Conseil de
l'Union européenne

Bruxelles, le 6 juin 2025
(OR. en)

9794/25

Dossier interinstitutionnel:
2025/0036 (NLE)

CYBER 157
IPCR 42
RELEX 706
JAI 738
JAIEX 54
POLMIL 138
HYBRID 63
TELECOM 178
COSI 108

RÉSULTATS DES TRAVAUX

Origine:	Secrétariat général du Conseil
en date du:	6 juin 2025
Destinataire:	délégations
Objet:	Recommandation du Conseil sur un schéma directeur de l'UE pour la gestion des crises de cybersécurité - Recommandation du Conseil approuvée par le Conseil lors de sa session du 6 juin 2025

Les délégations trouveront en annexe la recommandation du Conseil approuvée par le Conseil lors de sa session du 6 juin 2025

ANNEXE

RECOMMANDATION DU CONSEIL

sur un schéma directeur de l'UE pour la gestion des crises de cybersécurité

LE CONSEIL DE L'UNION EUROPÉENNE,

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

vu la proposition de la Commission européenne,

considérant ce qui suit:

(1) Les technologies numériques et la connectivité mondiale constituent l'épine dorsale de la croissance économique, de la compétitivité et de la transformation des infrastructures critiques de l'Union. Toutefois, une économie interconnectée et de plus en plus numérique augmente également le risque d'incidents de cybersécurité et de cyberattaques. En outre, l'augmentation des tensions géopolitiques, des conflits et des rivalités stratégiques se reflète dans l'incidence, le volume et la sophistication des actes de cybermalveillance. Ces activités peuvent s'inscrire dans le cadre de campagnes hybrides ou d'opérations militaires. Elles peuvent également avoir une incidence directe sur la sécurité, l'économie et la société de l'Union. En outre, elles sont susceptibles d'avoir des retombées, en particulier lorsque ces activités ciblent des pays partenaires stratégiques internationaux tels que les pays candidats ou les pays voisins.

(2) Un incident de cybersécurité majeur peut provoquer des perturbations dépassant les capacités de réaction du seul État membre concerné ou a un impact important sur plusieurs États membres. En fonction de sa cause et de son impact, un tel incident peut dégénérer et se transformer en une crise à part entière, empêchant le bon fonctionnement du marché intérieur ou présentant de graves risques de sûreté et de sécurité publiques pour les entités ou les citoyens dans plusieurs États membres ou dans l'Union dans son ensemble. Une gestion efficace des crises est fondamentale pour maintenir la stabilité économique et protéger les gouvernements, les infrastructures critiques, les entreprises et les citoyens européens, ainsi que pour contribuer à la sécurité et à la stabilité internationales dans le cyberespace. La gestion des crises de cybersécurité fait donc partie intégrante du cadre global de gestion des crises de l'UE.

(3) Compte tenu des interdépendances et des interconnexions entre les environnements TIC des entités de l'Union et des États membres, un incident survenu dans une entité de l'Union pourrait présenter un risque de cybersécurité pour les États membres et inversement. Le partage d'informations pertinentes et la coordination en ce qui concerne tant les incidents de cybersécurité majeurs que les incidents majeurs, tels que définis à l'article 3, point 8, du règlement (UE, Euratom) 2023/2841[1], sont essentiels dans le contexte du schéma directeur de l'UE pour la gestion des crises de cybersécurité (ci-après le "schéma directeur en matière de cybersécurité").

[1] Règlement (UE/Euratom) 2023/2841 du Parlement européen et du Conseil du 13 décembre 2023 établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union (JO L, 2023/2841, 18.12.2023, p. 1).

(4) En cas de crise pour laquelle le dispositif intégré de l'UE pour une réaction au niveau politique dans les situations de crise (IPCR) au titre de la décision d'exécution (UE) 2018/1993 du Conseil[2] (ci-après les "dispositions relatives à l'IPCR") a été activé, le schéma directeur en matière de cybersécurité devrait respecter pleinement les dispositions relatives à l'IPCR en ce qui concerne la coordination et la réaction. La coordination politique et stratégique se ferait dans le cadre de l'IPCR. Les dispositions relatives à l'IPCR constituent l'outil de coordination et de réaction horizontales au niveau politique de l'Union. Conformément aux dispositions relatives à l'IPCR, la décision d'activer ou de désactiver l'IPCR est prise par la présidence du Conseil de l'Union européenne. Les rapports sur la connaissance et l'analyse intégrées de la situation (ISAA) élaborés par les services de la Commission et le Service européen pour l'action extérieure (SEAE) soutiennent les travaux de l'IPCR tant dans son mode "partage de l'information" que dans son mode "activation totale".

(5) Les États membres ont la responsabilité première dans la gestion des incidents de cybersécurité et des crises de cybersécurité. La nature transfrontière et transsectorielle potentielle des incidents de cybersécurité exige toutefois des États membres et des entités concernées de l'Union qu'ils coopèrent aux niveaux technique, opérationnel et politique en vue d'une coordination efficace dans l'ensemble de l'Union. La gestion des crises de cybersécurité sur l'ensemble du cycle de vie comprend donc la préparation et une appréciation commune de la situation afin d'anticiper les incidents de cybersécurité majeurs, les capacités de détection nécessaires pour recenser les outils de réaction et de rétablissement nécessaires pour atténuer et contenir les incidents de cybersécurité majeurs, ainsi que les capacités de réaction nécessaires pour décourager et prévenir de nouveaux incidents.

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

(6) La recommandation (UE) 2017/1584 de la Commission[3] sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs énonce les objectifs et les modalités de coopération entre les États membres et les entités de l'Union dans les réactions aux incidents et aux crises de cybersécurité majeurs. Elle a cartographié les acteurs concernés aux niveaux technique, opérationnel et politique et expliqué comment ils étaient intégrés dans les mécanismes existants de gestion des crises de l'Union, comme les dispositions relatives à l'IPCR. Les principes fondamentaux énoncés dans la recommandation (UE) 2017/1584 restent valables, à savoir la subsidiarité, la complémentarité et la confidentialité des informations, ainsi que l'approche à trois niveaux (technique, opérationnel et politique). La présente recommandation s'appuie sur ces principes fondamentaux et vise à remplacer la recommandation (UE) 2017/1584, en établissant un nouveau cadre de l'Union pour la gestion des crises de cybersécurité.

(7) Certaines définitions utilisées dans la présente recommandation sont fondées sur les définitions et termes utilisés dans la directive (UE) 2022/2555[4]. Toutefois, le champ d'application de la présente recommandation est différent de celui de la directive (UE) 2022/2555. La présente recommandation définit le cadre de l'Union pour la gestion des crises de cybersécurité dans le contexte de la préparation globale de l'UE aux incidents de cybersécurité majeurs et aux crises de cybersécurité découlant de tels incidents, indépendamment du secteur ou de l'entité concerné. Dans la mesure du possible, les définitions sont fondées sur celles qui figurent dans la directive (UE) 2022/2555.

---

[3] 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).

[4] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80).

(8) Un schéma directeur en matière de cybersécurité actualisé est nécessaire pour fournir des orientations claires et accessibles expliquant ce qu'est un incident de cybersécurité majeur ou une crise de cybersécurité au niveau de l'Union, la manière dont le cadre de gestion des crises est déclenché et le rôle des réseaux, acteurs et mécanismes pertinents au niveau de l'Union, ainsi que l'interaction entre ces acteurs et mécanismes tout au long du cycle de vie des crises de cybersécurité. Le schéma directeur en matière de cybersécurité vise à soutenir le cadre plus large des relations civilo-militaires de l'UE dans le contexte de la gestion des crises de cybersécurité, y compris dans le contexte de l'approfondissement des relations entre l'UE et l'OTAN, dans la mesure du possible, notamment au moyen de mécanismes d'échange d'informations renforcés inclusifs, réciproques et non discriminatoires dans la gestion des crises de cybersécurité.

(9) La gestion transsectorielle des crises au niveau de l'Union devrait être renforcée afin de permettre une réaction intégrée en cas de crise, en particulier dans les cas où les incidents et crises de cybersécurité majeurs ont des conséquences physiques. La présente recommandation complète les dispositions relatives à l'IPCR et d'autres mécanismes de crise de l'Union, dont le système général d'alerte rapide ARGUS de la Commission, le mécanisme de protection civile de l'Union (MPCU) soutenu par le centre de coordination de la réaction d'urgence (ERCC) créé dans le cadre du MPCU par la décision no 1313/2013/UE du Parlement européen et du Conseil relative au mécanisme de protection civile de l'Union[5] (ci-après la "décision relative au MPCU"), le mécanisme de réaction aux crises (CRM) du SEAE, ainsi que d'autres processus, tels que ceux décrits dans la boîte à outils cyberdiplomatique de l'UE[6], dans la boîte à outils hybride[7] et dans le protocole opérationnel révisé de l'UE pour la lutte contre les menaces hybrides[8]. Elle complète également la recommandation du Conseil (UE) 2024/4371 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[9] (ci-après le "schéma directeur de l'UE pour les infrastructures critiques"), qui couvre la résilience physique, autre que cyber, et qui vise à améliorer la coordination de la réaction au niveau de l'Union dans ce domaine, et devrait être cohérente avec cette recommandation.

---

5 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).

6 Conclusions du Conseil relatives à un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance (9916/17).

7 Conclusions du Conseil sur un cadre pour une réponse coordonnée de l'UE aux campagnes hybrides, 22 juin 2022.

8 Document de travail conjoint - Protocole opérationnel de l'Union européenne de lutte contre les menaces hybrides (SWD(2023) 116 final).

9 JO C, C/2024/4371, 5.7.2024.

(10) Le réseau européen pour la préparation et la gestion des crises cyber (ci-après "EU-CyCLONe)" est le réseau de coordination de la gestion des incidents et crises de cybersécurité majeurs au niveau opérationnel, y compris en cas d'incident ou de crise de cybersécurité majeur transsectoriel. Afin de ne pas compliquer davantage les cadres existants, il convient d'éviter la création de structures sectorielles qui feraient double emploi avec les tâches d'EU-CyCLONe. EU-CyCLONe devrait également recevoir des informations opérationnelles liées à la cybersécurité provenant des secteurs concernés et les transmettre au niveau politique.

(11) Les États membres sont encouragés à utiliser pleinement les ressources financières disponibles pour la cybersécurité prévues par les programmes pertinents de l'Union. Il convient de veiller à ce que ces programmes imposent des charges administratives minimales aux demandeurs de financement et à ce que la participation des États membres à ces programmes soit facilitée en fournissant des orientations pertinentes sur les options de soutien financier viables.

(12) La présente recommandation contribue aux actions plus larges de préparation requises pour l'Union face aux crises transsectorielles, conformément aux principes inscrits dans la stratégie de l'UE pour une union de la préparation, à savoir une approche intégrée tous risques, pangouvernementale et pansociétale, en particulier en ce qui concerne l'amélioration de la sensibilisation aux risques et aux menaces et la réaction transsectorielle aux crises.

A ADOPTÉ LA PRÉSENTE RECOMMANDATION:

I: Objectif, champ d'application et principes directeurs du cadre de l'UE relatif à la gestion des crises de cybersécurité

Objectif et champ d'application

1) La présente recommandation relative à un schéma directeur de l'UE pour la gestion des crises de cybersécurité (ci-après le "schéma directeur en matière de cybersécurité") définit le cadre de l'Union relatif à la gestion des crises de cybersécurité dans le contexte de la préparation globale de l'UE aux incidents de cybersécurité majeurs et aux crises de cybersécurité. Le cadre reflète les rôles des États membres et des institutions, organes et organismes de l'Union (ci-après les "entités de l'Union") dans le cadre de leurs compétences respectives, dans le plein respect des législations nationales et des règles internes, afin de garantir une action globale et coordonnée au niveau de l'Union.

2) Le schéma directeur en matière de cybersécurité devrait être appliqué en cohérence avec le schéma directeur de l'UE pour les infrastructures critiques, en particulier en cas d'incidents affectant à la fois la résilience physique et la cybersécurité des infrastructures critiques[10].

