COMMISSION
EUROPÉENNE

Bruxelles, le 24.2.2025
COM(2025) 66 final

2025/0036 (NLE)

Proposition de

RECOMMANDATION DU CONSEIL

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

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Justification et objectifs de la proposition

Le Conseil, dans ses conclusions du 22 mai 2024 sur l'avenir de la cybersécurité,

> «*[a appelé] la Commission à évaluer rapidement l'actuel schéma directeur en matière de cybersécurité et, sur cette base, à proposer un schéma directeur révisé sous la forme d'une recommandation du Conseil qui portera sur les défis actuels et le panorama complexe des cybermenaces, renforcera les réseaux existants, accroîtra la coopération et brisera les cloisonnements entre les organisations, en recourant en premier lieu aux structures existantes. En outre, le schéma directeur révisé devrait s'appuyer sur des principes de coopération qui ont fait leurs preuves (proportionnalité, subsidiarité, complémentarité et confidentialité des informations), les étendre à l'ensemble du cycle de vie de la gestion des crises et contribuer à aligner ainsi qu'à renforcer la sécurité de la communication dans le domaine de la cybersécurité. Il conviendrait d'assurer la compatibilité du schéma directeur révisé avec les cadres existants, tels que l'IPCR, la boîte à outils cyberdiplomatique de l'UE, la boîte à outils hybride de l'UE et le protocole de réaction d'urgence des services répressifs de l'UE pour les cyberattaques transfrontières majeures, ainsi que les cadres en devenir, tels que le schéma directeur pour les infrastructures critiques, les procédures sectorielles et les structures globales de gestion des crises au sein des entités de l'Union, en associant en outre le haut représentant et Europol. Dans ce schéma directeur révisé, le rôle de la Commission, du haut représentant et de l'ENISA, selon leurs compétences, devrait surtout consister à soutenir la coordination horizontale.*»

L'objectif du présent projet de recommandation du Conseil concernant le schéma directeur de l'Union pour la gestion des crises de cybersécurité (ci-après le «schéma directeur en matière de cybersécurité») est de présenter, de manière claire, simple et accessible, le cadre de l'Union européenne (UE) pour la gestion des crises de cybersécurité. Celui-ci devrait permettre aux acteurs concernés de l'Union (c'est-à-dire les entités individuelles et les réseaux d'entités au niveau de l'Union) de comprendre comment interagir et utiliser au mieux les mécanismes disponibles tout au long du cycle de vie de la gestion des crises. Il vise à expliquer ce qu'est une crise de cybersécurité et ce qui déclenche un mécanisme de crise de cybersécurité au niveau de l'Union. Il explique l'utilisation des mécanismes disponibles tels que le mécanisme d'urgence dans le domaine de la cybersécurité, y compris la réserve de cybersécurité de l'Union, pour préparer la manière de gérer une crise résultant d'un incident de cybersécurité majeur, d'y réagir et de revenir à la normale. Il vise en outre à favoriser une coopération plus structurée entre les acteurs civils et militaires, y compris la coopération avec l'Organisation du traité de l'Atlantique Nord (OTAN), étant donné qu'un cyberincident de grande ampleur affectant des infrastructures civiles de l'Union sur lesquelles l'armée s'appuie peut également activer les mécanismes de réaction de l'OTAN.

Le schéma directeur en matière de cybersécurité est un instrument non contraignant qui définit des actions spécifiques pour les acteurs concernés dans une crise de cybersécurité et qui peut améliorer l'efficacité globale du cadre de gestion des crises de cybersécurité. Il met à jour le schéma directeur présenté dans la recommandation (UE) 2017/1584 de la Commission sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs et s'appuie sur les résultats et les enseignements tirés des exercices au niveau de l'Union depuis l'adoption de cette recommandation. Il s'inscrit dans le cadre plus large des priorités politiques dans les domaines de la préparation et de la sécurité.

Conformément à la directive (UE) 2022/2555 (directive SRI 2), un «incident de cybersécurité majeur» est 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. En fonction de sa cause et de son impact, un tel incident peut dégénérer et se transformer en une crise à part entière, perturbant 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.

