Conseil de
l'Union européenne

Bruxelles, le 7 septembre 2023
(OR. en)

12485/23
ADD 1

Dossier interinstitutionnel:
2023/0318(NLE)

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

NOTE DE TRANSMISSION

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

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

p.j.: COM(2023) 526 final - ANNEXE

COMMISSION
EUROPÉENNE

Bruxelles, le 6.9.2023
COM(2023) 526 final

ANNEX

ANNEXE

à la

proposition de RECOMMANDATION DU CONSEIL

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

ANNEXE

La présente annexe présente les principes, les objectifs, les principaux acteurs et les interactions avec les mécanismes de réaction aux crises existants, et décrit le fonctionnement d'un schéma directeur visant à coordonner la réponse aux incidents majeurs affectant des infrastructures critiques (ci-après le «schéma directeur pour les infrastructures critiques») et à améliorer la coopération entre les États membres et les institutions, organes et organismes compétents de l'Union en ce qui concerne ces incidents, conformément aux règles et procédures applicables. Le présent schéma directeur n'affecte en aucune manière le rôle et le fonctionnement d'autres dispositifs.

PARTIE I: OBJECTIFS, PRINCIPES, ACTEURS ET AUTRES INSTRUMENTS

1. Objectifs

Le schéma directeur pour les infrastructures critiques vise à atteindre les trois principaux objectifs suivants lors de la réponse à un incident majeur affectant une infrastructure critique:

(a) Une **connaissance situationnelle partagée**, étant donné qu'une bonne compréhension de l'incident majeur affectant une infrastructure critique dans les États membres, de son origine et de ses conséquences potentielles pour toutes les parties prenantes concernées au niveau opérationnel et stratégique/politique est essentielle pour une réponse coordonnée appropriée.

(b) Une **communication publique coordonnée**, car celle-ci contribue à atténuer les effets négatifs d'un incident majeur affectant une infrastructure critique et à réduire au minimum les divergences dans les messages transmis au public dans et entre les États membres. Une communication publique claire est également importante pour atténuer les conséquences de la désinformation.

(c) Une **réponse efficace**, étant donné que le renforcement de la réponse des États membres et de la coopération entre les États membres et avec les institutions, organes et organismes compétents de l'Union contribue à atténuer les effets d'un incident majeur affectant une infrastructure critique et à permettre le rétablissement rapide des services essentiels de manière à réduire au minimum la vulnérabilité à d'autres incidents importants.

2. Principes

Proportionnalité

Les incidents qui perturbent des infrastructures critiques et/ou la fourniture de services essentiels n'atteignent souvent pas le seuil établi pour constituer un incident majeur affectant une infrastructure critique, conformément au point 2) de la présente recommandation. En tant que tels, ils peuvent, en principe, être traités efficacement au niveau national. Par conséquent, l'application du schéma directeur pour les infrastructures critiques est limitée aux incidents majeurs affectant des infrastructures critiques.

Subsidiarité

C'est aux États membres qu'il appartient au premier chef de répondre aux perturbations d'une infrastructure critique ou des services essentiels fournis par des entités critiques, conformément au droit de l'Union. Toutefois, les institutions, organes et organismes compétents de l'Union et le Service européen pour l'action extérieure (ci-après le «SEAE») jouent un rôle complémentaire important en cas d'incident majeur affectant une infrastructure

critique ayant une dimension transfrontière notable, étant donné qu'un tel incident peut avoir des conséquences sur plusieurs pans de l'activité économique au sein du marché unique, voire sur tous les pans de celle-ci, sur la vie des citoyens vivant dans l'Union ainsi que sur la sécurité et les relations internationales de l'Union.

Complémentarité

Le schéma directeur pour les infrastructures critiques prend en considération et reflète le fonctionnement des mécanismes de gestion de crise existants à l'échelon de l'Union, à savoir le dispositif intégré de l'Union européenne pour une réaction au niveau politique dans les situations de crise (ci-après l'«IPCR»), le processus interne de coordination des crises de la Commission (ARGUS), le mécanisme de protection civile de l'Union (ci-après le «MPCU»), soutenu par le centre de coordination de la réaction d'urgence (ci-après l'«ERCC»), et le mécanisme de réaction aux crises du SEAE. Il s'appuie également sur des dispositifs sectoriels, y compris les dispositions relatives à la gestion coordonnée des incidents de cybersécurité majeurs prévues par la directive (UE) 2022/2555 du Parlement européen et du Conseil[1] et le cadre défini dans le plan d'action pour une réaction coordonnée aux incidents et crises transfrontières de cybersécurité majeurs (ci-après le «plan d'action pour la cybersécurité»)[2], le réseau des points de contact pour les transports[3] et la cellule européenne de coordination de l'aviation en cas de crise[4].

Le schéma directeur pour les infrastructures critiques complète en outre les structures et mécanismes établis par la directive (UE) 2022/2557 du Parlement européen et du Conseil[5] et doit être appliqué conformément à ces structures et mécanismes, notamment en ce qui concerne la coopération entre les autorités compétentes, avec la Commission et au sein du groupe sur la résilience des entités critiques. Il tient également compte des responsabilités des institutions, organes et organismes compétents de l'Union au titre du cadre juridique qui leur est applicable. Les activités de réaction aux crises affectant des infrastructures critiques sont complémentaires par rapport aux autres mécanismes de gestion de crise au niveau de l'Union, au niveau national et au niveau sectoriel, qui soutiennent la coordination multisectorielle.

