient soutenir les opérateurs des infrastructures critiques afin qu'ils procèdent à ces tests dès que possible et s'efforcent de les achever au plus tard d'ici la fin de 2023, conformément au droit national. Le Conseil a l'intention d'évaluer l'état d'avancement des tests de résistance d'ici la fin du mois d'avril 2023.

(7) Eu égard à l'évolution rapide des menaces qui pèsent sur les infrastructures critiques, il est d'une importance capitale de continuer d'en assurer la protection à un niveau élevé. Les États membres sont encouragés à allouer des ressources financières suffisantes pour renforcer les capacités de leurs autorités nationales compétentes, et à les soutenir, afin d'être en mesure de renforcer la résilience des infrastructures critiques. Ils sont également incités à allouer des ressources financières suffisantes aux autorités chargées de la gestion des incidents de cybersécurité majeurs, à les soutenir et à veiller à ce que leurs centres de réponse aux incidents de sécurité informatique (CSIRT) et leurs autorités compétentes soient pleinement mobilisés dans le cadre du réseau et du réseau des CSIRT et du réseau UE-CyCLONe, respectivement.

(8) Les États membres sont invités à utiliser eux-mêmes, dans le respect des exigences applicables, les possibilités de financement qui peuvent exister au niveau de l'Union et au niveau national pour renforcer la résilience des infrastructures critiques dans l'Union, mais aussi à encourager les opérateurs d'infrastructures critiques à utiliser ces possibilités de financement, y compris, par exemple, en lien avec les réseaux transeuropéens, face à tout l'éventail des menaces importantes, en particulier dans le cadre des programmes financés au titre du Fonds pour la sécurité intérieure établi par le règlement (UE) 2021/1149 du Parlement européen et du Conseil[6], au titre du Fonds européen de développement régional établi par le règlement (UE) n° 1301/2013 du Parlement européen et du Conseil[7], du MPCU et du plan REPowerEU de la Commission. Les États membres sont également encouragés à tirer le meilleur parti des résultats des projets pertinents développés dans le cadre de programmes de recherche, tels qu'Horizon Europe, établi par le règlement (UE) 2021/695 du Parlement européen et du Conseil[8].

---

6 Règlement (UE) 2021/1149 du Parlement européen et du Conseil du 7 juillet 2021 établissant le Fonds pour la sécurité intérieure (JO L 251 du 15.7.2021, p. 94).

7 Règlement (UE) nº 1301/2013 du Parlement européen et du Conseil du 17 décembre 2013 relatif au Fonds européen de développement régional et aux dispositions particulières relatives à l'objectif "Investissement pour la croissance et l'emploi", et abrogeant le règlement (CE) nº 1080/2006 (JO L 347 du 20.12.2013, p. 289).

8 Règlement (UE) 2021/695 du Parlement européen et du Conseil du 28 avril 2021 portant établissement du programme-cadre pour la recherche et l'innovation "Horizon Europe" et définissant ses règles de participation et de diffusion, et abrogeant les règlements (UE) nº 1290/2013 et (UE) nº 1291/2013 (JO L 170 du 12.5.2021, p. 1).

(9) En ce qui concerne les infrastructures de communication et de réseaux dans l'Union, le groupe de coopération SRI est invité, tout en agissant dans le respect de l'article 11 de la directive (UE) 2016/1148, à accélérer ses travaux en cours fondés sur l'appel ministériel conjoint de Nevers en ce qui concerne une évaluation ciblée des risques, et il devrait présenter ses premières recommandations dès que possible. Cette évaluation des risques devrait fournir des informations visant à contribuer à l'évaluation intersectorielle des risques cyber, actuellement en cours, et aux scénarios demandés par le Conseil dans ses conclusions sur la posture cyber de l'UE. De plus, ces travaux devraient être menés en veillant à leur cohérence et à leur complémentarité avec les travaux réalisés par le groupe de travail ad hoc sur la sécurité de la chaîne d'approvisionnement des technologies de l'information et de la communication, ainsi que par d'autres groupes concernés.