3) Le schéma directeur en matière de cybersécurité fournit des orientations pour la réaction aux incidents de cybersécurité majeurs ou aux crises de cybersécurité, et il devrait être utilisé en complément de tout mécanisme de réaction sectoriel pertinent, tels que ceux énumérés à l'annexe II. Les parties prenantes concernées en matière de cybersécurité devraient contribuer à la réalisation des objectifs de ces mécanismes sectoriels, tant au niveau national qu'au niveau de l'Union.

4) En cas de crise transsectorielle à l'échelle de l'UE caractérisée par des aspects cyber pour lesquels l'IPCR est activé, la coordination de la réaction au niveau politique de l'Union devrait être assurée par le Conseil, au moyen des dispositions relatives à l'IPCR. Lorsque l'IPCR a été activé, les mesures relevant du schéma directeur en matière de cybersécurité devraient soutenir la réaction de l'UE au niveau politique, en fournissant un soutien spécifique en matière de cybersécurité.

---

[10] Le schéma directeur de l'UE pour les infrastructures critiques définit plus précisément la coordination dans de tels cas à la partie I, section 4, de son annexe.

Principes directeurs

5) Les principes directeurs suivants s'appliquent à la gestion des crises de cybersécurité au niveau de l'Union:

a) *Proportionnalité*: la majorité des incidents de cybersécurité touchant les États membres ont une portée inférieure à celle qui permettrait de les considérer comme un incident de cybersécurité majeur ou une crise de cybersécurité au niveau national ou de l'Union. En cas d'incidents et de menaces en matière de cybersécurité, les États membres coopèrent et échangent régulièrement des informations, sur une base volontaire, au sein du réseau des centres de réponse aux incidents de sécurité informatiques (ci-après le "réseau des CSIRT") et d'EU-CyCLONe, conformément aux instructions permanentes des réseaux.

b) *Subsidiarité*: c'est aux États membres qu'il appartient au premier chef de répondre et de remédier aux incidents de cybersécurité, aux incidents de cybersécurité majeurs ou aux crises de cybersécurité qui les touchent. En tenant compte d'éventuels effets transfrontières, le Conseil, la Commission, le haut représentant, l'Agence de l'Union européenne pour la cybersécurité (ENISA), le service de cybersécurité pour les institutions, organes et organismes de l'Union (CERT-UE), Europol et toutes les autres entités concernées de l'Union devraient coopérer tout au long du cycle de vie d'une crise. Ce rôle découle du droit de l'Union et met en évidence la manière dont les incidents de cybersécurité majeurs et les crises de cybersécurité ont une incidence sur un ou plusieurs secteurs de l'activité économique au sein du marché unique, sur la sécurité et les relations internationales de l'Union ainsi que sur les entités de l'Union elles-mêmes.

c) *Complémentarité*: la présente recommandation tient pleinement compte des mécanismes existants de gestion des crises au niveau de l'Union énumérés à l'annexe II, en particulier le dispositif IPCR, ARGUS, et le mécanisme de réaction aux crises du SEAE. La présente recommandation tient compte des mandats du réseau des CSIRT et d'EU-CyCLONe, ainsi que du règlement (UE, Euratom) 2023/2841. Lorsque l'IPCR est activé, les travaux des réseaux, entités et mécanismes sectoriels activés concernés devraient se poursuivre et devraient alimenter et soutenir la coordination politique et stratégique en cours au sein de l'IPCR.

d) *Confidentialité des informations*: tous les échanges d'informations ayant lieu dans le contexte de la présente recommandation devraient respecter les règles applicables en matière de sécurité et de protection des données à caractère personnel. Les accords informels de non-divulgation, tels que le protocole d'échange d'information "Traffic Light Protocol" pour l'étiquetage des informations sensibles, devraient être pris en compte, le cas échéant. Aux fins de l'échange d'informations classifiées, quel que soit le régime de classification appliqué, les règles et accords contraignants existants sur le traitement des informations classifiées devraient être utilisés parallèlement aux outils agréés disponibles.

6) Conformément aux principes directeurs susmentionnés, les États membres et les entités de l'Union devraient approfondir leur coopération en matière de gestion des crises de cybersécurité, en favorisant la confiance mutuelle et en s'appuyant sur les réseaux et mécanismes existants. Cette coopération, dans le cadre du schéma directeur en matière de cybersécurité, bénéficie de la mise en œuvre des articles 22 et 23 du règlement (UE, Euratom) 2023/2841. En particulier, le plan de gestion des crises de cybersécurité établi sur la base de l'article 23 du règlement (UE, Euratom) 2023/2841 contribue, entre autres, à l'échange régulier d'informations pertinentes entre les entités de l'Union et avec les États membres, et définit les modalités de coordination et de flux d'informations entre les entités de l'Union.

II: Définitions

7) Aux fins de ce schéma directeur en matière de cybersécurité, on entend par:

a) "incident": un événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles;

b) "incident important": un incident qui:

a. a causé ou est susceptible de causer une perturbation opérationnelle grave des services ou des pertes financières pour l'entité concernée;

b. a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables;

c) "incident de cybersécurité majeur": un incident qui provoque des perturbations dépassant les capacités de réaction du seul État membre concerné ou qui a un impact important sur au moins deux États membres;

d) "crise de cybersécurité": un incident de cybersécurité majeur qui a dégénéré en une crise à part entière, empêchant le bon fonctionnement du marché intérieur ou présentant de graves risques de sûreté et de sécurité publiques pour les entités ou les citoyens dans plusieurs États membres ou dans l'Union dans son ensemble.

III: Structures et responsabilités nationales de gestion des crises de cybersécurité

8) C'est aux États membres qu'il appartient au premier chef de répondre aux incidents de cybersécurité majeurs ou aux crises de cybersécurité qui les touchent. Conformément à la directive (UE) 2022/2555, chaque État membre dispose d'une ou de plusieurs autorités de gestion des crises de cybersécurité, ainsi que d'un ou de plusieurs CSIRT.

9) Grâce à l'adoption de la directive (UE) 2022/2555 et d'autres instruments législatifs et non législatifs en matière de cybersécurité, les États membres ont aligné leurs cadres de cybersécurité en définissant des règles minimales concernant le fonctionnement du cadre réglementaire coordonné, en établissant des mécanismes permettant une coopération efficace entre les autorités compétentes de chaque État membre et en prévoyant des recours et des mesures d'exécution effectifs, qui sont essentiels à l'exécution effective de ces obligations.

10) Conformément à l'article 9, paragraphe 4, de la directive (UE) 2022/2555, les États membres devraient adopter des plans nationaux de réaction aux crises et incidents de cybersécurité majeurs. Ces plans comprennent, entre autres, des mesures de préparation nationales, des procédures de gestion des crises de cybersécurité et des procédures et arrangements nationaux entre les autorités et organismes nationaux visant à garantir leur participation et leur soutien effectifs à la gestion coordonnée des incidents de cybersécurité majeurs et des crises de cybersécurité au niveau de l'Union. Les procédures de gestion des crises de cybersécurité incluent également des dispositions sur leur intégration dans le cadre national général de gestion des crises et les canaux d'échange d'informations.

11) Conformément à l'article 9, paragraphe 1, de la directive (UE) 2022/2555, les États membres devraient veiller à la cohérence avec les cadres nationaux existants pour la gestion générale des crises. En cas d'activation de l'IPCR, les autorités nationales de gestion des crises devraient, aux fins d'informer l'IPCR, recueillir des contributions auprès des autorités de gestion des crises de cybersécurité et des mécanismes sectoriels de gestion des crises au niveau national.

12) Conformément à l'article 9, paragraphe 5, de la directive (UE) 2022/2555, EU-CyCLONe devrait, à la demande d'un État membre concerné, échanger des informations sur les parties pertinentes des plans nationaux d'intervention en cas d'incident de cybersécurité majeur et de crise, en particulier sur les dispositions visant à garantir la participation et le soutien effectifs à la gestion coordonnée des incidents de cybersécurité majeurs et des crises de cybersécurité au niveau de l'Union, afin d'échanger les meilleures pratiques et d'examiner si le cadre global fonctionnerait dans la pratique.

13) EU-CyCLONe et le conseil interinstitutionnel de cybersécurité (IICB) sont invités à échanger, le cas échéant, sur la cohérence du plan de gestion des crises établi par l'IICB conformément à l'article 23 du règlement (UE, Euratom) 2023/2841 avec les plans nationaux d'intervention en cas d'incident de cybersécurité majeur et de crise.

14) EU-CyCLONe, avec le soutien de l'ENISA en tant que secrétariat, devrait tenir à jour une liste des autorités nationales de gestion des crises de cybersécurité avec les coordonnées des responsables et des organes exécutifs d'EU-CyCLONe, et la mettre à la disposition des membres d'EU-CyCLONe.

IV: Principaux réseaux et acteurs de l'écosystème de l'UE en matière de gestion des crises de cybersécurité

15) Le réseau des CSIRT est le principal réseau technique pour échanger des informations pertinentes sur les incidents, en particulier dans le champ d'application de la présente recommandation, conformément aux tâches pertinentes décrites à l'article 15, paragraphe 3, de la directive (UE) 2022/2555. Il contribue au renforcement de la confiance et promeut une coopération opérationnelle rapide et efficace entre les États membres. Le président du réseau des CSIRT peut participer en tant qu'observateur à l'IICB.

16) Le CERT-UE est le service de cybersécurité pour toutes les entités de l'Union. Le CERT-UE fait office de pôle d'échange d'informations sur la cybersécurité et de coordination des réponses aux incidents pour les entités de l'Union conformément à l'article 13 du règlement (UE/Euratom) 2023/2841. Le CERT-UE est membre du réseau des CSIRT et soutient la Commission au sein du réseau EU-CyCLONe. Le CERT-UE opère au niveau technique et est chargé de coordonner la gestion des incidents majeurs affectant les entités de l'Union.

17) EU-CyCLONe sert d'intermédiaire entre le niveau technique et le niveau politique, en particulier lors d'incidents de cybersécurité majeurs et de crises de cybersécurité. EU-CyCLONe contribue à la gestion coordonnée, au niveau opérationnel, des incidents de cybersécurité majeurs et des crises de cybersécurité, et garantit l'échange régulier d'informations pertinentes entre les États membres et les institutions, organes et organismes de l'Union, conformément à l'article 16 de la directive (UE) 2022/2555. Le président du réseau EU-CyCLONe peut participer en tant qu'observateur à l'IICB.

18) L'ENISA est l'agence de l'Union qui exécute les tâches assignées par le règlement (UE) 2019/881[11] dans le but de parvenir à un niveau commun élevé de cybersécurité dans l'ensemble de l'Union, y compris en aidant activement les États membres et les institutions, organes et organismes de l'Union. L'ENISA assure, entre autres, le secrétariat du réseau des CSIRT et d'EU-CyCLONe, des services d'appréciation de la situation, et aide les États membres en organisant régulièrement des exercices de cybersécurité au niveau de l'Union. Conformément à la directive (UE) 2022/2555 et au règlement (UE) 2024/2847[12], l'ENISA reçoit des informations sur les incidents transfrontières importants, les vulnérabilités exploitées activement et les incidents affectant les produits numériques.

19) Le Conseil de l'Union européenne (ci-après le "Conseil") est l'institution exerçant des fonctions de définition des politiques et de coordination conformément à l'article 16 du traité sur l'Union européenne (TUE) et se voit confier l'IPCR qui concerne la coordination et la réaction au niveau politique de l'Union. Le Conseil opère par l'intermédiaire des formations du Conseil, du Comité des représentants permanents et des instances préparatoires compétentes du Conseil, en particulier le groupe horizontal "Questions cyber" (GHQC), ainsi que, le cas échéant, du dispositif IPCR.

---

11 Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

12 Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) nº 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience) (JO L, 2024/2847, 20.11.2024, p. 1).