Confidentialité des informations

Le schéma directeur pour les infrastructures critiques tient compte de l'importance de préserver la confidentialité des informations classifiées et sensibles non classifiées relatives aux infrastructures critiques et aux entités critiques.

3. Acteurs concernés

Chaque État membre et les institutions, organes et organismes compétents de l'Union visés aux points a) à e) ci-dessous décideront, conformément aux règles et procédures qui leur sont

---

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

[2] 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).

[3] Communication de la Commission intitulée «Un plan d'urgence pour les transports» [COM(2022) 211 final].

[4] Créée en vertu de l'article 19 du règlement d'exécution (UE) 2019/123 de la Commission du 24 janvier 2019 établissant les modalités d'exécution des fonctions de réseau de la gestion du trafic aérien.

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

applicables, du ou des acteurs pertinents pour chaque incident majeur affectant une infrastructure critique, en fonction du ou des secteurs concernés et du type d'incident.

a) États membres

– Les autorités compétentes [par exemple, les autorités chargées des infrastructures critiques, les autorités sectorielles concernées, les points de contact uniques désignés ou mis en place conformément à l'article 9, paragraphe 2, de la directive (UE) 2022/2557 et les autorités désignées ou mises en place conformément à l'article 9, paragraphe 1, de la directive (UE) 2022/2557];

– le cas échéant, le réseau européen d'organisations de liaison en cas de crises de cybersécurité (ci-après «UE-CyCLONe») prévu à l'article 16 de la directive (UE) 2022/2555;

– le groupe de coopération prévu à l'article 14 de la directive (UE) 2022/2555;

– le cas échéant, d'autres parties prenantes, y compris des entités ou des personnes du secteur privé comme les exploitants d'infrastructures critiques, y compris celles recensées en tant qu'entités critiques;

– les ministres chargés de la résilience des infrastructures critiques et/ou le ou les ministres responsables du ou des secteurs les plus touchés par l'incident majeur affectant une infrastructure critique en question.

b) Le Conseil

– La présidence tournante;

– les groupes de travail concernés, tels que le groupe de travail «Protection civile», y compris le sous-groupe sur la résilience des entités critiques PROCIV-CER, et le ou les présidents des groupes de travail concernés en fonction du ou des secteurs touchés et de la nature de l'incident, tels que le groupe de travail horizontal «Questions cyber» et le groupe de travail horizontal «Renforcement de la résilience et lutte contre les menaces hybrides»;

– le Coreper, le comité politique et de sécurité et l'IPCR, tous soutenus par le secrétariat général du Conseil.

c) La Commission, y compris ses groupes d'experts

— Le service chef de file désigné (en fonction du secteur touché) soutenu par l'ERCC en tant que plateforme opérationnelle 24 heures sur 24, 7 jours sur 7, gérant les réponses aux crises, et par la direction générale de la migration et des affaires intérieures en tant que service responsable dans la zone et, en cas d'incident intersectoriel, la direction générale de la migration et des affaires intérieures et d'autres services compétents de la Commission;

– la direction générale de la communication, y compris le service du porte-parole;

– la direction générale HERA, l'autorité de préparation et de réaction en cas d'urgence sanitaire;

– le groupe sur la résilience des entités critiques, présidé par un représentant de la Commission (direction générale de la migration et des affaires intérieures) et établi par la directive (UE) 2022/2557, et le cas échéant, d'autres groupes et comités d'experts pertinents;

– l'ERCC créé dans le cadre du MPCU par la décision nº 1313/2013/UE du Parlement européen et du Conseil[6] (plateforme opérationnelle 24 heures sur 24, 7 jours sur 7, pour la gestion des urgences, établie dans le cadre du MPCU et relevant de la direction générale de la protection civile et des opérations d'aide humanitaire européennes);

– le groupe de coopération prévu à l'article 14 de la directive (UE) 2022/2555;

– le centre de sensibilisation et d'analyse de la situation en matière de cybersécurité;

– le comité de sécurité sanitaire prévu à l'article 4 du règlement (UE) 2022/2371[7];

– le secrétariat général de la Commission (secrétariat du système ARGUS) et le secrétaire général (adjoint) (système ARGUS), direction générale des ressources humaines (direction de la sécurité);

– d'autres groupes d'experts compétents de la Commission qui assistent cette dernière dans la coordination des mesures en situation d'urgence ou de crise;

– d'autres réseaux de gestion de crise, y compris sectoriels (par exemple, le réseau des points de contact pour les transports géré par la direction générale de la mobilité et des transports, la task force (ou équipe spéciale) interinstitutionnelle chargée des crises cyber[8], la Cellule européenne de coordination de l'aviation en cas de crise);

– le/la président(e) et/ou le/la vice-président(e)/commissaire responsable.

d) Le SEAE

– la capacité unique d'analyse du renseignement (SIAC) composée du Centre de situation et du renseignement de l'UE («INTCEN») et de la direction «Renseignement» de l'État-major de l'Union européenne («EUMS INT»);

– le centre de réaction aux crises («CRC»);

– le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité/vice-président de la Commission.

e) Les organes et organismes compétents de l'Union, tels qu'Europol, en fonction du ou des secteurs concernés[9].