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

La proposition est cohérente avec les instruments pertinents de l'Union dans le domaine de la cybersécurité, notamment la directive SRI 2 et le règlement (UE/Euratom) 2023/2841 établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union. Elle est également conforme au cadre du mécanisme de protection civile de l'Union (MPCU), institué par la décision nº 1313/2013/UE du Parlement européen et du Conseil, à la décision d'exécution (UE) 2018/1993 du Conseil concernant le dispositif intégré de l'Union européenne pour une réaction au niveau politique dans les situations de crise (IPCR), et aux instruments sectoriels pour l'appréciation de la situation et la gestion des crises, y compris dans le secteur de l'électricité.

- **Cohérence avec les autres politiques de l'Union**

Le schéma directeur en matière de cybersécurité complète et s'inscrit dans le droit fil de la recommandation du Conseil, récemment adoptée, 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, étant donné que cette dernière couvre les perturbations liées à la résilience physique, autre que cyber. Elle interagit étroitement avec les mécanismes et outils de gestion des crises de la politique étrangère et de sécurité commune (PESC) et de la politique de sécurité et de défense commune (PSDC), comme le prévoit la boussole stratégique en matière de sécurité et de défense du Conseil. En outre, les initiatives de l'Union visant à lutter contre la cybercriminalité peuvent soutenir les objectifs poursuivis par la présente recommandation.

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

- **Base juridique**

La proposition est fondée sur l'article 292 du traité sur le fonctionnement de l'Union européenne (TFUE), qui établit les règles pertinentes concernant l'adoption de recommandations.

La proposition compléterait l'ensemble du cadre législatif en matière de cybersécurité établi au niveau de l'Union. La proposition ne traite pas de la gestion des incidents majeurs affectant les entités de l'Union au sens du règlement (UE/Euratom) 2023/2841, adopté sur la base de l'article 298 du TFUE. Elle traite toutefois de l'échange d'informations entre les entités de l'Union et les États membres, y compris les dispositions du règlement (UE/Euratom) 2023/2841 selon lesquelles le représentant de la Commission au conseil institutionnel de cybersécurité (IICB) devrait faire office de point de contact pour faciliter le partage des informations pertinentes relatives aux incidents majeurs avec le réseau européen d'organisations de liaison en cas de crises de cybersécurité (EU-CyCLONe), afin de contribuer à l'appréciation commune de la situation.

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

Alors que la réponse aux perturbations des infrastructures critiques ou des services fournis par des entités essentielles et importantes relève avant tout de la responsabilité des États membres, certains actes de cybermalveillance de nature transfrontière peuvent perturber et endommager des infrastructures d'information critiques dont dépend le bon fonctionnement du marché intérieur. Par conséquent, l'Union joue un rôle important en cas d'incident ou de crise notable. Une telle perturbation peut avoir des effets dommageables sur plusieurs pans de l'activité économique au sein du marché unique, voire sur l'ensemble de celles-ci, et pourrait avoir une incidence sur la sécurité et les relations internationales de l'Union. Dans le but de garantir le fonctionnement du marché intérieur, une coordination au niveau de l'Union en cas de perturbations des infrastructures critiques ayant des effets transfrontières importants est non seulement appropriée, mais également nécessaire. Des réponses coordonnées au niveau de l'Union aideront les États membres à réagir à la perturbation grâce à une appréciation commune de la situation, à une communication publique coordonnée et à l'atténuation des conséquences de la perturbation sur le marché intérieur.

- **Proportionnalité**

La présente proposition est conforme au principe de proportionnalité prévu à l'article 5, paragraphe 4, du traité sur l'Union européenne (TUE). Ni le contenu ni la forme de cette recommandation du Conseil telle qu'elle est proposée n'excèdent ce qui est nécessaire pour atteindre ses objectifs. Les actions proposées sont proportionnées aux objectifs poursuivis, qui visent à garantir une gestion coordonnée des crises de cybersécurité au niveau de l'Union.

- **Choix de l'instrument**

Pour atteindre les objectifs susmentionnés, le TFUE prévoit, notamment en son article 292, l'adoption de recommandations par le Conseil, sur la base d'une proposition de la Commission. Conformément à l'article 288 du TFUE, les recommandations ne lient pas. Une recommandation du Conseil est un instrument approprié dans ce cas, car elle marque l'engagement des États membres en faveur des mesures qui y figurent et fournit une base solide pour la coopération dans le domaine de la coordination de la gestion des incidents et crises de cybersécurité majeurs. De cette manière, la recommandation proposée viendrait compléter le cadre juridique contraignant (en particulier la directive SRI 2).