20) La Commission, en tant qu'institution promouvant l'intérêt général de l'Union, prenant les initiatives appropriées à cette fin et assurant l'application des traités et des mesures adoptées par les institutions en vertu de l'article 17 du TUE, est responsable de certaines actions générales de préparation au niveau de l'Union et de certaines actions d'appréciation de la situation, y compris la gestion de l'ERCC et du système commun de communication et d'information d'urgence (CECIS), conformément à la décision relative au MPCU. Elle facilite la cohérence et la coordination entre les actions connexes de réaction aux crises menées à l'échelle de l'Union au niveau opérationnel. Elle est consultée sur les décisions d'activer ou de désactiver l'IPCR. Les services de la Commission élaborent, avec le SEAE, les rapports ISAA. La Commission participe aux activités d'EU-CyCLONe en qualité de membre en cas d'incident de cybersécurité majeur, potentiel ou en cours, qui a ou est susceptible d'avoir un impact important sur les services et les activités relevant du champ d'application de la directive (UE) 2022/2555, et en qualité d'observateur dans les autres cas. C'est le point de contact pour EU-CyCLONe au sein de l'IICB. Elle participe au réseau des CSIRT en qualité d'observateur.

21) Le haut représentant pour les affaires étrangères et la politique de sécurité (ci-après le "haut représentant"), assisté par le SEAE, conduit la politique étrangère et de sécurité commune (PESC) de l'Union et contribue par ses propositions au développement de cette politique, y compris la politique de sécurité et de défense commune (PSDC). Cela inclut notamment les structures et mécanismes diplomatiques, de renseignement et militaires, notamment la capacité unique d'analyse du renseignement (SIAC) en tant que point d'entrée unique pour le renseignement dans les États membres, l'État-major de l'UE (EMUE) en tant que source d'expertise militaire, la boîte à outils cyberdiplomatique de l'UE, ainsi que le réseau des délégations de l'UE, qui peuvent contribuer à la gestion des crises à partir d'une dimension extérieure. Le SEAE élabore également, avec la Commission, les rapports ISAA.

22) L'annexe II décrit les rôles et les compétences des acteurs concernés au niveau de l'Union en ce qui concerne la gestion des crises de cybersécurité, y compris les principaux réseaux et acteurs.

V: Se préparer à des incidents de cybersécurité majeurs et à une crise de cybersécurité

Panorama des menaces

23) Les États membres et les entités concernées de l'Union devraient prendre les mesures nécessaires pour améliorer l'appréciation de la situation, en reconnaissant que le panorama des menaces et l'appréciation de la situation propre à un incident nécessitent des modes d'opération distincts. Les États membres et les entités concernées de l'Union devraient travailler ensemble sur la base de données vérifiées et fiables, y compris les tendances en matière d'incidents, de tactiques, de techniques et de procédures, et les vulnérabilités activement exploitées.

24) Lorsqu'ils partagent des informations au niveau de l'UE, les États membres devraient tirer pleinement parti des plateformes existantes de coopération technique et opérationnelle, telles que celles utilisées par le réseau des CSIRT et le réseau EU-CyCLONe.

25) Afin d'améliorer l'appréciation commune de la situation et de faciliter l'évaluation de l'incidence sur l'UE, le réseau EU-CyCLONe et le réseau des CSIRT, avec le soutien de l'ENISA, devraient recourir au mécanisme d'information convenu en interne pour produire une vue d'ensemble, à l'échelle de l'Union, des activités techniques et opérationnelles sur la base des informations recueillies au niveau national.

26) Le réseau EU-CyCLONe et le réseau des CSIRT devraient:

a) coopérer pour améliorer le partage d'informations entre les niveaux technique et opérationnel et l'appréciation de la situation dans son ensemble;

b) continuer à instaurer un climat de confiance entre leurs membres et entre les réseaux;

c) tirer pleinement parti des outils disponibles pour le partage d'informations, avec le soutien de l'ENISA, et réfléchir à la manière d'améliorer ces outils et d'assurer l'interopérabilité entre les réseaux.

27) Le réseau EU-CyCLONe, le réseau des CSIRT et l'IICB devraient coopérer pour assurer un échange efficace d'informations pertinentes.

28) L'ENISA, en tant que secrétariat du réseau des CSIRT et du réseau EU-CyCLONe, joue un rôle central en aidant les États membres et les institutions, organes et organismes de l'Union à parvenir à une appréciation commune de la situation de l'UE au niveau technique et opérationnel afin de soutenir la préparation aux incidents et crises de cybersécurité majeurs.

29) Conformément à la directive (UE) 2022/2555 et au règlement (UE) 2019/881, les États membres et les entités concernées de l'Union devraient se coordonner avec le secteur privé, y compris les communautés et les fabricants de logiciels libres, afin d'améliorer le partage d'informations. En particulier, l'ENISA devrait utiliser son programme de partenariat à cet effet. En outre, les États membres et les entités concernées de l'Union pourraient également s'appuyer sur les centres d'échange et d'analyse d'informations (ISAC) existants au niveau de l'UE et au niveau national, afin de renforcer les capacités en matière de cybersécurité et de réagir aux incidents de cybersécurité, y compris au moyen de réunions conjointes du secteur privé avec le réseau EU- CyCLONe et le réseau des CSIRT.

30) Afin d'améliorer le partage d'informations entre les réseaux et en leur sein, et de clarifier les attentes mutuelles concernant un tel partage, le réseau EU-CyCLONe devrait, avec le soutien de l'ENISA en tant que secrétariat et après consultation du réseau des CSIRT et du groupe de coopération SRI, convenir, dans les 24 mois suivant l'adoption de la présente recommandation, d'une taxinomie commune et harmonisée pour les niveaux de gravité des incidents. Cette taxinomie devrait permettre de comparer la gravité des incidents d'un État membre à l'autre en tenant compte de l'impact sur la prestation de services, du nombre d'entités touchées et de leur importance respective, de l'incidence sur d'autres services et infrastructures, ainsi que des dommages monétaires, politiques et de réputation infligés. Elle devrait s'appuyer sur des barèmes ou des taxinomies pertinents déjà disponibles, telles que la taxinomie de classification des incidents de référence.

Niveau technique

31) Le réseau des CSIRT est la plateforme de coopération technique et de partage d'informations entre tous les États membres et, par l'intermédiaire du CERT-UE, avec les entités de l'Union.

32) Conformément à la directive (UE) 2022/2555, chaque CSIRT a pour mission de surveiller et d'analyser les cybermenaces, les vulnérabilités et les incidents au niveau national. Les CSIRT devraient échanger, à la fois au sein du réseau des CSIRT et de manière bilatérale, des informations pertinentes sur les incidents, les incidents évités de justesse, les cybermenaces, les risques et les vulnérabilités, afin de parvenir à une appréciation commune de la situation.

33) Afin de renforcer la coopération opérationnelle au niveau de l'Union, le réseau des CSIRT devrait envisager d'inviter les organes et organismes de l'Union associés à la politique de cybersécurité, tels qu'Europol, à participer à ses travaux.

34) Conformément au règlement (UE) 2023/2841, le CERT-UE devrait recueillir, gérer, analyser et partager des informations avec les institutions, organes et organismes de l'Union en ce qui concerne les cybermenaces, les vulnérabilités et les incidents relatifs aux infrastructures TIC non classifiées et soumettre, le cas échéant, des propositions spécifiques à l'IICB en vue de l'adoption d'orientations et de recommandations destinées aux institutions, organes et organismes de l'Union. Le CERT-UE devrait coopérer et échanger des informations avec ses homologues des États membres, y compris au moyen du réseau des CSIRT.

Niveau opérationnel

35) Conformément à la directive (UE) 2022/2555, le réseau EU-CyCLONe devrait servir de plateforme de coopération entre les autorités des États membres en matière de gestion des crises de cybersécurité et, par l'intermédiaire de la Commission, avec les entités concernées de l'Union, dans le but de renforcer le niveau de préparation à la gestion des incidents de cybersécurité majeurs et des crises de cybersécurité et de développer une appréciation commune de la situation en cas d'incidents de cybersécurité majeurs et de crises de cybersécurité.

36) Conformément à la directive (UE) 2022/2555 et au règlement (UE) 2024/2847, l'ENISA reçoit des informations sur les incidents importants ayant une dimension transfrontière, les vulnérabilités activement exploitées et les incidents affectant les produits numériques. L'ENISA, agissant en tant que secrétariat, devrait conseiller le réseau des CSIRT et le réseau EU-CyCLONe dans le but d'aider les réseaux à déterminer si d'autres mesures devraient être prises et de contribuer à l'appréciation commune de la situation.

Niveau politique

37) Les États membres et les entités concernées de l'Union devraient surveiller les évolutions internationales qui ont une incidence sur la cybersécurité (y compris les cybermenaces, les menaces hybrides et les activités de manipulation de l'information et d'ingérence menées depuis l'étranger, y compris la désinformation, le cas échéant). Des initiatives telles que les rapports de situation technique en matière de cybersécurité de l'UE, les analyses fournies dans le cadre de la SIAC et d'autres produits pertinents fournissant des indications spécialisées devraient être prises en compte.

38) Le haut représentant devrait continuer à informer les États membres et à les associer aux efforts diplomatiques de l'Union concernant les cybermenaces, en particulier lorsque des acteurs étatiques sont impliqués, à son dialogue avec des pays tiers et des organisations internationales, y compris l'OTAN, et à la mise en œuvre de mesures diplomatiques, y compris de mesures restrictives.

39) La présidence du Conseil de l'Union européenne pourrait créer une page de surveillance sur la plateforme web de l'IPCR, où les États membres et les institutions et organes de l'UE pourraient échanger des informations sur une crise susceptible de se développer.

Exercices communs

40) La Commission, en coordination avec le haut représentant et avec le soutien de l'ENISA, après consultation du réseau EU-CyCLONe et du réseau des CSIRT, devrait élaborer un programme annuel continu efficace d'exercices de cybersécurité afin de se préparer aux crises de cybersécurité et d'améliorer l'efficacité organisationnelle. Le programme continu d'exercices de cybersécurité devrait tenir compte des exercices du MPCU et d'autres exercices de mécanismes de réaction aux crises au niveau de l'Union, y compris l'exercice décrit dans le schéma directeur de l'UE pour les infrastructures critiques. Le premier programme continu devrait être élaboré dans les douze mois suivant l'adoption du schéma directeur en matière de cybersécurité, les programmes ultérieurs devant être achevés au plus tard le 31 mars de chaque année. Le programme continu devrait être soumis au Conseil pour information.

41) Le programme continu devrait également couvrir les exercices élaborés à l'aide des scénarios d'évaluation des risques coordonnées au niveau de l'UE. Il devrait couvrir des exercices faisant intervenir tous les acteurs concernés, en particulier le secteur privé et l'OTAN.

42) L'ENISA, dans son rôle de secrétariat du réseau des CSIRT et du réseau EU-CyCLONe, devrait veiller à la collecte systématique des enseignements tirés des exercices, ainsi qu'à recenser les actions qui en résultent et à proposer des modalités de mise en œuvre de celles-ci, afin d'en garantir l'exécution effective et l'incidence positive sur la résilience commune de l'UE, y compris en ce qui concerne les instructions permanentes respectives.

43) L'ensemble des acteurs et des réseaux devraient améliorer leur coordination en cas d'incident de cybersécurité majeur ou de crise de cybersécurité, sur la base des enseignements tirés des exercices. En particulier, le réseau EU-CyCLONe et le réseau des CSIRT devraient relever les défis recensés lors des exercices afin d'améliorer la coordination, notamment en ce qui concerne la coopération entre les réseaux, et, si nécessaire, adapter rapidement les instructions permanentes.

44) Le groupe de coopération SRI devrait inviter le réseau des CSIRT, le réseau EU-CyCLONe et l'ENISA à présenter les enseignements tirés des exercices, ainsi qu'à recenser les actions qui en résultent et à en proposer des modalités proposées de mise en œuvre.

45) Le Conseil peut inviter les présidents du réseau des CSIRT, du réseau EU-CyCLONe, du groupe de coopération SRI et de l'ENISA, à présenter la manière dont les enseignements tirés des exercices ont été mis en œuvre.