---

[6] 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).

[7] Règlement (UE) 2022/2371 du Parlement européen et du Conseil du 23 novembre 2022 concernant les menaces transfrontières graves pour la santé et abrogeant la décision nº 1082/2013/UE (JO L 314 du 6.12.2022, p. 26).

[8] Un groupe informel comprenant les services compétents de la Commission, le SEAE, l'Agence de l'Union européenne pour la cybersécurité (ENISA), la CERT-UE et Europol, coprésidé par la direction générale des réseaux de communication, du contenu et des technologies et le SEAE.

[9] Par exemple, Europol; pour les transports: l'Agence de l'Union européenne pour la sécurité aérienne (AESA), l'Agence européenne pour la sécurité maritime (AESM), l'Agence ferroviaire européenne (AFE); pour la santé: le Centre européen de prévention et de contrôle des maladies (ECDC) et l'Agence européenne des médicaments (EMA); pour l'énergie: l'Agence de l'Union européenne pour la coopération des régulateurs de l'énergie (ACER); pour l'espace: l'Agence de l'Union européenne pour le programme spatial (EUSPA); pour le secteur de l'alimentation: l'Autorité européenne de sécurité des aliments (EFSA); pour le secteur maritime: l'Agence européenne de contrôle des pêches (AECP); pour les cyberincidents: l'Agence de l'Union européenne pour la cybersécurité (ENISA), les centres de réponse aux incidents de sécurité informatiques (CSIRT) et

4. Interaction avec les autres mécanismes et instruments de gestion de crise pertinents

Le schéma directeur pour les infrastructures critiques est un instrument souple qui répertorie les différentes mesures susceptibles d'être prises, en tout ou partie, en faisant appel à différents dispositifs existants, en fonction de la nature et de la gravité de l'incident majeur affectant une infrastructure critique et de la nécessité d'une coordination opérationnelle et stratégique/politique.

a) le protocole de l'Union de lutte contre les menaces hybrides[10] (ci-après le «protocole de l'Union»)

Le protocole de l'Union peut servir, en cas de menace hybride[11], à donner un aperçu des processus et outils pouvant être utilisés dans le cadre de telles menaces ou campagnes.

En cas d'incident majeur affectant une infrastructure critique qui revêt une dimension hybride, le protocole de l'Union s'applique en complémentarité avec le schéma directeur pour les infrastructures critiques, le cas échéant, par exemple pour obtenir des informations, des analyses ou des communications spécifiques sur les aspects hybrides de l'incident majeur affectant une infrastructure critique et en ce qui concerne la coopération avec des partenaires extérieurs.

b) Le plan d'action pour une réaction coordonnée aux incidents et crises transfrontières de cybersécurité majeurs

Le plan d'action pour la cybersécurité s'applique aux incidents transfrontières de grande ampleur qui provoquent des perturbations dépassant les capacités d'action du seul État membre concerné ou qui frappent plusieurs États membres ou institutions de l'Union en s'accompagnant de répercussions techniques ou politiques si vastes et significatives qu'ils requièrent une coordination et une réaction rapides au niveau politique de l'Union.

En cas d'incident majeur affectant une infrastructure critique qui coïncide avec un incident de cybersécurité majeur ou qui semble être lié à un tel incident, les groupes de travail compétents du Conseil établissent une coordination appropriée au niveau opérationnel, notamment avec UE-CyCLONe ou en organisant une réunion conjointe du groupe sur la résilience des entités critiques et du groupe de coopération. L'objectif de la coordination est de déterminer quel acteur et quel(s) instrument(s) ou mécanisme(s) pourraient contribuer le plus efficacement à la réponse à l'incident majeur affectant une infrastructure critique, tout en évitant les doubles emplois et les axes de travail parallèles.

c) Le mécanisme de protection civile de l'Union et le Centre de coordination de la réaction d'urgence

Conformément à la décision nº 1313/2013/UE relative au mécanisme de protection civile de l'Union, les réponses opérationnelles mises en œuvre au titre du MPCU en cas de catastrophes naturelles et d'origine humaine, réelles ou imminentes, (y compris celles entraînant des

---

l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'Union européenne (CERT-UE).

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

[11] Les menaces hybrides peuvent être décrites comme étant un mélange d'activités coercitives et subversives, de méthodes conventionnelles et non conventionnelles, susceptibles d'être utilisées de façon coordonnée par des acteurs étatiques ou non étatiques en vue d'atteindre certains objectifs, sans que le seuil d'une guerre déclarée officiellement ne soit dépassé; voir le protocole de l'Union de lutte contre les menaces hybrides.

perturbations d'infrastructures critiques) à l'intérieur comme à l'extérieur de l'UE sont dirigées par l'ERCC, la plateforme unique de la Commission, opérationnelle 24 heures sur 24, 7 jours sur 7, qui gère les réponses aux crises. Dans de tels cas, l'ERCC peut assurer une alerte précoce, une notification et une analyse et faciliter le partage d'informations, et, en cas d'activation du MPCU par un État membre, déployer une assistance opérationnelle et des experts dans les zones touchées. Elle peut également faciliter la coordination sectorielle et intersectorielle tant au niveau de l'UE qu'entre l'UE et les autorités nationales compétentes, y compris celles chargées de la protection civile et de la résilience des infrastructures critiques.