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

- **Consultation des parties intéressées**

Lors de l'élaboration de la présente proposition, la Commission a procédé à une consultation sur le réexamen du schéma directeur en matière de cybersécurité et a invité les États membres et les entités concernées de l'Union à apporter leur contribution. Elle a examiné les points de vue exprimés par les experts des États membres, ainsi que par l'ENISA, lors de l'atelier organisé conjointement à Karpacz le 5 septembre 2024 par la Commission et la Pologne.

La Commission a consulté les représentants des États membres au sein du réseau des centres de réponse aux incidents de sécurité informatiques (réseau des CSIRT), du réseau EU-CyCLONe et du groupe de coopération SRI lors de réunions tenues en septembre 2024 et a sollicité des contributions écrites.

La Commission a présenté et recueilli les retours d'information du Conseil lors de deux discussions spécifiques qui se sont tenues dans le cadre du groupe de travail horizontal «Questions cyber» en octobre et en novembre 2024.

La Commission a consulté des représentants du secteur privé, ainsi que des États membres, du Service européen pour l'action extérieure (SEAE) et de l'ENISA, lors d'un atelier organisé par la représentation permanente de la Pologne auprès de l'UE à Bruxelles en novembre 2024.

La Commission a consulté les entités concernées de l'Union, à savoir le SEAE, l'ENISA, Europol et le service de cybersécurité pour les institutions, organes et organismes de l'Union (CERT-UE), notamment dans le cadre de discussions de haut niveau lors des réunions de la task-force (ou équipe spéciale) chargée des crises cyber[1] qui se sont tenues en juillet et novembre 2024.

Un consensus s'est dégagé sur la nécessité d'un document clair, simple et opérationnel mis à jour permettant aux acteurs concernés de comprendre le cadre de gestion des crises de cybersécurité et d'utiliser efficacement les mécanismes disponibles. Un consensus s'est également dégagé sur la nécessité d'éviter la duplication des instruments et de faire bon usage des mécanismes existants au niveau de l'Union pour la coordination, l'échange d'informations et la réponse, sans créer de nouvelles structures ni interférer avec les procédures opérationnelles standard internes des réseaux et mécanismes sectoriels existants.

[1] Un groupe informel constitué des services de la Commission et d'autres services de l'UE.

2025/0036 (NLE)

Proposition de

RECOMMANDATION DU CONSEIL

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

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 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 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 d'opérations militaires ou de menaces hybrides pluridimensionnelles. 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 citoyens et les entreprises 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) Conformément aux procédures définies dans la décision d'exécution (UE) 2018/1993 du Conseil[2], une décision d'activer ou de désactiver le dispositif intégré de l'Union européenne pour une réaction au niveau politique dans les situations de crise (IPCR) est prise par la présidence du Conseil, qui consulte (sauf lorsque la clause de solidarité

[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, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

a été invoquée) les États membres concernés, la Commission et le haut représentant (HR). En outre, conformément aux instructions de l'IPCR, le secrétariat général du Conseil, les services de la Commission et le SEAE peuvent également convenir, en consultation avec la présidence, d'activer l'IPCR en mode «partage de l'information». Les discussions menées dans le cadre de l'IPCR s'appuient sur des rapports de connaissance et d'analyse intégrées de la situation élaborés par les services de la Commission et le SEAE.

(4) Si les États membres ont une responsabilité première dans la gestion des crises de cybersécurité nationales, la nature transfrontière et transsectorielle potentielle des incidents de cybersécurité exige 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. Dans le même temps, la réaction aux crises et le retour à la normale sont coûteux pour les entités et les secteurs touchés. La gestion des crises 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, les capacités de détection nécessaires pour recenser les outils de réaction et de rétablissement nécessaires pour atténuer, décourager et contenir les incidents de cybersécurité.

(5) La recommandation (UE) 2017/1584 de la Commission[3] sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs a énoncé 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 la gestion des crises au sens large de l'Union, comme le dispositif 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).

(6) 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: le règlement (UE) 2019/881 du Parlement européen et du Conseil[4], la directive (UE) 2022/2555 du Parlement européen et du Conseil[5], le règlement d'exécution (UE) 2024/2690 de la Commission[6], le règlement

---

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, ELI: http://data.europa.eu/eli/reco/2017/1584/oj).

4 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).

5 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).