46) L'ENISA, en coopération avec la Commission et le haut représentant, est invitée à organiser un exercice pour tester le schéma directeur en matière de cybersécurité lors du prochain exercice Cyber Europe. L'exercice devrait associer tous les acteurs concernés, y compris au niveau politique. L'ENISA est invitée à coordonner avec la présidence du Conseil de l'Union européenne l'intervention du niveau politique. L'exercice peut également inclure le secteur privé et l'OTAN.

VI: Détecter un incident susceptible d'évoluer vers un incident de cybersécurité majeur ou une crise de cybersécurité

47) Conformément à leurs mandats respectifs et sur la base de l'approche "tous risques", tous les acteurs devraient communiquer aux réseaux concernés des informations indiquant un possible incident de cybersécurité majeur ou une crise de cybersécurité.

48) Conformément au règlement (UE) 2025/38[13], lorsque les cyberpôles transfrontières obtiennent des informations relatives à un incident de cybersécurité majeur potentiel ou en cours, ils devraient veiller à ce que des informations pertinentes soient fournies sans retard injustifié aux autorités des États membres et à la Commission par l'intermédiaire du réseau EU-CyCLONe et du réseau des CSIRT aux fins d'une appréciation commune de la situation.

[13] Règlement (UE) 2025/38 du Parlement européen et du Conseil du 19 décembre 2024 établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les cybermenaces et incidents, de s'y préparer et d'y réagir et modifiant le règlement (UE) 2021/694 (règlement sur la cybersolidarité) JO L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj.

49) Lorsqu'un incident important est observé, en particulier lorsqu'il a un impact immédiat, il peut être notifié ou détecté par un CSIRT, ainsi que par les autorités des États membres en matière de gestion des crises de cybersécurité ou par d'autres autorités sectorielles. Les États membres sont encouragés à partager les informations relatives à cet incident avec les réseaux, qui devraient envisager de prendre les mesures qui s'imposent. L'activation du réseau des CSIRT et celle du réseau EU-CyCLONe peuvent être indépendantes l'une de l'autre en fonction de la nature de l'incident et de la réponse requise. Toutefois, les deux réseaux sont encouragés à poursuivre leur coopération sur la base de modalités procédurales convenues. La décision d'activer repose uniquement et indépendamment sur chaque réseau respectif.

50) Le réseau des CSIRT devrait conseiller le réseau EU-CyCLONe sur la question de savoir si un incident de cybersécurité observé peut être considéré comme un incident de cybersécuroté majeur potentiel ou en cours.

51) Comme indiqué dans la directive (UE) 2022/2555, le réseau des CSIRT et le réseau EU-CyCLONe devraient établir des modalités procédurales en cas d'incident de cybersécurité majeur potentiel ou en cours, afin de garantir une coordination technico-opérationnelle et des informations pertinentes en temps utile au niveau politique.

VII: Réagir à un incident de cybersécurité majeur ou à une crise de cybersécurité au niveau de l'Union

Réaction à un incident de cybersécurité majeur ou à une crise de cybersécurité pour lesquels l'IPCR n'est pas en mode "activation totale"

52) L'efficacité de la réaction à des incidents de cybersécurité majeurs ou à des crises de cybersécurité au niveau de l'UE dépend de l'efficacité de la coopération technique, opérationnelle et politique dans le cadre d'une approche pangouvernementale, qui inclut dans la mesure du possible les services répressifs.

53) À chaque niveau, les acteurs concernés devraient mener des activités spécifiques pour parvenir à une appréciation commune de la situation et à une réponse coordonnée. De telles mesures assurent une diffusion ordonnée et efficace des informations.

54) La réaction devrait être adaptée à l'impact de l'incident de cybersécurité majeur ou de la crise de cybersécurité Conformément à la directive (UE) 2022/2555, les autorités de gestion des crises de cybersécurité des États membres devraient veiller à la cohérence et la coordination nationales entre les réactions sectorielles à la crise de cybersécurité.

55) En cas d'incident de cybersécurité majeur ou de crise de cybersécurité, tous les acteurs et réseaux devraient réagir en étroite coordination, comme suit:

a) au niveau technique:

i. les États membres concernés et leurs CSIRT devraient coopérer avec les entités concernées pour réagir aux incidents et fournir une assistance, le cas échéant;

ii. les CSIRT devraient coopérer via leur réseau pour partager les informations techniques pertinentes relatives à l'incident; les CSIRT coopèrent dans le cadre de leurs efforts d'analyse des éléments techniques disponibles et d'autres informations techniques liées à l'incident, en vue d'en déterminer la cause et de définir les mesures techniques d'atténuation envisageables;

iii. lorsqu'un CSIRT ou l'autorité de gestion des crises de cybersécurité d'un État membre prend connaissance d'un incident important, il ou elle est encouragé(e) à le faire savoir dans le cadre du réseau des CSIRT ou d'EU-CyCLONe;

iv. le réseau des CSIRT, avec le soutien de l'ENISA, devrait établir une compilation des rapports nationaux fournis par les CSIRT, qu'il convient de présenter à EU-CyCLONe;

v. lorsqu'un incident de cybersécurité est susceptible d'évoluer vers un incident de cybersécurité majeur ou une crise de cybersécurité, le réseau des CSIRT devrait partager les informations appropriées avec EU-CyCLONe. EU-CyCLONe devrait utiliser ces informations pour informer le Conseil;

vi. le réseau des CSIRT devrait être en contact étroit avec Europol afin de veiller à l'échange d'informations techniques pertinentes. Le réseau des CSIRT et Europol devraient établir des points de contact pour renforcer le partage d'informations lorsque cela est pertinent en cas d'incident de cybersécurité majeur;

b) au niveau opérationnel:

i. les États membres devraient atténuer l'impact de l'incident au niveau national au moyen de mesures appropriées;

ii. le réseau des CSIRT devrait fournir à EU-CyCLONe des évaluations techniques des incidents en cours, qui peuvent être utilisées par EU-CyCLONe;

iii. il convient qu'EU-CyCLONe évalue les conséquences et l'impact des incidents de cybersécurité majeurs et crises de cybersécurité concernés, propose de possibles mesures d'atténuation et soutienne la gestion coordonnée des incidents de cybersécurité majeurs et des crises de cybersécurité, ainsi que la prise de décision au niveau politique;

iv. dans l'hypothèse où un incident de cybersécurité majeur ayant des effets transsectoriels nécessiterait l'activation d'actions de réaction au niveau de l'Union, en particulier les mécanismes horizontaux et sectoriels pertinents de gestion des crises au niveau de l'Union énumérés à l'annexe II,

(a) les acteurs appropriés peuvent, en fonction du type de mécanisme sectoriel de gestion des crises au niveau de l'Union, demander l'activation dudit mécanisme;

(b) en cas d'activation d'un tel mécanisme sectoriel, les entités concernées aident les entités sectorielles à atténuer l'impact de l'incident;

(c) la Commission devrait faciliter la circulation des informations nécessaires entre les points de contact pour les mécanismes horizontaux et sectoriels pertinents de gestions des crises au niveau de l'Union énumérés à l'annexe II et EU-CyCLONe, et devrait mener une analyse transsectorielle intégrée et proposer des options pour un plan de réaction intégré approprié;

(d) la Commission, par l'intermédiaire d'EU-CyCLONe, le cas échéant, en coopération avec le haut représentant, devrait veiller à la cohérence et à la coordination des mesures opérationnelles au niveau de l'UE dans le domaine cyber avec les actions de réaction connexes au niveau de l'Union, en particulier en ce qui concerne les demandes d'assistance au titre du MPCU;

(e) si une page de surveillance relative à l'IPCR a été lancée, des informations sur l'incident, son impact et les mesures prises devraient également être partagées entre les États membres et les entités de l'Union via la plateforme web de l'IPCR;

v. les États membres peuvent demander des services à la réserve de cybersécurité de l'Union conformément à l'article 15 du règlement (UE) 2025/38. Sans préjudice de tout futur acte d'exécution au titre dudit règlement, les services de la réserve de cybersécurité de l'Union devraient être déployés dans les 24 heures suivant la demande;

c) au niveau politique:

i. le Conseil peut demander des informations aux principales parties prenantes, en particulier à la Commission, au haut représentant et à EU-CyCLONe, afin d'assurer une réaction politique et stratégique appropriée;

ii. le Conseil, avec le soutien de la Commission et du haut représentant, pourrait décider des mesures appropriées pour réagir à l'incident de cybersécurité majeur, y compris les éventuelles réponses diplomatiques conformément au chapitre IX;

iii. les États membres peuvent activer des mécanismes ou instruments supplémentaires de gestion des crises de cybersécurité en fonction de la nature et de l'impact de l'incident;

iv. lorsque l'IPCR est activé en mode "partage de l'information", la capacité de soutien à l'ISAA est déclenchée, ce qui accroît les échanges d'informations via la plateforme web de l'IPCR et assure une vue d'ensemble commune de la situation. Les rapports de situation d'EU-CyCLONe et du réseau des CSIRT devraient rester les principaux instruments présentant l'appréciation commune de la situation aux niveaux opérationnel et technique, respectivement. Ces rapports peuvent servir de base aux rapports ISAA;

v. en cas d'incident nécessitant l'activation d'actions de réaction au niveau de l'Union, en particulier les mécanismes horizontaux et sectoriels pertinents de gestion des crises au niveau de l'Union énumérés à l'annexe II, le Conseil, en coopération avec la Commission et le haut représentant, devrait veiller à la cohérence et à la coordination entre les réactions à la crise de cybersécurité et les actions de réaction connexes au niveau de l'Union;

vi. lorsque des mécanismes pertinents, en particulier les services de la réserve de cybersécurité, sont sollicités, les services de la Commission et, le cas échéant, le SEAE, ainsi que les instances compétentes du Conseil, notamment le GHQC et le groupe horizontal "Renforcement de la résilience et lutte contre les menaces hybrides", selon qu'il convient, devraient se coordonner en ce qui concerne l'élaboration et la mise en œuvre de mesures, ainsi que le processus décisionnel approprié pour des mesures supplémentaires, conformément à la boîte à outils hybride[14] en cas d'actes de cybermalveillance s'inscrivant dans le cadre d'une campagne hybride plus large.

Réaction à un incident de cybersécurité majeur ou à une crise de cybersécurité pour lesquels l'IPCR est en mode "activation totale"

56) Il convient de mettre en œuvre les mesures énoncées dans la section ci-dessus intitulée "*Réaction à un incident de cybersécurité majeur ou à une crise de cybersécurité pour lesquels l'IPCR n'est pas en mode "activation totale*"".

57) Lorsque l'IPCR est activé en mode "activation totale", les rapports ISAA servent à veiller à une appréciation commune de la situation au niveau politique. Les rapports de situation d'EU-CyCLONe et du réseau des CSIRT devraient rester les principaux instruments présentant l'appréciation commune de la situation aux niveaux opérationnel et technique, respectivement. Ces rapports peuvent servir de base aux rapports ISAA.

58) En cas d'incident de cybersécurité majeur ou de crise de cybersécurité entraînant l'activation de l'IPCR en mode "activation totale", tous les acteurs devraient réagir en étroite coordination dans le cadre d'une approche pangouvernementale, comme suit:

a) la coordination de la réponse au niveau politique de l'Union est assurée par le Conseil, au moyen du dispositif IPCR;

[14] La boîte à outils hybride constitue un cadre pour apporter une réponse coordonnée aux campagnes hybrides touchant l'UE et ses États membres, comprenant, par exemple, des mesures préventives, coopératives, de stabilité, restrictives et de rétablissement et soutenant la solidarité et l'assistance mutuelle.

b) EU-CyCLONe, en coopération avec le réseau des CSIRT, devrait fournir au niveau politique des informations claires sur l'impact, les conséquences possibles et les mesures de réaction à l'incident et de retour à la normale, y compris en contribuant aux rapports ISAA;

c) outre la capacité d'ISAA, la présidence du Conseil de l'Union européenne convoquerait des tables rondes de l'IPCR pour permettre la coordination politique et stratégique de la réaction de l'UE avec les actions relevant du schéma directeur en matière de cybersécurité et les travaux des mécanismes sectoriels pertinents contribuant aux travaux de l'IPCR. Les tables rondes peuvent en outre mettre en évidence des lacunes spécifiques dans la réaction et inviter certains acteurs de l'UE à y remédier et à en rendre compte lors de futures tables rondes, afin de soutenir la coordination politique et stratégique dans le cadre de l'IPCR;

d) la présidence du Conseil de l'Union européenne devrait envisager d'inviter EU-CyCLONe aux réunions pertinentes, y compris aux tables rondes relevant du dispositif IPCR et à d'autres réunions pertinentes du Conseil;

e) les autorités de gestion des crises des États membres devraient veiller à la cohérence et à la coordination entre les réactions sectorielles à la crise de cybersécurité soutenues par les autorités de gestion des crises de cybersécurité;

f) les éventuelles réponses diplomatiques devraient être examinées et menées conformément au chapitre IX.