(10) Le groupe de coopération SRI est également invité, avec le soutien de la Commission et de l'ENISA, à poursuivre ses travaux sur la sécurité des infrastructures numériques, y compris en ce qui concerne les infrastructures sous-marines, à savoir les câbles de communication sous-marins. Il est invité aussi à entamer ses travaux concernant le secteur spatial, notamment en définissant, le cas échéant, des orientations stratégiques et des méthodes de gestion des risques en matière de cybersécurité, selon une approche "tous risques" et une approche fondée sur les risques pour les opérateurs du secteur spatial, afin d'accroître la résilience des infrastructures terrestres soutenant la fourniture de 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, par exemple 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 tirer pleinement parti du Centre de compétences européen en matière de cybersécurité. Ils devraient encourager leurs centres nationaux de coordination à dialoguer de manière proactive avec les membres de la communauté de la cybersécurité afin de renforcer les capacités au niveau de l'Union et au niveau national pour mieux soutenir les opérateurs de services essentiels.

(13) Il importe que les États membres mettent en œuvre les mesures recommandées dans la boîte à outils de l'UE sur la cybersécurité des réseaux 5G et, en particulier, qu'ils imposent des restrictions visant les fournisseurs à haut risque, tout retard risquant d'accroître la vulnérabilité des réseaux dans l'Union, et aussi qu'ils renforcent 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, afin de garantir un niveau uniforme de sécurité et de résilience des réseaux 5G.

(14) Les États membres devraient, en collaboration avec la Commission et l'ENISA, se concentrer sur la mise en œuvre des conclusions du Conseil du 17 octobre 2022 sur la sécurité de la chaîne d'approvisionnement des TIC.

(15) Les États membres devraient tenir compte du futur 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 (UE) 2016/1148 et sur les orientations définies en la matière par le groupe de coopération SRI, en particulier dans son document de référence relatif aux mesures de sécurité pour les opérateurs de services essentiels.

(16) Les États membres devraient développer l'utilisation de Copernicus, de Galileo et du système européen de navigation par recouvrement géostationnaire (EGNOS) pour la surveillance, afin de partager des informations pertinentes avec les 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 soutenir la prévision et la réaction face aux crises.

Mesures à prendre au niveau de l'Union

(17) Le dialogue et la coopération entre les experts désignés des États membres, ainsi qu'avec la Commission, devraient être renforcés, en vue de contribuer à renforcer la résilience physique des infrastructures critiques, en particulier:

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

b) en soutenant les États membres dans la mise en œuvre du nouveau cadre juridique applicable aux entités critiques, y compris en encourageant la Commission à adopter l'acte délégué en temps utile;

c) en soutenant la conduite des tests de résistance visés au point 6, sur la base de principes communs, en commençant par des tests mettant l'accent sur les menaces antagonistes d'origine humaine dans le secteur de l'énergie, puis dans d'autres secteurs clés; ainsi qu'en apportant soutien et conseils en ce qui concerne la conduite de ces tests de résistance, à la demande d'un État membre;

d) en ayant recours à une plateforme sécurisée, dès que celle-ci aura été mise en place par la Commission, pour rassembler, analyser et partager, sur une base volontaire, les bonnes pratiques, les enseignements tirés des expériences nationales et d'autres informations relatives à cette forme de résilience.

Les travaux de ces experts désignés devraient accorder une attention particulière aux dépendances transsectorielles et aux infrastructures critiques ayant une dimension transfrontière notable, et ils devraient se poursuivre au sein du Conseil et de la Commission, le cas échéant.

(18) Les États membres sont encouragés à faire usage de tout soutien offert par la Commission, par exemple par l'élaboration de manuels et de lignes directrices, tels qu'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, avec le soutien de la direction "Renseignement" de l'EMUE dans le cadre de la capacité unique d'analyse du renseignement (SIAC), 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'Union, afin d'améliorer l'appréciation de la situation.

(19) Les États membres devraient soutenir les actions menées par la Commission pour exploiter les résultats des projets sur la résilience des infrastructures critiques financés par les programmes de recherche et d'innovation de l'Union. Le Conseil prend note du fait que la Commission a l'intention d'augmenter, dans le cadre du budget alloué à Horizon Europe au titre du cadre financier pluriannuel 2021-2027, les financements consacrés à cette résilience, sans nuire au financement des autres projets de recherche et d'innovation en matière de sécurité civile dépendant d'Horizon Europe.