6 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

(UE/Euratom) 2023/2841 du Parlement européen et du Conseil[7], le règlement (UE) 2021/887 du Parlement européen et du Conseil[8], le règlement (UE) 2024/2847 du Parlement européen et du Conseil[9] et le règlement (UE) 2025/38 du Parlement européen et du Conseil (règlement sur la cybersolidarité)[10]. Les mesures sectorielles spécifiques en cas de crise de cybersécurité comprennent le règlement délégué (UE) 2024/1366 de la Commission[11] 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[12]. La directive 2013/40/UE[13] 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[14], une fois mises en œuvre, faciliteront considérablement l'action répressive dans ce domaine. La politique

---

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).

7 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).

8 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).

9 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).

10 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).

11 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/oj).

12 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/oj).

13 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).

14 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).

de cyberdéfense de l'UE[15] définit les rôles d'un réseau opérationnel d'équipes militaires d'intervention en cas d'urgence informatique de l'UE (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, qui ne sont pas 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»[16] prévoit une coopération entre les acteurs concernés lorsqu'un incident affecte à la fois les aspects physiques et la cybersécurité des infrastructures critiques.

(7) Au niveau de l'Union, les acteurs concernés qui ont des responsabilités en matière de gestion des crises de cybersécurité sont la Commission, le SEAE, y compris la capacité unique d'analyse du renseignement de l'UE (SIAC), 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 par l'intermédiaire de son Centre européen de lutte contre la cybercriminalité (CE3), le réseau européen d'organisations de liaison en cas de crises de cybersécurité (EU-CyCLONe), le réseau des centres de réponse aux incidents de sécurité informatique (CSIRT), le Centre satellitaire de l'UE (CSUE), le Centre de surveillance de la sécurité Galileo (CSSG) et le réseau de délégations de l'Union. Ces acteurs de l'Union devraient définir ensemble les domaines de coopération et contribuer à la mise en œuvre du cadre de gestion des crises de cybersécurité de l'Union, conformément à leurs compétences en vertu de la législation applicable.

(8) Une recommandation actualisée établissant un schéma directeur en matière de cybersécurité est nécessaire pour fournir des orientations claires et accessibles expliquant ce qu'est une crise de cybersécurité au niveau de l'Union, la manière dont le cadre de gestion des crises est déclenché et le rôle des 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 doit être considéré dans le contexte plus large des relations civilo-militaires et des relations UE-OTAN.

(9) La présente recommandation complète le dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR) et les mécanismes de crise plus larges 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), le système de réponse aux crises (SRC) du Service européen pour l'action extérieure (SEAE), ainsi que d'autres processus, tels que ceux décrits dans la boîte à outils hybride de l'UE[17] et dans le protocole opérationnel révisé de l'UE pour la lutte contre les menaces hybrides. Elle complète également 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 (ci-après le «schéma directeur pour les infrastructures critiques»), qui couvre la résilience physique, autre que cyber,

15 JOIN(2022) 49 final.

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

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

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.

(10) Une approche globale et intégrée de la gestion des crises devrait être encouragée dans tous les secteurs et à tous les niveaux de gouvernance. 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 cyberincidents ont des conséquences réelles. Lorsque des incidents de cybersécurité s'inscrivent dans le cadre d'une campagne ou d'une crise hybride plus large, les acteurs concernés devraient soutenir les efforts visant à dresser un tableau de situation unifié dans plusieurs secteurs et domaines. La recommandation contribue aux actions de préparation plus larges requises pour l'Union face aux menaces hybrides pluridimensionnelles [conformément aux principes inscrits dans la stratégie pour une union de la préparation].