VIII: Efforts de communication publique

59) Lors de la communication d'informations à la population d'un État membre donné sur un incident de cybersécurité majeur ou une crise de cybersécurité en cours, y compris dans le cadre de la sensibilisation, qui est une compétence nationale, les États membres, la Commission et le haut représentant devraient viser à coordonner, dans la mesure du possible, leur communication publique. Le réseau informel des responsables de la communication de crise de l'IPCR peut être associé, le cas échéant.

60) Aux fins de la préparation à des incidents de cybersécurité majeurs ou à des crises de cybersécurité, les États membres et, le cas échéant, la Commission et le CERT-UE sont invités à échanger sur leurs efforts de communication dans le cadre d'EU- CyCLONe et du réseau des CSIRT, y compris sur les bonnes pratiques, en ce qui concerne par exemple les avertissements et les campagnes de sensibilisation. L'ENISA devrait fournir des outils à l'appui d'un tel échange et permettant un accès facile.

61) En cas d'incident de cybersécurité majeur ou de crise de cybersécurité, les États membres sont invités à partager, dans le cadre d'EU-CyCLONe, des informations sur leurs efforts de communication publique afin de favoriser une prise de conscience commune et de coordonner les actions. EU-CyCLONe, de sa propre initiative ou à la demande du Conseil, peut communiquer à ce dernier une vue d'ensemble de ces approches.

IX: Réponse diplomatique et coopération avec les partenaires stratégiques

62) Le haut représentant, en étroite coopération avec la Commission et les autres entités concernées de l'Union, devrait:

a) soutenir la prise de décision au sein du Conseil, y compris au moyen d'analyses, de rapports et de propositions, sur le recours à d'éventuelles mesures dans le cadre de la boîte à outils cyberdiplomatique de l'UE. Cela permettra d'utiliser toute la panoplie d'instruments dont l'Union dispose pour prévenir et décourager les actes de cybermalveillance et y réagir, en renforçant sa posture cyber et en promouvant la paix, la sécurité et la stabilité internationales dans le cyberespace;

b) lorsqu'un incident pertinent est détecté, faciliter le flux d'informations nécessaires avec les partenaires stratégiques, y compris avec l'OTAN, le cas échéant;

c) renforcer la coordination avec les partenaires stratégiques, y compris avec l'OTAN, le cas échéant, en ce qui concerne la réaction aux activités de cybermalveillance menées par des acteurs de menaces persistantes, notamment lors de l'utilisation de la boîte à outils cyberdiplomatique de l'UE, conformément aux orientations d'application.

63) Les États membres, le haut représentant, la Commission et les autres entités concernées de l'Union devraient coopérer avec les partenaires stratégiques et les organisations internationales afin de promouvoir les bonnes pratiques et les comportements responsables des États dans le cyberespace et d'assurer une réaction rapide et coordonnée en cas d'incidents de cybersécurité potentiels ou majeurs.

64) La coopération entre l'Union européenne et l'OTAN devrait se faire conformément aux principes directeurs convenus que sont l'inclusivité, la réciprocité et la transparence et dans le plein respect de la prise de décision autonome de l'Union.

65) La Commission et le haut représentant, compte tenu des accords existants tels que l'accord technique CERT-UE/OTAN de 2016, devraient établir des points de contact pour la coordination avec l'OTAN en cas de crise de cybersécurité afin d'échanger les informations nécessaires sur la situation et l'utilisation des mécanismes de réaction aux crises en vue d'accroître la coopération et l'efficacité en matière de réaction. À cette fin, l'Union devrait étudier les moyens d'améliorer le partage d'informations avec l'OTAN, de manière inclusive, réciproque et non discriminatoire, en particulier en veillant à l'existence d'outils de communication sécurisée tout en tenant compte des normes de partage d'informations des différents États membres.

66) Dans le cadre du programme continu d'exercices de cybersécurité de l'Union visé au chapitre V ci-dessus, les services de la Commission et le SEAE devraient envisager d'organiser avec l'OTAN un exercice au niveau du personnel, afin de tester la coopération entre les entités civiles et militaires en cas d'incident de cybersécurité majeur ou de crise de cybersécurité dans le cadre desquels les États membres de l'Union ou les pays membres de l'OTAN cherchent à réagir face à une cyberattaque portant atteinte à leur sécurité. L'exercice devrait être mené de manière inclusive et non discriminatoire, dans le plein respect des principes convenus en ce qui concerne les paramètres de la coopération entre l'UE et l'OTAN. L'exercice devrait être mené dans le cadre de l'exercice EU Integrated Resolve (exercice parallèle et coordonné ou "PACE"). Toutes les mesures nécessaires devraient être prises pour assurer la participation de tous les acteurs visés dans le schéma directeur en matière de cybersécurité.

67) Il convient également d'envisager des exercices de cybersécurité conjoints au niveau de l'Union avec les pays des Balkans occidentaux, la République de Moldavie, l'Ukraine, ainsi que d'autres partenaires stratégiques et pays tiers partageant les mêmes valeurs, en concertation avec le Conseil, la Commission et le haut représentant.

X. Coordination de la gestion des crises de cybersécurité avec des acteurs militaires au niveau de l'UE

68) Les États membres devraient continuer à renforcer la coopération entre les cyberacteurs civils et militaires au niveau national.

69) EU-CyCLONe et le réseau des CSIRT devraient recenser les pistes et les procédures envisageables pour coopérer avec les acteurs militaires concernés de l'UE, tels que la conférence des cybercommandants de l'UE et le réseau opérationnel d'équipes militaires d'intervention en cas d'urgence informatique (MICNET) afin de bénéficier d'une démarche conjointe militaire et civile, en particulier dans le cadre de réunions conjointes. EU-CyCLONe et le réseau des CSIRT devraient informer le Conseil des progrès réalisés dans le cadre de cette coopération.

70) L'État membre touché est invité à indiquer à EU-CyCLONe, ainsi qu'au SEAE, si des capacités de réaction militaires nationales ou multinationales pertinentes sont utilisées dans le contexte d'un incident de cybersécurité majeur ou d'une crise de cybersécurité, la fourniture de cette information faisant l'objet d'un accord mutuel entre l'utilisateur et le fournisseur de cette capacité de réaction.

71) Dans le cadre du programme continu d'exercices de cybersécurité de l'Union visé au chapitre V ci-dessus, la Commission et le haut représentant devraient envisager d'organiser un exercice conjoint afin de tester la coopération entre les cyberacteurs civils et militaires en cas d'incident de cybersécurité majeur touchant les États membres.

XI: Rétablissement et enseignements tirés après une crise de cybersécurité

72) Les États membres, les entités concernées de l'Union et les réseaux devraient coopérer au cours de la phase de rétablissement après une crise de cybersécurité afin de veiller à la restauration rapide des fonctionnalités essentielles. Les services répressifs devraient également, le cas échéant, être associés à cette coopération. Au cours de cette phase, la coopération avec le secteur privé est essentielle, en particulier pour ce qui est de faciliter la récupération des données et le rétablissement des systèmes. Une coordination efficace entre les parties prenantes devrait viser en priorité à réduire au minimum les perturbations et à assurer la continuité des opérations.

73) Les États membres, les entités concernées de l'Union et les réseaux devraient coopérer au cours de la phase de rétablissement en s'appuyant sur les enseignements tirés des crises de cybersécurité ou des incidents de cybersécurité gérés dans le passé, ainsi que sur les rapports d'incidents, en particulier dans le cadre du mécanisme européen d'examen des incidents de cybersécurité établi par le règlement (UE) 2025/38.

74) EU-CyCLONe devrait fournir au réseau des CSIRT, au groupe de coopération SRI et au Conseil une liste complète des enseignements tirés des crises de cybersécurité ou des incidents de cybersécurité gérés dans le passé ainsi que des bonnes pratiques. L'ENISA devrait veiller à ce que ces enseignements tirés soient dûment pris en considération lors des futures activités de préparation et de la planification des futurs exercices.

XII: Communications sécurisées

75) Sur la base de la cartographie des outils de communication sécurisés existants[15], la Commission devrait proposer, d'ici fin 2026, un ensemble interopérable de solutions de communication sécurisées. Le Conseil, la Commission, le haut représentant, EU-CyCLONe et le réseau des CSIRT devraient convenir de cet ensemble d'ici fin 2027. Ces solutions devraient tirer parti des actions que les institutions de l'UE pourraient entreprendre dans le domaine des communications sécurisées dans le cadre de la stratégie de l'UE pour une union de la préparation et couvrir l'ensemble des modes de communication requis (voix, données, vidéoconférence, messagerie, collaboration, partage et consultation de documents). Les solutions devraient répondre à des exigences communément définies en matière de protection des informations sensibles non classifiées. Il convient d'utiliser des solutions fondées sur un protocole ouvert avec des applications en source ouverte adaptées à la communication en temps réel, gérées par une entité résidente de l'UE.

76) Aux fins de l'échange d'informations classifiées RESTREINT UE/EU RESTRICTED, EU-CyCLONe et le réseau des CSIRT devraient, si nécessaire, pouvoir utiliser des canaux de communication sécurisés permettant aux institutions, organes et organismes de l'Union d'échanger, entre eux et avec les États membres, des informations classifiées.

---

15 WK 862/2023.

77) Le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité institué en vertu du règlement (UE) 2021/887[16], sans préjudice du futur cadre financier pluriannuel, devrait envisager un financement par l'intermédiaire du programme pour une Europe numérique afin d'aider les États membres à déployer des outils de communication sécurisés. Il convient d'éviter toute duplication des investissements dans des systèmes sécurisés interopérables.

78) En particulier, les entités de l'UE et les États membres devraient pouvoir parer à l'éventualité d'une crise grave, lorsque les canaux de communication normaux s'appuyant sur l'internet ou les réseaux de télécommunications sont perturbés ou indisponibles.

79) Des mécanismes de communication et de partage d'informations entre les services répressifs et les réseaux de cybersécurité, en particulier au niveau technique, devraient être mis en place en vue d'une réaction efficace aux crises de cybersécurité. Ces mécanismes devraient respecter le rôle de chaque partie, éviter toute ingérence dans les opérations en cours et assurer la redondance des communications. Le système de communication critique de l'UE en cours d'élaboration peut être utile à la réponse conjointe avec les cybercommunautés concernées.

XIII: Dispositions finales

80) EU-CyCLONe devrait, en coopération avec le réseau des CSIRT et d'autres acteurs majeurs de l'écosystème de gestion des crises de cybersécurité de l'UE et avec l'appui de l'ENISA, mettre au point, dans un délai d'un an à compter de la publication de la recommandation, des ordinogrammes détaillés des processus présentant les flux d'information entre les acteurs concernés, les processus décisionnels et les rapports élaborés au cours de la gestion des incidents de cybersécurité majeurs ou des crises de cybersécurité décrits dans la présente recommandation. Les ordinogrammes devraient couvrir différents modes et niveaux de coopération. Ils devraient être mis à jour lorsque cela est nécessaire.

---

[16] Règlement (UE) 2021/887 du Parlement européen et du Conseil du 20 mai 2021 établissant le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination (JO L 202 du 8.6.2021, p. 1).