(20) En fonction du mandat conféré dans les conclusions du Conseil sur la posture cyber de l'UE, la Commission, le haut représentant et le groupe de coopération SRI sont invités à intensifier, conformément à leurs missions et responsabilités respectives en vertu du droit de l'Union, les travaux menés avec les réseaux et les organes et organismes civils et militaires concernés en vue d'évaluer les risques et d'élaborer des scénarios de risques en matière de cybersécurité, en prenant en compte notamment l'importance de l'énergie, des infrastructures numériques, des transports et des infrastructures spatiales, ainsi que des interdépendances entre secteurs et entre États membres. Cet exercice devrait tenir compte des risques corollaires pour les infrastructures dont dépendent ces secteurs. Lorsque cela s'avère utile, l'évaluation des risques et des scénarios de risques pourrait avoir lieu régulièrement et devrait 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.

(21) La Commission est invitée à accélérer ses activités, conformément à ses tâches respectives dans le cadre de la gestion des crises de cybersécurité, pour venir en appui à la préparation des États membres et à leur réaction aux incidents de cybersécurité majeurs, et en particulier:

a) à réaliser, en complément des évaluations de risques pertinentes dans le contexte de la sécurité des réseaux et de l'information, une étude complète[9] dressant une état des lieux des infrastructures sous-marines, à savoir les câbles de communication sous-marins, qui relient les États membres entre eux, ainsi que l'Europe au reste du monde, dont les conclusions devraient être partagées avec les États membres;

b) à soutenir la préparation et la capacité de réponse des États membres et des institutions, organes et organismes de l'Union à des incidents de cybersécurité majeurs ou à des incidents de grande ampleur, conformément au cadre juridique renforcé en matière de cybersécurité et aux autres règles pertinentes applicables[10];

c) à accélérer le développement du concept principal pour le fonds d'intervention d'urgence en matière de cybersécurité par des discussions appropriées avec les États membres.

22) La Commission est encouragée à intensifier ses travaux sur des mesures d'anticipation à visée prospective, notamment 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 (ERCC) et sa réponse aux perturbations des infrastructures critiques; à accroître les investissements dans des approches préventives et dans la préparation de la population; et à accroître le soutien lié au renforcement des capacités dans le cadre du réseau européen de connaissances en matière de protection civile.

---

9 Cette étude devrait comporter une cartographie en termes de capacités et de redondances, de vulnérabilités, de menaces et de risques pour la disponibilité des services, de répercussions des coupures de câbles sous-marins (transatlantiques) pour les États membres et l'Union dans son ensemble, ainsi que de possibilités d'atténuation des risques, tout en tenant compte de la sensibilité de telles informations et de la nécessité de les protéger.

10 Il convient également d'accorder une attention particulière à toutes les activités visant à mettre en place une réponse coordonnée efficace au niveau de l'Union en cas de cyber incident transfrontière majeur ou de menace connexe susceptible d'avoir un effet systémique sur le secteur financier de l'Union, comme le prévoit le nouveau cadre juridique en matière de résilience opérationnelle numérique.

23) La Commission devrait encourager l'utilisation des moyens de surveillance de l'Union (Copernicus, Galileo et EGNOS) 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, telles que les cadres en matière de surveillance de l'espace et en matière de surveillance de l'espace et de suivi des objets en orbites de l'UE.

24) S'il y a lieu, et conformément à leurs mandats respectifs, les organismes et autres organes concernés de l'Union sont invités à apporter leur soutien sur les questions relatives à la résilience des infrastructures critiques; sont concernées en particulier:

a) l'Agence de l'Union européenne pour la coopération des services répressifs (EUROPOL), pour la collecte d'informations, l'analyse de la criminalité et le soutien aux enquêtes menées dans le cadre d'actions répressives transfrontières, en partageant, le cas échéant, les résultats avec les États membres;

b) l'Agence européenne pour la sécurité maritime (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'Agence de l'Union européenne pour le programme spatial (EUSPA) et le Centre satellitaire de l'UE (CSUE), qui pourraient fournir une assistance dans le cadre d'opérations menées au titre du programme spatial de l'Union;

d) le Centre de compétences européen en matière de cybersécurité, pour les activités en rapport avec la cybersécurité, également en coopération avec l'ENISA, qui pourrait soutenir l'innovation et la politique industrielle en matière de cybersécurité.