d) Autres mécanismes et instruments sectoriels ou intersectoriels

Le schéma directeur pour les infrastructures critiques ne fait pas double emploi avec d'autres instruments de gestion des crises ou mécanismes de coordination sectoriels ou intersectoriels. Lorsque de tels instruments ou mécanismes existent déjà dans le secteur concerné, le schéma directeur pour les infrastructures critiques peut être utilisé, dans les limites de son champ d'application, comme un instrument complémentaire aux instruments ou mécanismes sectoriels ou intersectoriels, mais ne les remplace pas. La coordination nécessaire entre les différents acteurs devrait être assurée afin d'éviter de tels doubles emplois. Cet objectif pourrait notamment être atteint dans le cadre du processus interne de coordination des crises de la Commission (ARGUS), soutenu par l'ERCC, et/ou des réunions de coordination de l'IPCR.

PARTIE II: ÉCHANGE D'INFORMATIONS ET REPONSE COORDONNEE

Les actions décrites ci-dessous consistent en des modes de coopération, à savoir des échanges d'informations, une communication coordonnée et des réponses. Cette structure correspond aux modes de fonctionnement du mécanisme du Conseil pour la coordination des crises (IPCR) et tient compte, plus largement, de l'utilisation potentielle des mécanismes de coordination de crise qui existent déjà au niveau de l'UE. Elle montre comment ces modes de coopération s'y intégreraient s'ils étaient utilisés. Toutefois, la plupart de ces mesures peuvent également être prises de manière autonome: elles ne dépendent pas de l'utilisation de ce mécanisme, mais le complètent. Les mesures sont présentées dans un ordre chronologique, tout en tenant compte du fait qu'en cas de crise de grande ampleur constituant un incident majeur affectant une infrastructure critique, plusieurs mesures peuvent être prises simultanément et de manière continue.

1. ÉCHANGE D'INFORMATIONS

(a) Au niveau opérationnel

Les États membres concernés par un incident majeur affectant une infrastructure critique appliquent leurs propres mesures d'urgence, assurent la coordination avec les mécanismes nationaux de gestion de crise pertinents et veillent à ce que tous les acteurs nationaux, régionaux et locaux concernés se mobilisent, le cas échéant.

S'il y a lieu, en ce qui concerne l'assistance relevant de la protection civile, la coordination entre les États membres et avec la Commission est assurée par l'intermédiaire de l'ERCC dans le cadre du MPCU.

i) Partage d'informations et notification par les autorités nationales compétentes

Outre les obligations de notification et d'information prévues à l'article 15 de la directive (UE) 2022/2557, les autorités nationales compétentes chargées des infrastructures critiques dans les États membres concernés par un incident majeur affectant une infrastructure critique

partagent avec la présidence tournante du Conseil et la Commission, par l'intermédiaire de leurs points de contact uniques et dans les meilleurs délais, les informations pertinentes reçues du ou des exploitants d'infrastructures critiques, d'entités critiques ou d'autres sources, ainsi que les informations relatives aux mécanismes de gestion de crise qui ont été activés. Pour la Commission, l'ERCC assure les contacts et capacités opérationnels 24 heures sur 24, 7 jours sur 7, et coordonne, surveille et soutient en temps réel la réaction aux situations d'urgence au niveau de l'Union, tout en servant les États membres et la Commission en tant que plateforme opérationnelle pour la réaction aux crises promouvant une approche intersectorielle de la gestion des catastrophes.

Ce partage d'informations concerne la nature de l'incident majeur affectant une infrastructure critique, sa cause, les conséquences observées ou estimées de la perturbation sur l'infrastructure critique et la fourniture de services essentiels, les conséquences de l'incident par-delà les secteurs et les frontières et les mesures d'atténuation, déjà prises ou envisagées, au niveau national ou avec d'autres États membres concernés et la Commission dans le cadre d'accords existants, par exemple les accords de partage d'informations prévus aux articles 9 et 15 de la directive (UE) 2022/2557. Cette notification est fournie sans détourner les ressources de l'infrastructure critique, ou, dans certains cas, de l'entité critique ou de l'État membre des activités liées à la gestion de l'incident, qui devraient être prioritaires.

Afin d'assurer le suivi, l'ERCC ou les services de la Commission notifiés, responsables du ou des secteurs dans lesquels l'incident majeur affectant une infrastructure critique s'est produit, informent le point de contact de la direction générale de la migration et des affaires intérieures et le secrétariat général de la Commission. Dans l'intervalle, si ce n'est déjà le cas, l'ERCC commence à surveiller les événements, en particulier en cas d'activation du MPCU par un ou plusieurs des États membres concernés.

Si les informations peuvent être pertinentes pour traiter un aspect relatif à la cybersécurité ou être liées à un incident de cybersécurité, la Commission partage les informations pertinentes avec UE-CyCLONe.

Les autorités nationales compétentes au titre de la directive (UE) 2022/2557 sont tenues de coopérer et d'échanger des informations avec les autorités compétentes en vertu de la directive (UE) 2022/2555, dans les meilleurs délais, pour ce qui est des incidents et cyberincidents concernant des entités critiques, y compris les mesures de cybersécurité et les mesures physiques adoptées par les entités critiques.