81) Afin de soutenir l'application effective du schéma directeur révisé en matière de cybersécurité, et sur la base de l'expérience acquise lors des exercices conjoints de cybersécurité menés dans ce cadre, le Conseil peut élaborer, si nécessaire, un ensemble d'orientations d'application. Ces orientations pourraient répondre aux défis pratiques recensés au cours des exercices et remédier aux points faibles et aux chaînons manquants en ce qui concerne la coordination, la communication et l'interaction opérationnelle.

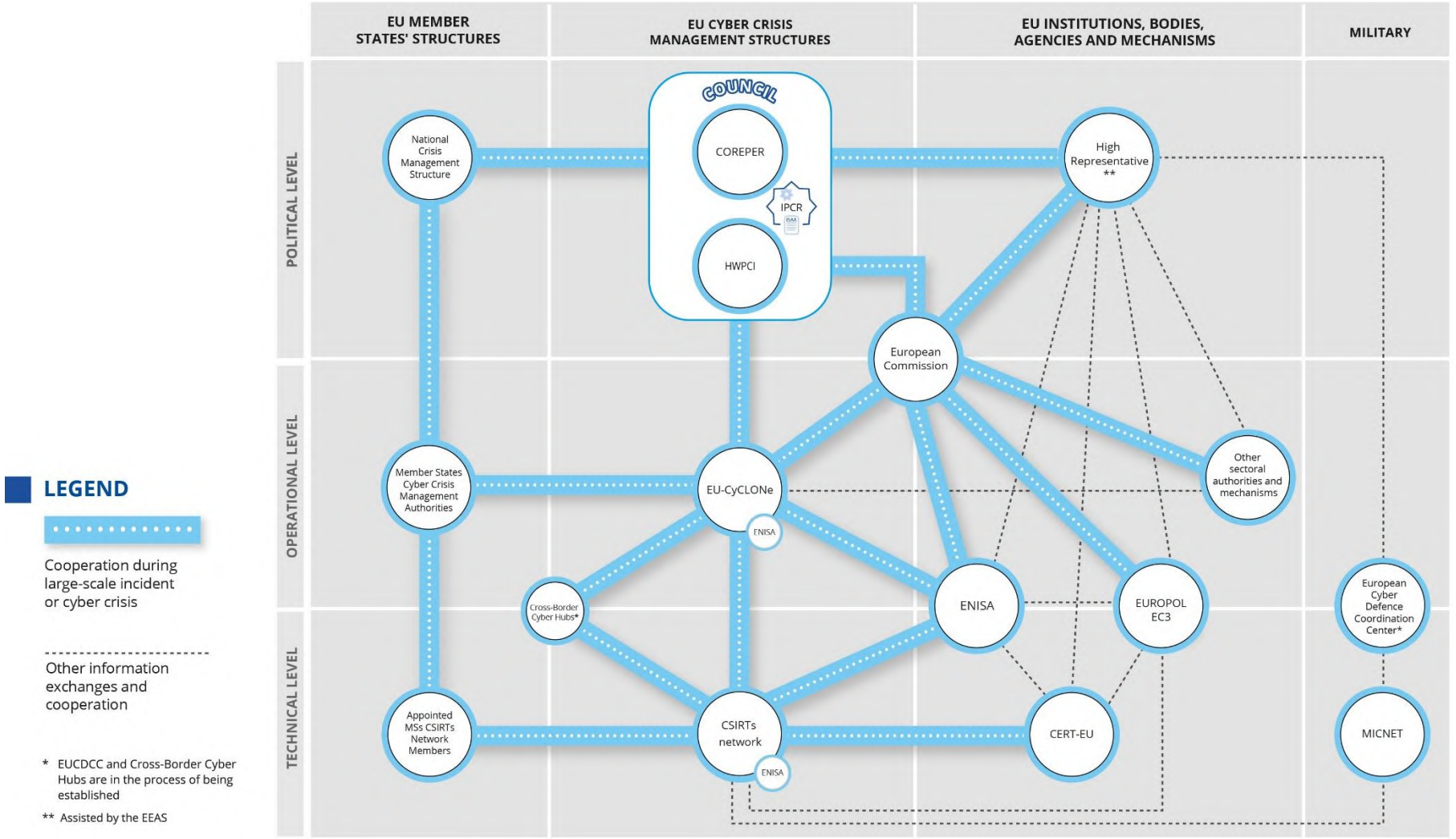
82) La présente recommandation devrait faire l'objet d'un réexamen par la Commission, en coopération avec les États membres, au moins tous les quatre ans après sa publication. Après chaque réexamen, la Commission devrait publier un rapport et le présenter au Conseil. La Commission et les États membres devraient tenir compte, en particulier, de l'incidence de l'évolution du panorama des menaces, des résultats des exercices conjoints ainsi que des changements législatifs, notamment toute modification éventuelle découlant de la révision du règlement (UE) 2019/881.

Fait à Bruxelles, le

Par le Conseil

Le président/La présidente

ANNEXE I – Le schéma directeur de l'Union pour réagir à une crise de cybersécurité



ANNEXE II – ACTEURS CONCERNÉS AU NIVEAU DE L'UNION (ENTITÉS ET RÉSEAUX) ET MÉCANISMES DE GESTION DES CRISES

(1) Participation des principaux acteurs tout au long du cycle de vie de la gestion des crises de cybersécurité (incidents de cybersécurité majeurs et crises de cybersécurité)

	Préparation	Détection	Réaction à un incident de cybersécurité majeur ou à une crise de cybersécurité			Communication publique	Rétablissement et enseignements tirés
			au niveau technique	au niveau opérationnel	au niveau politique		
États membres	X	X	X	X	X	X	X
Commission	X			X	X	X	
Haut représentant, assisté par le SEAE	X			X	X	X	
Conseil	X				X	X	X
ENISA	X		X	X			
CERT-UE	X	X	X	X		X	X
Réseau des CSIRT	X	X	X				X
EU-CyCLONe	X			X	X		X

(2) Rôles et compétences des acteurs et mécanismes concernés au niveau de l'Union (par ordre alphabétique en anglais) en ce qui concerne la gestion des crises de cybersécurité

Acteur	Niveau	Rôle et compétence	Référence
CERT-UE	Technique/opérationnel	Coordonne la réaction aux crises au niveau technique et la gestion des incidents majeurs affectant les entités de l'Union. Tient à jour un inventaire de l'expertise technique disponible qui serait nécessaire pour réagir aux incidents en cas d'incidents majeurs et assiste l'IICB dans la coordination des plans de gestion des crises de cybersécurité des entités de l'Union en cas d'incidents majeurs. Appartient au réseau des CSIRT. Soutient la Commission au sein du réseau EU-CyCLONe pour ce qui est de la gestion coordonnée des crises et incidents de cybersécurité majeurs. Fait office de pôle d'échange d'informations sur la cybersécurité et de coordination des réponses aux incidents, en facilitant l'échange d'informations en ce qui concerne les incidents, les cybermenaces, les vulnérabilités et les incidents	Règlement (UE/Euratom) 2023/2841 Règlement (UE) 2025/38

Acteur	Niveau	Rôle et compétence	Référence
		évités entre les entités de l'Union et les homologues. Demande le déploiement de la réserve de cybersécurité de l'Union au nom d'entités de l'Union. Coopère avec le Centre de cybersécurité de l'OTAN sur la base de leur accord technique.	
Conseil de l'Union européenne	Politique	Fonctions de définition des politiques et de coordination. Est chargé de l'IPCR, qui concerne la coordination et la réaction au niveau politique de l'Union.	Article 16 du traité sur l'Union européenne
Présidence du Conseil de l'Union européenne	Politique	Décide (sauf lorsque la clause de solidarité est invoquée en vertu de l'article 222 du TFUE) s'il y a lieu d'activer l'IPCR, en concertation avec les États membres concernés, le cas échéant, ainsi que la Commission et le haut représentant.	Article 16 du traité sur l'Union européenne Décision d'exécution (UE) 2018/1993 du Conseil
Cyberpôles transfrontières	Technique	Un cyberpôle transfrontière est une plateforme multinationale, établie par un accord de consortium écrit, qui rassemble, au sein d'une structure de réseau coordonnée, les cyberpôles nationaux d'au moins trois États membres, et qui est	Règlement (UE) 2025/38

Acteur	Niveau	Rôle et compétence	Référence
		conçue pour améliorer le suivi, la détection et l'analyse des cybermenaces pour prévenir les incidents et pour soutenir la production de renseignements sur les cybermenaces, notamment par l'échange de données et d'informations pertinentes, le cas échéant anonymisées, ainsi que par le partage d'outils de pointe et le développement conjoint de capacités de détection, d'analyse, de prévention et de protection en matière de cybersécurité dans un environnement de confiance. Coopèrent étroitement avec le réseau des CSIRT pour le partage des informations. Fournissent des informations relatives à un incident de cybersécurité majeur potentiel ou en cours aux autorités des États membres et à la Commission par l'intermédiaire du réseau EU-CyCLONe et du réseau des CSIRT.	
Réseau des CSIRT	Technique	Contribue au renforcement de la confiance et promeut une coopération opérationnelle rapide entre les États membres. Est le réseau principal pour l'échange d'informations	Directive (UE) 2022/2555 Règlement (UE) 2025/38

Acteur	Niveau	Rôle et compétence	Référence
		pertinentes sur les incidents, les incidents évités, les cybermenaces, les risques et les vulnérabilités. À la demande d'un membre du réseau des CSIRT potentiellement affecté par un incident, le réseau échange sur les informations en rapport avec cet incident et les cybermenaces connexes. Le réseau peut également faciliter une réponse coordonnée à un incident déterminé qui relève de la compétence de l'État membre demandeur. Fournit une assistance aux États membres dans la gestion des incidents transfrontières et étudie d'autres formes de coopération, y compris l'assistance mutuelle. Reçoit des informations des États membres concernant les demandes qu'ils ont adressées à la réserve de cybersécurité de l'Union.	
Conférence des cybercommandants		Un forum permettant aux cybercommandants au niveau national au sein des États membres de coopérer et d'échanger des informations essentielles	Communication conjointe sur la politique de

Acteur	Niveau	Rôle et compétence	Référence
		concernant les opérations et les stratégies en cours dans le cyberespace pour atténuer les incidents de cybersécurité majeurs. Ce forum est organisé par la présidence tournante du Conseil de l'Union européenne avec le soutien de l'Agence européenne de défense (AED) et du Service européen pour l'action extérieure (SEAE), y compris l'État-major de l'UE (EMUE).	cyberdéfense de l'UE (2022)
Commission	Opérationnel/politique	Organe exécutif de l'Union européenne. Assure le bon fonctionnement du marché intérieur. Facilite la cohérence et la coordination entre les actions connexes de réaction aux crises menées au niveau de l'Union. Assume la réalisation de certaines actions générales en matière de préparation au niveau de l'Union au titre de la décision relative au mécanisme de protection civile de l'Union, y compris la gestion du centre de coordination de la réaction d'urgence et du système commun de communication et d'information d'urgence.	Article 17 du traité sur l'Union européenne Décision d'exécution (UE) 2018/1993 Décision n° 1313/2013/UE Directive (UE) 2022/2555 Règlement (UE) 2025/38 Règlement (UE/Euratom) 2023/2841

Acteur	Niveau	Rôle et compétence	Référence
		Participe aux activités d'EU-CyCLONe en qualité d'observateur, et en qualité de membre en cas d'incident de cybersécurité majeur, potentiel ou en cours, qui a ou est susceptible d'avoir un impact important sur les services et les activités relevant du champ d'application de la directive (UE) 2022/2555. Participe au réseau des CSIRT en qualité d'observateur. A la responsabilité générale de la mise en œuvre de la réserve de cybersécurité de l'Union. Fait office de point de contact au sein du conseil interinstitutionnel de cybersécurité pour le partage des informations pertinentes relatives aux incidents majeurs avec EU-CyCLONe. Est consultée par la présidence du Conseil sur les décisions d'activation ou de désactivation de l'IPCR (sauf lorsque la clause de solidarité est invoquée en vertu de l'article 222 du TFUE).	