CHAPITRE III: RENFORCEMENT DE LA RÉACTION

Mesures à prendre au niveau des États membres

(25) Les États membres sont invités à:

a) poursuivre la coordination de leur réaction, le cas échéant, et garder une vision d'ensemble des réactions transsectorielles aux perturbations graves des services essentiels fournis par les infrastructures critiques. Cela pourrait se faire dans le cadre d'un futur schéma directeur sur une réponse coordonnée en cas de perturbations des infrastructures critiques ayant une dimension transfrontière notable; de l'actuel dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR) en ce qui concerne les infrastructures critiques ayant une dimension transfrontière; du schéma directeur sur les incidents et crises de cybersécurité majeurs (plan d'action pour une réaction coordonnée aux incidents et crises transfrontières de cybersécurité majeurs) prévu par la recommandation (UE) 2017/1584 de la Commission[11]; du réseau UE-CyCLONe; dans le cadre pour une réponse coordonnée de l'UE aux campagnes hybrides et de la boîte à outils de l'UE en cas de menaces et campagnes hybrides; et du système d'alerte rapide en cas de désinformation;

b) accroître les échanges d'informations au niveau opérationnel avec l'ERCC dans le cadre du MPCU, afin de favoriser le lancement d'alertes précoces et de coordonner leur réaction au sein de ce mécanisme en cas de perturbations d'infrastructures critiques ayant une dimension transfrontière notable, de manière à réagir plus rapidement, avec l'appui de l'Union, lorsque cela est nécessaire;

c) accroître leur capacité à réagir aux perturbations importantes visées au point a), le cas échéant, au moyen d'outils existants ou à développer;

[11] 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).

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

e) encourager les opérateurs d'infrastructures critiques et les autorités nationales compétentes à renforcer leur capacité à rétablir rapidement un fonctionnement de base des services essentiels fournis par ces opérateurs d'infrastructures critiques;

f) encourager les opérateurs d'infrastructures critiques, lorsqu'ils reconstruisent leurs infrastructures critiques, à faire en sorte qu'elles soient aussi résilientes que possible à tout l'éventail des risques majeurs auxquels elles peuvent être exposées, y compris dans des scénarios climatiques défavorables, en tenant compte de la proportionnalité des mesures au regard des évaluations des risques et des coûts.

(26) Les États membres sont invités à accélérer leurs travaux préparatoires, dans la mesure du possible, comme le prévoit le cadre juridique renforcé en matière de cybersécurité, en ayant pour objectif de renforcer les capacités des centres nationaux CSIRT au vu des nouvelles tâches confiées à ces centres et du nombre accru d'entités opérant dans de nouveaux secteurs, en réexaminant et en actualisant en temps opportun leurs stratégies de cybersécurité et en adoptant dès que possible des plans nationaux de réponse aux incidents et aux crises en matière de cybersécurité, si de tels plans n'existent pas encore.

(27) Les États membres sont invités à examiner, au niveau national, les moyens les plus pertinents de faire en sorte que les parties prenantes concernées soient conscientes de la nécessité de faire progresser la résilience des infrastructures critiques en coopérant avec des fournisseurs et partenaires de confiance. Il est important d'investir dans des capacités supplémentaires, en particulier dans les secteurs où l'infrastructure actuelle arrive au terme de sa durée de vie, par exemple les infrastructures sous-marines de câbles de communications, afin de pouvoir assurer la continuité de la fourniture des services essentiels en cas de perturbations, et de réduire les dépendances indésirables.

(28) Les États membres sont encouragés à accorder une attention particulière à la communication stratégique proactive au niveau national dans le cadre de la lutte contre les menaces et campagnes hybrides, et compte tenu de la possibilité que les adversaires cherchent à mener des activités de manipulation de l'information et d'ingérence depuis l'étranger en façonnant les discours autour des incidents ciblant les infrastructures critiques.

Mesures à prendre au niveau de l'Union

(29) La Commission est invitée à travailler en étroite collaboration avec les États membres pour continuer à développer les organes, instruments et capacités de réaction nécessaires, en vue d'améliorer la préparation opérationnelle permettant de faire face aux effets immédiats et indirects de perturbations majeures des services essentiels concernés fournis par les infrastructures critiques, en particulier les experts et les ressources disponibles via la REPC et rescEU dans le cadre du MPCU ou les futures équipes d'intervention rapide en cas de menaces hybrides.

(30) Compte tenu de l'évolution du paysage des menaces, et en coopération avec les États membres, la Commission, dans le cadre du MPCU, est invitée à:

a) analyser et tester en continu l'adéquation et l'état de préparation opérationnelle des capacités de réaction existantes;

b) surveiller et recenser régulièrement les déficits de capacité de réaction potentiellement importants au sein de la REPC et de la réserve rescEU;

c) intensifier encore la collaboration transsectorielle afin de garantir une réponse adéquate au niveau de l'Union, et organiser régulièrement des formations ou des exercices pour tester cette collaboration, en coopération avec un ou plusieurs États membres;

d) continuer de développer l'ERCC, en tant que plateforme transsectorielle d'urgence au niveau de l'Union pour la coordination du soutien aux États membres touchés.