En ce qui concerne le domaine maritime, les autorités nationales compétentes envisagent la possibilité d'utiliser l'environnement commun de partage de l'information («CISE») pour partager des informations dans les meilleurs délais.

ii) Organisation de réunions d'experts

La Commission convoque dès que possible le groupe sur la résilience des entités critiques afin de faciliter les échanges d'informations pertinentes entre les autorités nationales compétentes chargées des infrastructures critiques et les institutions, organes et organismes compétents de l'Union au sujet de l'incident (nature, cause, incidence et conséquences par-delà les secteurs et les frontières) et des mesures de réponse, y compris les mesures d'atténuation et le soutien technique aux États membres concernés. En fonction du centre de gravité de l'incident, les services compétents de la Commission seront étroitement associés à la réunion du groupe sur la résilience des entités critiques afin de partager les informations recueillies au moyen des instruments sectoriels existants. En cas d'incidents présentant à la fois une dimension de cybersécurité et une dimension physique non liée à la cybersécurité, les services compétents de la Commission, la CERT-UE et le SEAE, le cas échéant, notifient et consultent dès que

possible la task force (ou équipe spéciale) chargée des crises cyber, ainsi que les présidents respectifs du groupe de coopération mentionné à l'article 14 de la directive (UE) 2022/2555 et d'UE-CyCLONe, le cas échéant, au sujet de la nécessité d'activités de coordination. En accord avec les présidents respectifs, la Commission (direction générale de la migration et des affaires intérieures et direction générale des réseaux de communication, du contenu et des technologies) peut proposer une réunion conjointe du groupe sur la résilience des entités critiques et du groupe de coopération en vue d'élaborer une appréciation commune de la situation et de coordonner les réponses respectives.

En cas d'incident majeur affectant une infrastructure critique de nature intersectorielle qui nécessite ou est susceptible de nécessiter une gestion des conséquences au niveau de l'Union, la Commission peut convoquer des réunions de coordination intersectorielles associant toutes les parties prenantes concernées.

Si un incident majeur affectant une infrastructure critique affecte également un pays tiers, la Commission consulte les autorités compétentes du pays tiers affecté et peut les inviter à une réunion du Groupe sur la résilience des entités critiques.

iii) Soutien de la Commission et des agences de l'Union

Le cas échéant et conformément à son mandat, Europol présente un rapport de situation sur l'incident au niveau de l'Union. D'autres agences de l'Union, le cas échéant et en agissant conformément à leurs mandats respectifs, communiquent à leurs directions générales de tutelle respectives, qui font rapport à la Commission (direction générale de la migration et des affaires intérieures, en tant que présidente du groupe sur la résilience des entités critiques), les informations pertinentes qui contribuent à la connaissance de la situation ou à la réponse coordonnée à l'incident majeur affectant une infrastructure critique.

La Commission peut contribuer à la connaissance de la situation en utilisant les moyens du programme spatial de l'Union[12] tels que Copernicus, Galileo et EGNOS, le cas échéant et conformément au cadre juridique applicable.

(b) Au niveau stratégique

i) Élaboration de rapports sur la connaissance de la situation

Sur la base des informations partagées par les autorités nationales compétentes lors d'une réunion du groupe sur la résilience des entités critiques, ou de réunions conjointes avec les services, groupes d'experts ou réseaux concernés, la Commission élabore un rapport sur la connaissance de la situation sur la base des contributions des autorités nationales compétentes et des autres informations disponibles.

Le cas échéant, ce rapport tiendra compte des résultats des évaluations des risques, des appréciations et des scénarios pertinents au niveau de l'UE du point de vue de la cybersécurité, y compris ceux réalisés par la Commission, le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité et le groupe de coopération.

En cas d'activation de l'IPCR, ce rapport peut contribuer au rapport sur la connaissance et l'analyse intégrées de la situation («ISAA») préparé par les services de la Commission et le SEAE.

[12] 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).

Le cas échéant, la SIAC présente une évaluation actualisée de l'incident fondée sur des renseignements.

ii) Activation des mécanismes de coordination de crise de l'Union et utilisation des instruments de l'Union

L'ERCC commence à fournir un soutien en matière de connaissance de la situation relative à l'incident, le cas échéant, en particulier si l'événement entraîne une activation du MPCU[13]. Les États membres concernés peuvent également demander des images satellite de leur territoire en faisant appel au service Copernicus de gestion des urgences.

Lorsque cela est jugé approprié pour partager des informations au sein de la Commission avec le SEAE et les agences compétentes de l'Union, la direction générale chef de file ou la direction générale de la migration et des affaires intérieures, en coordination avec le secrétariat général, active la phase I du processus interne de coordination des crises de la Commission (ARGUS) en ouvrant un événement sur l'outil informatique ARGUS.

La présidence tournante du Conseil de l'Union peut activer le dispositif IPCR en mode «partage de l'information», ce qui entraîne l'élaboration de rapports ISAA par la Commission et le SEAE avec des contributions des autorités nationales compétentes et d'autres sources, le cas échéant. Même sans activer l'IPCR, une page de surveillance peut être ouverte sur la plateforme web de l'IPCR par la présidence tournante du Conseil ou par la Commission, à certaines conditions.