Acteur	Niveau	Rôle et compétence	Référence
		Les services de la Commission élaborent, avec le SEAE, les rapports ISAA.	
Agence de l'Union européenne pour la cybersécurité (ENISA)	Technique/opérationnel	Exécute des tâches visant à atteindre un niveau élevé de cybersécurité dans l'ensemble de l'Union, y compris en soutenant activement les États membres et les institutions de l'Union. Assure le secrétariat du réseau des CSIRT et d'EU-CyCLONe. Prépare à intervalles réguliers un rapport de situation technique en matière de cybersécurité de l'Union européenne sur les incidents et cybermenaces (avec l'EC3 et la CERT-UE et en coopération étroite avec les États membres). Contribue à l'élaboration d'une réponse commune aux incidents ou crises transfrontières majeurs, principalement: - en agrégeant et en analysant des rapports provenant de sources nationales; - en assurant la circulation de l'information entre les niveaux technique,	Directive (UE) 2022/2555 Règlement (UE) 2019/881 Règlement (UE) 2025/38 Règlement (UE) 2024/2847

Acteur	Niveau	Rôle et compétence	Référence
		opérationnel et politique; - sur demande, en facilitant la gestion des incidents; - en soutenant les entités de l'Union en ce qui concerne la communication publique; - en soutenant les États membres, à leur demande, en ce qui concerne la communication publique; - en mettant à l'épreuve les capacités de réaction aux incidents et en organisant régulièrement des exercices de cybersécurité. Agit en tant que pouvoir adjudicateur lorsque le fonctionnement et l'administration de la réserve de cybersécurité de l'Union lui ont été confiés, en tout ou en partie. Organise tous les deux ans un exercice global de cybersécurité à grande échelle au niveau de l'Union, comportant des aspects techniques, opérationnels ou stratégiques.	

Acteur	Niveau	Rôle et compétence	Référence
		Prépare un rapport d'analyse en collaboration avec l'État membre concerné et d'autres parties prenantes concernées, afin d'évaluer les causes et les effets d'un incident ainsi que les mesures d'atténuation connexes (à la demande de la Commission ou d'EU-CyCLONe et avec l'approbation de l'État membre concerné). Informe EU-CyCLONe si les informations fournies au titre des obligations de déclaration prévues par le règlement sur la cyberrésilience sont pertinentes pour la gestion coordonnée au niveau opérationnel des crises et incidents de cybersécurité majeurs.	
Réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONe)	Opérationnel	Contribue à la gestion coordonnée, au niveau opérationnel, des incidents de cybersécurité majeurs et des crises. Garantit l'échange régulier d'informations pertinentes entre les États membres et les institutions, organes et organismes de l'Union. Coordonne la gestion des incidents de cybersécurité majeurs et des crises et soutient la prise de décision	Directive (UE) 2022/2555 Règlement (UE) 2025/38

Acteur	Niveau	Rôle et compétence	Référence
		au niveau politique en ce qui concerne ces incidents et ces crises. Évalue les conséquences et l'impact des incidents de cybersécurité majeurs et des crises en question et propose d'éventuelles mesures d'atténuation. Examine, à la demande de l'État membre concerné, le plan national de réaction aux crises et aux incidents de cybersécurité majeurs. Élabore, en collaboration avec l'ENISA et la Commission, un modèle pour faciliter la présentation des demandes d'aide adressées à la réserve de cybersécurité de l'Union. Reçoit des informations des États membres concernant les demandes qu'ils ont adressées à la réserve de cybersécurité de l'Union. Reçoit des informations relatives à un incident de cybersécurité majeur potentiel ou en cours de la part des cyberpôles transfrontières ou du réseau des CSIRT.	

Acteur	Niveau	Rôle et compétence	Référence
Haut représentant de l'Union pour les affaires étrangères et la politique de sécurité, avec le soutien du Service européen pour l'action extérieure	Politique	Dirige et coordonne les efforts déployés par l'Union afin de faire face aux menaces pour la sécurité d'origine extérieure dans les domaines des menaces hybrides et des cybermenaces. Responsable de la cyberdiplomatie et des instruments de cyberdéfense de l'Union visant à décourager les menaces extérieures et à y réagir, y compris en utilisant la boîte à outils hybride et la boîte à outils cyberdiplomatique de l'Union. Coopère avec des partenaires extérieurs, y compris dans le cadre de l'action menée au titre de la politique de sécurité et de défense commune (PSDC). Assure la préparation de l'Union et des États membres en matière d'appréciation de la situation et de capacité à réagir aux menaces hybrides et aux cybermenaces, par exemple au moyen d'exercices pratiques, de formations et de réseaux. Traite les implications en matière de sécurité et de défense des moyens spatiaux de l'Union, en particulier	Décision 2010/427/UE du Conseil

Acteur	Niveau	Rôle et compétence	Référence
		dans le cadre de la PSDC de l'Union. Soutient la conférence des cybercommandants de l'UE. Soutient le réseau opérationnel d'équipes militaires d'intervention en cas d'urgence informatique (MICNET), mis en place par l'UE Est consulté par la présidence du Conseil sur les décisions d'activation ou de désactivation de l'IPCR (sauf lorsque la clause de solidarité est invoquée en vertu de l'article 222 du TFUE). Le SEAE élabore, avec les services de la Commission, les rapports ISAA.	
Centre de coordination de l'UE en matière de cyberdéfense	Horizontal	Son objectif initial est principalement de renforcer l'appréciation commune de la situation de l'Union et de ses États membres en ce qui concerne les activités malveillantes dans le cyberespace, en particulier pour ce qui est des missions et opérations militaires relevant de la PSDC.	Communication conjointe sur la politique de cyberdéfense de l'UE (2022)
Europol	Opérationnel	Apporte un soutien opérationnel et technique aux autorités compétentes des États membres pour	Règlement (UE) 2016/794, y

Acteur	Niveau	Rôle et compétence	Référence
		prévenir et décourager la cybercriminalité. Aide les autorités compétentes des États membres, à leur demande, à répondre aux cyberattaques supposées être d'origine criminelle.	compris toutes les modifications
Conseil interinstitutionnel de cybersécurité		Établit un plan de gestion des crises de cybersécurité en vue de soutenir, au niveau opérationnel, la gestion coordonnée des incidents majeurs affectant les entités de l'Union et de contribuer à l'échange régulier d'informations pertinentes. Coordonne l'adoption des plans individuels de gestion des crises de cybersécurité des entités de l'Union. Adopte, sur la base d'une proposition du CERT-UE, des orientations ou des recommandations sur la coordination de la réaction aux incidents et la coopération en cas d'incident important concernant des entités de l'Union.	Règlement (UE/Euratom) 2023/2841
Réseau opérationnel d'équipes militaires d'intervention en	Technique	Favorise une réponse plus solide et plus coordonnée aux cybermenaces touchant les systèmes de défense de l'Union, y compris ceux utilisés dans le cadre des	Communication conjointe sur la cyberdéfense de 2022

Acteur	Niveau	Rôle et compétence	Référence
cas d'urgence informatique (MICNET)		missions et opérations militaires relevant de la PSDC; soutenu par l'Agence européenne de défense.	
Capacité unique d'analyse du renseignement (SIAC)		Composée 1) du Centre de situation et du renseignement de l'UE (INTCEN) et 2) de la direction du renseignement de l'État-major de l'UE (EUMS INT). Fournit des renseignements stratégiques sur la politique étrangère, le terrorisme, les cybermenaces et les menaces hybrides. Gère le renseignement militaire pour les missions PSDC et soutient les opérations de défense et de gestion de crise de l'Union. Placée sous l'autorité du haut représentant.	Article 38 et articles 42 à 46 du traité sur l'Union européenne.

(3) Mécanismes et plateformes pertinents de gestion des crises au niveau de l'Union

Mécanisme	Horizontal/sectoriel/spécifique au cyberespace	Description	Référence
ARGUS	Horizontal	Le processus de coordination et le système général d'alerte de la Commission pour une réponse cohérente en cas de crise transfrontière majeure nécessitant une action au niveau de l'UE. Réunit tous les services et cabinets concernés pour décider des mesures et les coordonner. Permet à la Commission d'échanger des informations pertinentes sur les crises multisectorielles émergentes ou les menaces prévisibles ou imminentes qui nécessitent une action au niveau de l'Union.	Communication (2005)662 de la Commission
Centre de réaction aux crises du SEAE (CRC)	Horizontal	Le point d'entrée unique au sein du SEAE pour toutes les questions liées aux crises et la capacité permanente (24 heures sur 24 et sept jours sur sept) de réaction aux crises pour les situations d'urgence menaçant la sécurité du personnel des délégations de l'UE et/ou de réaction à des crises touchant des citoyens de l'Union à l'étranger. Réunit des experts en matière de sécurité, de questions consulaires et d'appréciation de la	Une 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

Mécanisme	Horizontal/sectoriel/spécifique au cyberespace	Description	Référence
		situation, en s'appuyant sur des professionnels des délégations de l'Union engagés sur le terrain.	à la sécurité internationales (21 mars 2022)
Schéma directeur pour les infrastructures critiques	Horizontal	Coordonne au niveau de l'Union la réponse en cas de perturbations des infrastructures critiques ayant une dimension transfrontière notable.	Recommandation C/2024/4371 du Conseil
Système d'alerte en matière de cybersécurité	Spécifique au cyberespace	Garantit des capacités avancées permettant à l'Union de renforcer les capacités de détection, d'analyse et de traitement des données en rapport avec les cybermenaces et la prévention des incidents dans l'Union.	Règlement (UE) 2025/38
Boîte à outils cyberdiplomatique (cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance)	Spécifique au cyberespace	Permet une réponse diplomatique conjointe de l'Union face aux actes de cybermalveillance, qui contribue à la prévention des conflits, à l'atténuation des menaces en matière de cybersécurité et à une plus grande stabilité dans les relations internationales.	Conclusions du Conseil du 19 juin 2017 Lignes directrices révisées pour la mise en œuvre (10289/23), 8 juin 2023

Mécanisme	Horizontal/sectoriel/spécifique au cyberespace	Description	Référence
Réserve de cybersécurité de l'Union	Spécifique au cyberespace	Mobilise des experts et des ressources en matière de cybersécurité pendant les crises afin de soutenir les efforts de réaction dans les États membres, les institutions, organes ou organismes de l'Union	Règlement (UE) 2025/38
Code de réseau sur des règles sectorielles concernant les aspects liés à la cybersécurité des flux transfrontaliers d'électricité	Sectoriel	Établit un processus récurrent d'évaluation des risques de cybersécurité dans le secteur de l'électricité, aux niveaux de l'Union, des États membres, des régions et des entités. Comporte des dispositions spécifiques à la gestion des crises et à la coopération avec les CSIRT et EU-CyCLONe en cas d'incident de cybersécurité majeur ayant un impact sur d'autres secteurs dépendant de la sécurité de l'approvisionnement en électricité.	Règlement délégué (UE) 2024/1366 de la Commission
Boîte à outils hybride	Horizontal	Comprend un ensemble de dispositions visant à garantir une vue d'ensemble de ce qui est disponible au niveau de l'UE en réponse à tous les types de menaces hybrides, leur utilisation coordonnée et la cohérence des actions dans tous les domaines. La boîte à outils hybride	Conclusions du Conseil sur un cadre pour une réponse coordonnée de l'UE aux campagnes hybrides, 22 juin 2022

Mécanisme	Horizontal/sectoriel/spécifique au cyberespace	Description	Référence
		contribue à faire en sorte que la prise de décision soit fondée sur une appréciation complète de la situation et sur les enseignements tirés.	Lignes directrices de mise en œuvre du cadre pour une réponse coordonnée de l'UE aux campagnes hybrides, 14 décembre 2022
Équipes d'intervention rapide de l'UE en cas de menaces hybrides	Horizontal	Dans le cadre de la boîte à outils hybride de l'UE, les équipes d'intervention rapide de l'UE en cas de menaces hybrides s'appuient sur l'expertise civile et militaire sectorielle pertinente des États membres et de l'UE pour fournir une assistance à court terme sur mesure et ciblée aux États membres, aux missions et opérations relevant de la politique de sécurité et de défense commune et aux pays partenaires dans la lutte contre les menaces et les campagnes hybrides.	Cadre directeur pour la mise en place pratique des équipes d'intervention rapide de l'UE en cas de menaces hybrides (21 mai 2024) Orientations pratiques pour le déploiement des équipes d'intervention rapide, approuvées par le Coreper le 4 décembre 2024
IPCR	Horizontal	Soutient la prise de décision rapide et coordonnée au niveau politique de l'Union pour les crises majeures et complexes.	Décision d'exécution (UE) 2018/1993 du Conseil