(31) Le Conseil est déterminé à entamer les travaux en vue d'approuver un schéma directeur pour une réponse coordonnée en cas de perturbations des infrastructures critiques ayant une dimension transfrontière notable, qui définit et décrit les objectifs et les modalités de la coopération entre les États membres et les institutions, organes et organismes de l'Union pour réagir aux incidents touchant les infrastructures critiques. Le Conseil attend avec intérêt le projet de schéma directeur que présentera la Commission, en s'appuyant sur le soutien et les contributions des organismes de l'Union concernés. Ce schéma directeur sera pleinement cohérent et interopérable avec le protocole opérationnel révisé de l'Union pour la lutte contre les menaces hybrides ("EU Playbook") et tiendra compte du schéma directeur existant pour une réaction coordonnée aux incidents et crises transfrontières de cybersécurité majeurs[12] et du mandat d'UE-CyCLONe défini dans la directive SRI 2, et évitera la duplication des structures et des activités. Le nouveau schéma directeur devrait respecter pleinement l'actuel dispositif intégré IPCR pour coordonner la réponse apportée.

[12] Recommandation (UE) 2017/1584 de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs.

(32) La Commission est invitée à consulter les parties prenantes et experts concernés pour définir des mesures appropriées en réponse à de possibles incidents importants concernant les infrastructures sous-marines, mesures qui seront présentées en même temps que l'étude visant à dresser un état des lieux de ces infrastructures visée au point 21, lettre a), et à poursuivre la définition des plans d'urgence, des scénarios de risques et des objectifs de résilience de l'Union face aux catastrophes fixés dans la décision n° 1313/2013/UE.

CHAPITRE IV: COOPÉRATION INTERNATIONALE

Mesures à prendre au niveau des États membres

(33) Les États membres devraient coopérer avec les pays tiers concernés, lorsque cela est opportun et conformément au droit de l'Union, en matière de résilience des infrastructures critiques ayant une dimension transfrontière notable.

(34) Les États membres sont encouragés à coopérer avec la Commission et le haut représentant afin de lutter efficacement contre les risques pesant sur les infrastructures critiques dans les eaux internationales.

(35) 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 du 21 juin 2022 sur un cadre pour une réponse coordonnée de l'UE aux campagnes hybrides, 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'Union aux campagnes hybrides et aux menaces hybrides, notamment celles visant des opérateurs d'infrastructures critiques.

Mesures à prendre au niveau de l'Union

(36) La Commission et le haut représentant sont invités à soutenir, le cas échéant et conformément à leurs missions et responsabilités respectives en vertu du droit de l'Union, les pays tiers concernés afin de renforcer la résilience des infrastructures critiques sur leur territoire, et en particulier des infrastructures critiques qui sont physiquement connectées à leur territoire et à celui d'un État membre.

37) La Commission et le haut représentant, conformément à leurs missions et responsabilités respectives en vertu du droit de l'Union, renforceront la coordination avec l'OTAN en ce qui concerne la résilience des infrastructures critiques d'intérêt commun dans le cadre du dialogue structuré UE-OTAN sur la résilience, dans le plein respect des compétences de l'Union et des États membres conformément aux traités et des principes clés qui guident la coopération UE-OTAN, comme convenu par le Conseil européen, en particulier la réciprocité, l'inclusion et l'autonomie décisionnelle. Dans ce contexte, cette coopération sera poursuivie dans le cadre du dialogue structuré entre l'UE et l'OTAN sur la résilience, intégré dans le mécanisme interservices existant pour la mise en œuvre des déclarations communes, tout en garantissant une transparence et une participation totales de tous les États membres.

(38) La Commission est invitée à envisager la participation de représentants des pays tiers concernés, lorsque cela est nécessaire et approprié, dans le cadre de la coopération et de l'échange d'informations entre États membres en ce qui concerne la résilience des infrastructures critiques qui sont physiquement connectées au territoire d'un État membre et à celui d'un pays tiers.

Fait à …, le …

Par le Conseil

Le président/La présidente