D'autres mécanismes et outils (sectoriels) de gestion de crise de l'Union peuvent être activés en suivant les procédures respectives, le cas échéant. La Commission assurera la coordination entre ces mécanismes et instruments.

Si l'incident physique coïncide avec un incident de cybersécurité majeur, tel que défini à l'article 6, paragraphe 7, de la directive (UE) 2022/2555, ou semble être lié à un tel incident, la présidence tournante du Conseil peut utiliser le plan d'action pour la cybersécurité pour établir une coordination appropriée au niveau opérationnel associant, entre autres, l'UE-CyCLONe et le groupe sur la résilience des entités critiques.

iii) Coordination de la communication publique

Les États membres concernés par un incident majeur affectant une infrastructure critique coordonnent, dans la mesure du possible, leur communication publique sur la crise, tout en respectant les compétences nationales en la matière. Le réseau des responsables de la communication de crise de l'IPCR peut être associé, le cas échéant.

Sur la base de la connaissance situationnelle partagée, le groupe sur la résilience des entités critiques et les États membres concernés soutiennent la formulation de lignes de communication publique adoptées d'un commun accord, le cas échéant.

Europol et les autres agences compétentes de l'Union coordonnent leurs activités de communication publique avec le service du porte-parole de la Commission, sur la base d'une connaissance situationnelle partagée.

Si l'incident majeur affectant une infrastructure critique comporte une dimension externe, hybride ou qui relève de la politique de sécurité et de défense commune, la communication

[13] Prenant par exemple la forme de la publication de produits pour le suivi des médias, de messages de protection civile, de notes analytiques, de cartes quotidiennes («Daily Map») de la DG ECHO, de bulletins d'information quotidiens («Daily Flash») de la DG ECHO et d'autres produits sur mesure.

publique est coordonnée avec le SEAE et le service du porte-parole de la Commission, conformément au protocole de l'Union de lutte contre les menaces hybrides[14].

2. REPONSE (COMPOSEE NOTAMMENT DES ACTIONS CONTINUES DECRITES DANS LES SECTIONS «ÉCHANGE D'INFORMATIONS» ET «MESURES SUPPLEMENTAIRES AU NIVEAU STRATEGIQUE/POLITIQUE»)

(a) Au niveau stratégique

i) Élaboration continue de rapports sur la situation

Le groupe de travail «Protection civile – Résilience des entités critiques» (PROCIV-CER) est informé de l'élaboration d'un rapport sur la situation politico-stratégique (par exemple, le rapport ISAA en cas d'activation de l'IPCR ou le rapport relatif à l'appréciation commune de la situation établi par la Commission) et prépare la réunion du Coreper, si celle-ci n'a pas encore été convoquée, ou du comité politique et de sécurité, selon le cas.

La SIAC intensifie son action auprès des services de renseignement des États membres, regroupe les informations provenant de toutes les sources et prépare une analyse et une évaluation de l'incident, ainsi que des mises à jour régulières, si nécessaire.

ii) Activation totale des mécanismes de coordination de crise de l'Union et utilisation des instruments de l'Union

Si le président de la Commission active la phase II du processus interne de coordination des crises de la Commission (ARGUS), une ou plusieurs réunions du comité de coordination de crise auxquelles participent les services compétents de la Commission, les agences et le SEAE, le cas échéant, sont convoquées à bref délai afin de coordonner tous les aspects de l'incident majeur affectant une infrastructure critique.

Si l'IPCR est totalement activé par la présidence du Conseil:

– la présidence tournante du Conseil demande la tenue, en temps utile, d'une table ronde informelle réunissant les acteurs nationaux, européens et internationaux concernés, au cours de laquelle le représentant de la Commission agissant en tant que président du groupe sur la résilience des entités critiques (direction générale de la migration et des affaires intérieures) peut rendre compte de la ou des réunions du groupe précédemment convoquées; son compte rendu peut être complété, le cas échéant, par d'autres services de la Commission et le SEAE;

– la SIAC et les agences compétentes de l'Union peuvent être invitées à présenter une mise à jour de la situation en ce qui concerne l'incident majeur affectant une infrastructure critique lors de cette réunion.

Le service chef de file de l'ISAA (le service chef de file de la Commission ou le SEAE) prépare le rapport ISAA avec les contributions des services compétents de la Commission, des organes et organismes de l'Union concernés et des autorités nationales compétentes. Les États membres sont invités à contribuer, par l'intermédiaire de la plateforme internet de l'IPCR, à l'élaboration des rapports ISAA.

En cas d'incident majeur affectant une infrastructure critique qui présente un intérêt pour la sécurité internationale, les services de la Commission et le SEAE peuvent convoquer une réunion du dialogue structuré entre l'UE et l'OTAN sur la résilience afin de contribuer à

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

l'élaboration d'une appréciation commune de la situation et à l'échange d'informations sur les mesures prises respectivement par l'Union et l'OTAN.

iii) Communication publique

Le Conseil élabore des messages de communication publique communs. Le réseau informel des responsables de la communication de crise établi par l'intermédiaire de l'IPCR peut apporter son soutien à ces travaux. Le service du porte-parole de la Commission prépare également, le cas échéant, des messages de communication publique.