(11) La sécurité des infrastructures numériques critiques est fondamentale pour la résilience de l'économie, de la société et de la défense de l'Union. Les entités relevant du champ d'application de la directive (UE) 2022/2555, y compris celles qui fournissent des câbles de communication sous-marins, doivent prendre des mesures pour protéger la sécurité physique et environnementale des réseaux et des systèmes d'information sur la base d'une approche «tous risques», notamment les défaillances du système, les erreurs humaines, les actes malveillants ou les phénomènes naturels. En outre, ces entités devraient signaler les incidents, y compris ceux liés aux câbles de communication sous-marins, aux CSIRT ou, le cas échéant, à l'autorité compétente. Bien que les principes fondamentaux qui sous-tendent le schéma directeur en matière de cybersécurité soient pertinents pour la sécurité des câbles sous-marins, les mécanismes qu'il établit ne sont pas suffisamment complets pour couvrir l'ensemble du cycle de résilience aux crises. Sa nature spécifique justifie un effort concerté et sur mesure pour répondre aux besoins en matière de surveillance intégrée des menaces et d'appréciation de la situation pour les bassins maritimes autour de l'UE, des investissements stratégiques pour créer des redondances et une approche européenne commune pour renforcer les capacités de réparation et de rétablissement. La stratégie de sûreté maritime de l'UE comprend des actions visant à renforcer la cybersécurité dans le domaine maritime et à accroître la surveillance et la protection des infrastructures maritimes critiques, y compris les câbles sous-marins. Pour la gestion des crises au niveau de l'Union, un réseau spécifique de points de contact nationaux et des interactions civilo-militaires étroites, y compris avec l'OTAN, seraient une piste à envisager.

(12) La préparation à une crise nécessite une évaluation globale de tous les risques et de toutes les menaces, compte tenu de la convergence des intérêts de l'UE en matière économique et de sécurité. Une appréciation commune de la situation de l'Union par les États membres et les entités de l'Union, facilitée par l'adoption d'une taxinomie commune et de canaux de communication sécurisés, devrait permettre une réaction coordonnée et éclairée aux incidents de cybersécurité potentiels et majeurs, ainsi que la dissuasion des acteurs de menaces persistantes. Sur la base du principe du besoin d'en connaître et compte tenu de l'importance de la confiance dans le partage d'informations, des groupes d'États membres dans différentes configurations et, le cas échéant, des entités concernées de l'Union pourraient souhaiter coopérer et échanger des informations pertinentes pour la gestion des incidents de cybersécurité. Les États membres et les entités de l'Union qui échangent des informations sur les menaces, les risques et les lacunes en matière de maturité devraient permettre de définir les bonnes

priorités en matière d'investissements sains et d'actions concrètes susceptibles d'améliorer la cyberrésilience.

(13) Conformément à l'article 6 du règlement (UE) 2019/881, l'ENISA, en étroite coopération avec les États membres, élabore régulièrement un rapport approfondi de situation technique en matière de cybersécurité de l'UE sur les incidents et cybermenaces. Ce rapport s'intitule «EU Joint Cyber Assessment Report» (rapport conjoint de l'UE sur la cybersécurité) (EU-JCAR) et est élaboré avec Europol/EC3 et CERT-UE, dans le but de renforcer la préparation de l'Union, étant donné qu'il fournit une appréciation de la situation fondée sur une analyse des incidents et des cybermenaces.

(14) Les infrastructures critiques essentielles, telles que l'énergie, les transports, les infrastructures numériques, la santé ou les services financiers, ainsi que les solutions de sécurité déployées pour les protéger, sont généralement exploitées par des entreprises privées. La protection de ces infrastructures contre les incidents de cybersécurité majeurs nécessite une coopération étroite entre les entités publiques et privées, y compris les fabricants et les développeurs de logiciels libres, fondée sur la confiance et des procédures claires et spécifiques pour le partage d'informations, la diffusion et la coordination de la réaction.

(15) Les exercices de cybersécurité au niveau de l'Union sont un outil très efficace pour tester les procédures et les mécanismes de coopération et, partant, améliorer la préparation. Étant donné que les exercices nécessitent des ressources importantes, le programme des exercices doit être aussi rationalisé et consolidé que possible et tenir compte des scénarios élaborés dans le cadre d'évaluations des risques et d'autres initiatives pertinentes coordonnées au niveau de l'Union.

(16) Les infrastructures numériques européennes présentent de nombreuses dépendances techniques profondément ancrées. Il convient d'y remédier afin d'assurer la continuité des opérations en cas de crise. Cela concerne, par exemple, le système de noms de domaine (DNS), un élément essentiel qui sous-tend les activités de l'internet. Les services de résolution de noms de domaine sont fondamentaux pour accéder à l'internet, y compris en cas de crise de cybersécurité majeure, car ils traduisent les noms de domaine internet en adresses IP. La directive (UE) 2022/2555 encourage les parties prenantes concernées à adopter une stratégie de diversification de la résolution DNS. Elle incite également les États membres à encourager la mise au point et l'utilisation d'un service européen public et sécurisé de résolution de noms de domaine en tant que mesure essentielle pour garantir la préparation et la résilience aux crises.