Mécanisme	Horizontal/sectoriel/spécifique au cyberespace	Description	Référence
		La décision d'activer et de désactiver est prise par la présidence du Conseil, qui consulte (sauf lorsque la clause de solidarité a été invoquée) les États membres concernés, la Commission et le haut représentant. Le SGC, les services de la Commission et le SEAE peuvent également convenir, en concertation avec la présidence, d'activer l'IPCR en mode "partage de l'information". Les travaux de l'IPCR se fondent sur les rapports ISAA élaborés par les services de la Commission et le SEAE. Ces rapports sont fondés sur les informations et analyses pertinentes fournies par les États membres (par exemple, les centres de crise nationaux concernés), ainsi que par les organes et organismes de l'Union compétents.	
Protocole de réaction d'urgence des services répressifs de l'UE	Horizontal	Outil visant à aider les services répressifs de l'Union à apporter une réponse immédiate aux cyberattaques transfrontières majeures grâce à une évaluation rapide, au partage sécurisé et en temps utile d'informations critiques et à une coordination	Conclusions du Conseil du 26 juin 2018 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs de l'Union

Mécanisme	Horizontal/sectoriel/spécifique au cyberespace	Description	Référence
		efficace des aspects internationaux de leurs enquêtes.	
Équipes d'intervention rapide en cas d'incident informatique (CRRT) de la CSP	Spécifique au cyberespace	Les CRRT de la CSP sont une capacité de cyberdéfense civilo-militaire des États membres de l'UE développée conjointement dans le but de réagir rapidement aux incidents et aux crises de cybersécurité et de mener des actions préventives, telles que des évaluations de la vulnérabilité et la surveillance électorale. La mission des CRRT au titre de la CSP consiste à fournir, sur demande, un soutien cyber aux États membres de l'UE, aux institutions, organes et organismes de l'UE, aux missions et opérations militaires PSDC de l'UE, ainsi qu'aux pays partenaires.	Article 42, paragraphe 6, article 46 et protocole nº 10 du traité sur l'Union européenne.

Architecture de réaction aux menaces spatiales	Sectoriel (Menaces spatiales, y compris liées au cyberespace)	Architecture de réaction aux menaces spatiales sur les responsabilités à exercer par le Conseil et le haut représentant pour prévenir une menace découlant du déploiement, de l'exploitation ou de l'utilisation des systèmes mis en place et des services fournis dans le cadre du programme spatial de l'Union	Décision (PESC) 2021/698 du Conseil
Cadre de coordination des cyberincidents systémiques (EU-SCICF)	Sectoriel	Cadre en cours d'élaboration pour la communication et la coordination, qui traite et gère les éventuels cyberévénements systémiques dans le secteur financier. Il tirera parti de l'un des rôles envisagés pour les autorités européennes de surveillance (AES) au titre du règlement (UE) 2022/2554, à savoir favoriser la mise en place progressive d'une réponse efficace et coordonnée au niveau de l'Union en cas d'incident transfrontalier majeur lié aux technologies de l'information et de la communication (TIC) ou de menace connexe ayant une incidence systémique sur l'ensemble du secteur financier de l'Union.	Recommandation du Comité européen du risque systémique du 2 décembre 2021 sur un cadre paneuropéen de coordination des cyberincidents systémiques pour les autorités concernées (CERS/2021/17)
Mécanisme de protection civile de l'Union (MPCU)	Horizontal	Assure la coopération dans le domaine de la protection civile, en vue d'améliorer la prévention des catastrophes ainsi que la préparation et la réaction à celles-ci.	Décision nº 1313/2013/UE

CISE – environnement commun de partage de l'information	Propre au secteur maritime, couvrant sept secteurs.	Le CISE est un réseau qui relie les systèmes des autorités de l'UE/EEE chargées de la surveillance maritime. Le CISE permet l'échange d'informations pertinentes par-delà les frontières et dans différents secteurs de manière fluide et automatisée.	Une 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 (21 mars 2022)

(4) Secteurs hautement critiques et autres secteurs critiques au titre de la directive (UE) 2022/2555 et mécanismes sectoriels de gestion des crises au niveau de l'Union (le cas échéant)		
Secteurs	**Sous-secteur**	**Mécanismes sectoriels de gestion des crises applicables**
Énergie	Électricité	Groupe de coordination pour l'électricité
	Réseaux de chaleur et de froid	s.o.
	Pétrole	Groupe de coordination pour le pétrole et les produits pétroliers Groupe des autorités pour les opérations en mer de l'Union européenne (EUOAG)
	Gaz	Groupe de coordination pour le gaz
	Hydrogène	s.o.
Transports	Transports aériens	Cellule européenne de coordination de l'aviation en cas de crise (CECAC)
	Transports ferroviaires	s.o.

	Transports par eau	Agence européenne de contrôle des pêches (AECP) SafeSeaNet (SSN) Services maritimes intégrés (SMI) Centre de données d'identification et de suivi des navires à distance (LRIT) Services de soutien maritime de l'AESM
	Transports routiers	s.o.
	Horizontal	Le réseau de points de contact pour les transports, établi par le plan d'urgence pour les transports [COM(2022) 211]
Banque		EU-SCICF
Infrastructures de marchés financiers		EU-SCICF Mécanisme européen de stabilisation financière

Santé		Système d'alerte précoce et de réaction (SAPR) Système d'alerte rapide pour les tissus et les cellules ainsi que pour les composants sanguins (RATC/RAB) du Centre de gestion de crise sanitaire Cadre d'urgence de santé publique Système d'alerte rapide en cas d'incidents chimiques (RASCHEM) Portail européen de surveillance des maladies infectieuses Autorité de préparation et de réaction en cas d'urgence sanitaire (HERA) Système d'information médicale (MedISys) Groupe de pilotage exécutif sur les pénuries de dispositifs médicaux Alerte rapide en matière de pharmacovigilance Task-force de l'UE dans le domaine de la santé Comité de sécurité sanitaire

Eau potable		s.o.
Eaux résiduaires		s.o.
Infrastructure numérique		s.o.
Gestion des services TIC		s.o.
Administration publique		s.o.
Espace		Architecture de réaction aux menaces spatiales
Services postaux et d'expédition		s.o.
Gestion des déchets		s.o.
Fabrication, production et distribution de produits chimiques		Système d'alerte rapide en cas d'incidents chimiques (RASCHEM)

Production, transformation et distribution des denrées alimentaires		Système européen de surveillance de la production agricole Détection de foyers d'anomalies dans la production agricole mondiale (ASAP) Réseau européen de systèmes d'information sur la santé des végétaux (EUROPHYT) Équipe vétérinaire d'urgence de l'UE (EUVET) Système d'alerte rapide pour les denrées alimentaires et les aliments pour animaux (RASFF) Mécanisme européen de préparation et de réaction aux crises de sécurité alimentaire Règlement sur les situations d'urgence et la résilience du marché intérieur
Industrie manufacturière	Dispositifs médicaux	s.o.
	Produits informatiques, électroniques et optiques	s.o.
	Matériel	s.o.

	Construction de véhicules automobiles, remorques et semi-remorques	s.o.
	Fabrication d'autres matériels de transport	s.o.
Fournisseurs numériques		s.o.
Recherche		s.o.

ANNEXE III – Cadre de l'UE relatif à la gestion des crises de cybersécurité et instruments connexes

Depuis 2017, l'Union a élaboré son cadre en matière de cybersécurité au moyen de plusieurs instruments qui contiennent des dispositions pertinentes pour la gestion des crises de cybersécurité:

- règlement (UE) 2019/881 du Parlement européen et du Conseil[1],
- directive (UE) 2022/2555 du Parlement européen et du Conseil[2],
- règlement d'exécution (UE) 2024/2690 de la Commission[3], règlement (UE/Euratom) 2023/2841 du Parlement européen et du Conseil[4],
- règlement (UE) 2021/887 du Parlement européen et du Conseil[5],
- règlement (UE) 2024/2847 du Parlement européen et du Conseil[6], et
- règlement (UE) 2025/38 du Parlement européen et du Conseil ("règlement sur la cybersolidarité") [7].

Les mesures sectorielles spécifiques en cas de crise de cybersécurité comprennent le règlement délégué (UE) 2024/1366 de la Commission[8] et le futur cadre de coordination des cyberincidents systémiques (EU-SCICF) dans le contexte du règlement (UE) 2022/2554 du Parlement européen et du Conseil[9].

La directive 2013/40/UE[10] fournit la référence pour la définition des activités criminelles liées aux cyberattaques, et les règles de l'Union relatives à l'accès transfrontière à des preuves électroniques, en particulier le règlement (UE) 2023/1543 du Parlement européen et du Conseil[11], une fois mises en œuvre, faciliteront considérablement l'action répressive dans ce domaine.

La politique de cyberdéfense de l'UE[12] définit les rôles d'un réseau opérationnel de l'UE d'équipes militaires d'intervention en cas d'urgence informatique (MICNET) et de la conférence des cybercommandants de l'UE et envisage la création d'un Centre de coordination de l'UE en matière de cyberdéfense (EUCDCC).

D'autres mécanismes d'appréciation de la situation et de réaction aux crises, non liés au cyberespace, existent dans certains des secteurs critiques énumérés aux annexes I et II de la directive (UE) 2022/2555.

La "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"[13] prévoit une coopération entre les acteurs concernés lorsqu'un incident affecte à la fois les aspects physiques et la cybersécurité des infrastructures critiques.

[1] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

[2] 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 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

[3] Règlement d'exécution (UE) 2024/2690 de la Commission du 17 octobre 2024 établissant des règles relatives à l'application de la directive (UE) 2022/2555 pour ce qui est des exigences techniques et méthodologiques liées aux mesures de gestion des risques en matière de cybersécurité et précisant plus en détail les cas dans lesquels un incident est considéré comme important, en ce qui concerne les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux, et les prestataires de services de confiance (JO L, 2024/2690, 18.10.2024). ELI: https://data.europa.eu/eli/reg/2024/2690/oj).

[4] Règlement (UE, Euratom) 2023/2841 du Parlement européen et du Conseil du 13 décembre 2023 établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union (JO L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

[5] Règlement (UE) 2021/887 du Parlement européen et du Conseil du 20 mai 2021 établissant le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination (JO L 202 du 8.6.2021, p. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

[6] Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) nº 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience) (JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

[7] Règlement (UE) 2025/38 du Parlement européen et du Conseil du 19 décembre 2024 établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les cybermenaces et incidents,

de s'y préparer et d'y réagir et modifiant le règlement (UE) 2021/694 (règlement sur la cybersolidarité) (JO L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

[8] Règlement délégué (UE) 2024/1366 de la Commission du 11 mars 2024 complétant le règlement (UE) 2019/943 du Parlement européen et du Conseil en établissant un code de réseau sur des règles sectorielles concernant les aspects liés à la cybersécurité des flux transfrontaliers d'électricité (JO L, 2024/1366, 24.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/2024-05-24).

[9] Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011 (JO L 333 du 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/2022-12-27).

[10] Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil (JO L 218 du 14.8.2013, p. 8, ELI: http://data.europa.eu/eli/dir/2013/40/oj).

[11] Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue de procédures pénales; et directive (UE) 2023/1544 du Parlement européen et du Conseil du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de la collecte de preuves électroniques en matière pénale (JO L 191 du 28.7.2023, p. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

[12] JOIN(2022) 49 final. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022JC0049

[13] *JO C, C/2024/4371 du 5.7.2024.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202404371