Si l'incident majeur affectant une infrastructure critique comporte une dimension externe, hybride ou qui relève de la politique de sécurité et de défense commune, la communication publique est coordonnée avec le SEAE et le service du porte-parole de la Commission.

iv) Soutien aux États membres et réponse efficace

La présidence tournante peut convoquer une réunion du groupe PROCIV-CER pour soutenir les activités menées dans le cadre de l'IPCR, si celui-ci est activé.

Les États membres concernés par l'incident majeur affectant une infrastructure critique peuvent demander le soutien technique d'autres États membres ou d'institutions, d'organes et d'organismes compétents de l'Union par l'intermédiaire du groupe sur la résilience des entités critiques, par exemple une expertise spécifique afin d'atténuer les effets néfastes de l'incident majeur affectant une infrastructure critique.

Les États membres concernés par l'incident majeur affectant une infrastructure critique peuvent également demander le soutien technique et/ou financier de la Commission ou des agences compétentes de l'Union. La Commission, en coordination avec les agences compétentes de l'Union, évalue son éventuel soutien et active, le cas échéant, des mesures techniques d'atténuation au niveau de l'Union conformément à leurs procédures respectives et coordonne les capacités techniques nécessaires pour mettre fin aux effets de l'incident majeur affectant une infrastructure critique ou les réduire.

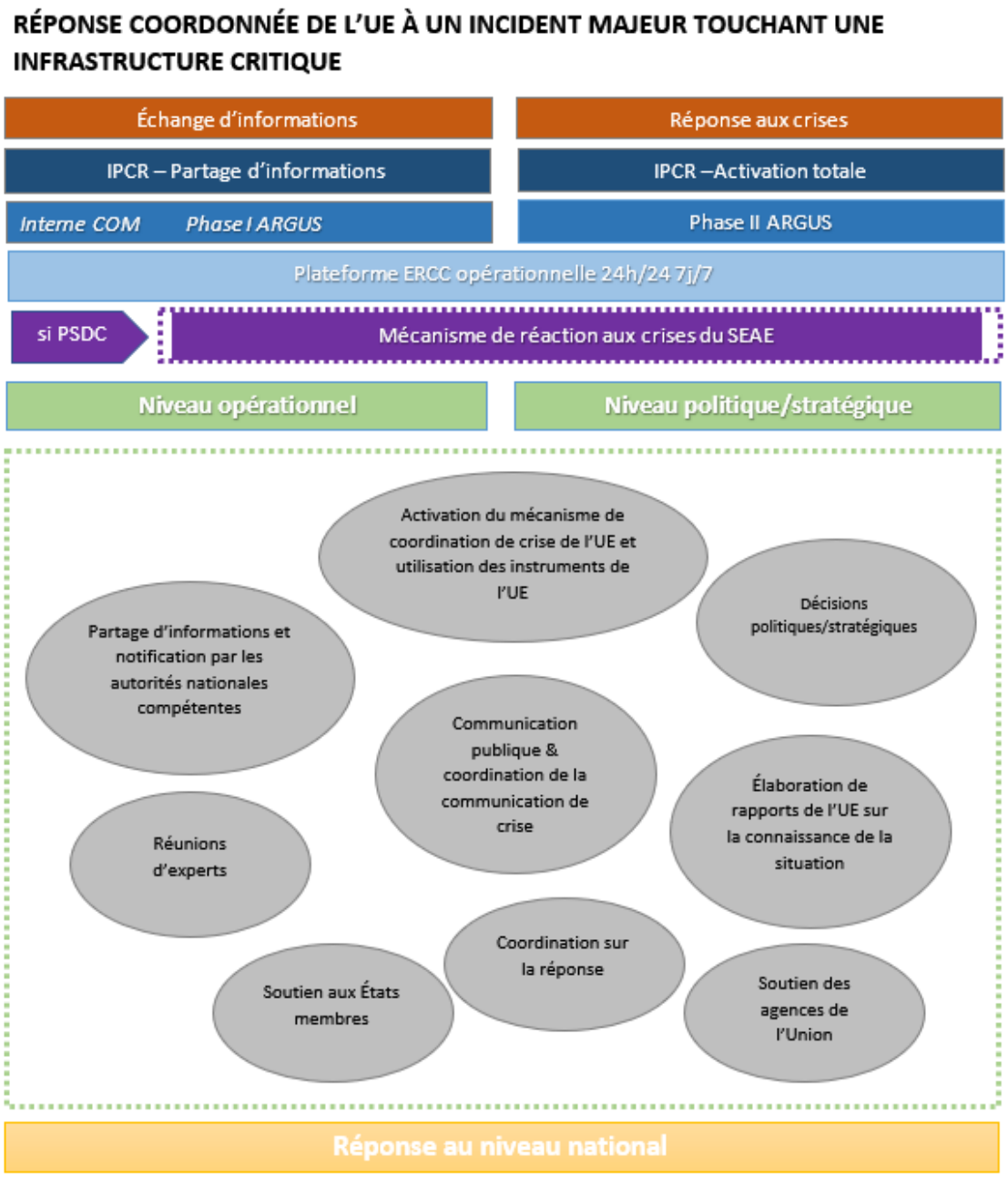
Dans le contexte spécifique du MPCU, les pays concernés pourraient demander une assistance en faisant appel au système commun de communication et d'information d'urgence («CECIS»), après quoi l'ERCC s'emploierait à coordonner l'assistance fournie par les États membres et les États participant au MPCU, ainsi que par l'intermédiaire de «rescEU».

Dans le cadre de leurs mandats respectifs et sur demande, Europol et d'autres agences compétentes de l'Union aident les États membres concernés par un incident majeur affectant une infrastructure critique à enquêter sur cet incident.

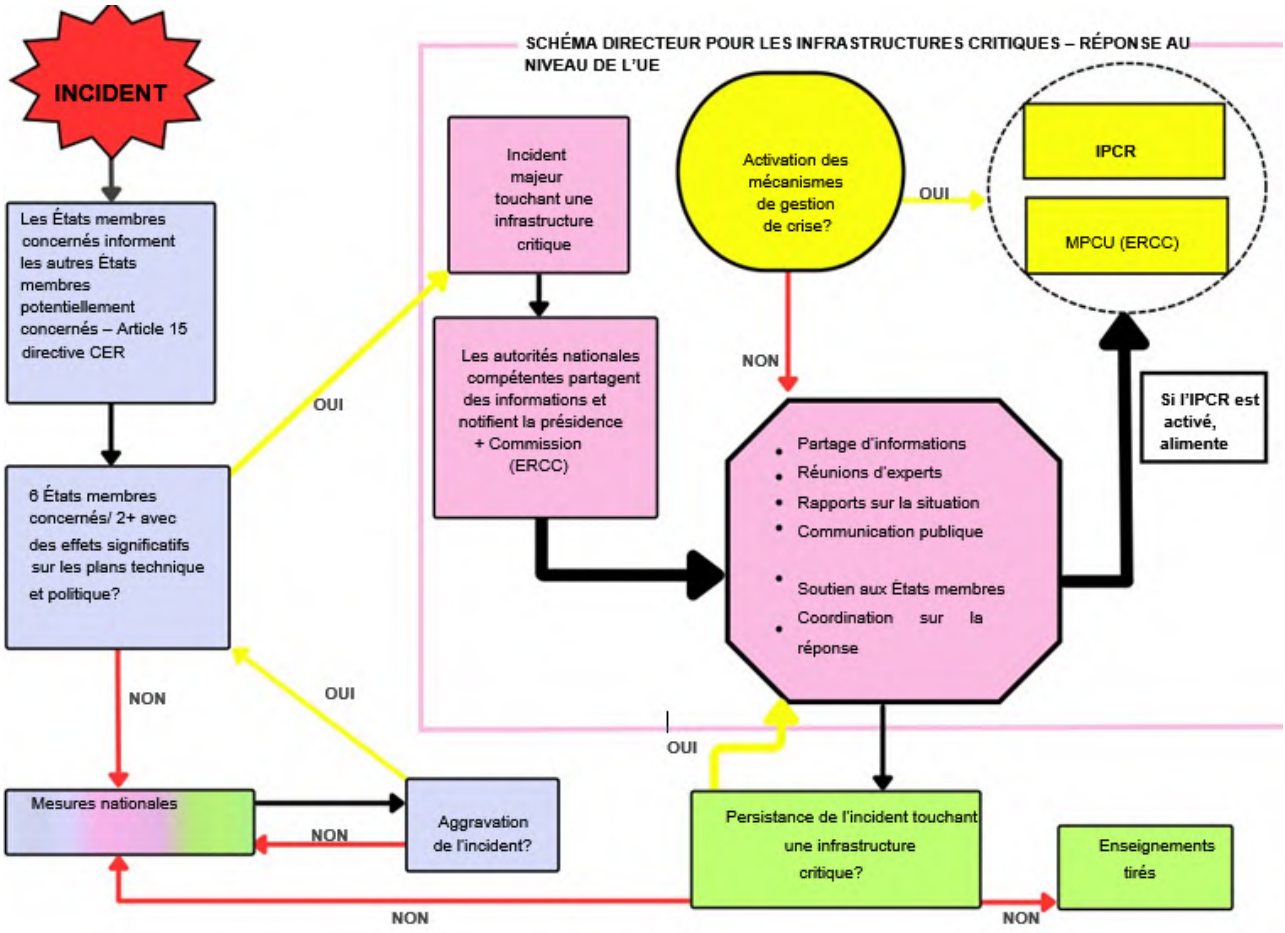
(b) Au niveau politique

La présidence du Conseil pourrait examiner la nécessité de convoquer des tables rondes de l'IPCR, des réunions des groupes de travail du Conseil, du Coreper ou du Conseil des ministres et/ou des sommets afin de procéder à un échange de vues sur l'origine possible et les conséquences attendues de l'incident majeur affectant une infrastructure critique pour les États membres et pour l'Union, de convenir de lignes directrices communes et d'adopter les mesures nécessaires pour soutenir les États membres concernés par l'incident majeur affectant une infrastructure critique et en atténuer les effets.

Graphique 1: aperçu schématique du schéma directeur pour les infrastructures critiques



Graphique 2: Décision dans le cadre du schéma directeur pour les infrastructures critiques



LÉGENDE

Phases préalables à la mise en œuvre du schéma directeur

Activation des mécanismes de gestion de crise

Schéma directeur

Phases postérieures à la mise en œuvre du schéma directeur