(17) En outre, afin de renforcer la résilience d'autres composants critiques, tels que le système de routage, et de garantir leur fonctionnalité en cas de crise de cybersécurité majeure, il est fondamental de mettre en œuvre en temps utile les bonnes pratiques correspondantes et les normes les plus récentes disponibles. Par conséquent, le règlement d'exécution (UE) 2024/2690 impose la création d'un forum multipartite afin de recenser les meilleures normes et techniques de déploiement disponibles pour les éléments essentiels de cybersécurité et encourage la participation des entités concernées.

(18) Pour détecter efficacement les activités malveillantes dans les chaînes d'approvisionnement mondiales de plus en plus complexes qui peuvent avoir une incidence à l'échelle de l'Union, une approche coordonnée est nécessaire. Une telle approche est particulièrement pertinente en ce qui concerne les secteurs dans lesquels l'Union s'appuie sur des technologies provenant de fournisseurs à haut risque relevant

de la juridiction d'un pays tiers qui exige que des informations sur les vulnérabilités logicielles ou matérielles soient communiquées à ses autorités avant qu'elles ne soient connues pour être exploitées. Les acteurs soutenus par un État peuvent également se prépositionner dans les infrastructures critiques dans l'intention de provoquer des perturbations ultérieurement, par exemple en cas de conflit. Cette manœuvre est difficile à détecter à l'aide de méthodes traditionnelles, étant donné que les acteurs de la menace dissimulent leurs activités en se mêlant au trafic légitime et en ayant recours à des techniques d'exploitation des ressources locales, qui reposent sur des outils et des processus légitimes pour dissimuler des activités malveillantes. Il en va de même pour les pays tiers dans lesquels, selon des déclarations publiques de l'Union ou de ses États membres, des acteurs de la menace opérant en dehors du territoire de ces pays ont mené des actes de cybermalveillance contre l'Union. Les chaînes d'approvisionnement devraient devenir plus résilientes et plus diversifiées, tout en maintenant une base de référence commune en matière de préparation.

(19) Au niveau technique, les CSIRT, les autorités répressives, ainsi que les cyberpôles nationaux et transfrontières qui seront mis en place en vertu du règlement (UE) 2025/38, jouent un rôle essentiel dans la détection des incidents, des cybermenaces et des vulnérabilités, dans le soutien aux attributions techniques et dans le rétablissement après les cyberattaques. Des modalités procédurales efficaces en matière de coopération entre le réseau des CSIRT et EU-CyCLONe, comme l'exige la directive (UE) 2022/2555, sont fondamentales. Le mécanisme européen d'alerte en matière de cybersécurité vise à soutenir le développement de 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.

(20) En ce qui concerne la réaction immédiate, les mécanismes à la disposition des États membres comprennent la réserve de cybersécurité de l'UE et les mesures de soutien à l'assistance mutuelle établies en vertu du règlement (UE) 2025/38, les équipes d'intervention rapide en cas de menaces hybrides et les équipes d'intervention rapide en cas d'incident informatique (CRRT) de la coopération structurée permanente (CSP), ainsi que des mécanismes prévus pour les alliés de l'OTAN. En outre, le protocole de réaction d'urgence des services répressifs de l'UE aide les autorités répressives 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 efficace des aspects internationaux de leurs enquêtes, y compris la déconfliction au niveau des services répressifs et la coordination avec les partenaires non chargés de la répression. L'obtention d'une vue d'ensemble claire des options de réaction disponibles en cas d'incidents de cybersécurité et d'activités hybrides et de la manière dont elles sont utilisées peut garantir une allocation efficace des ressources et éviter leur double emploi. Dès lors, en vertu du règlement (UE) 2025/38, les États membres sont tenus d'informer le réseau des CSIRT et EU-CyCLONe lorsqu'ils demandent des services de la réserve de cybersécurité de l'UE.

(21) Une lutte efficace contre la cybercriminalité est essentielle à la cybersécurité. La dissuasion ne peut être obtenue uniquement par la résilience, mais nécessite également l'identification, la poursuite des contrevenants et une réponse aux infractions qu'ils ont commises. La coopération au moyen de systèmes et de plateformes techniques adaptés et l'échange d'informations pertinentes entre les acteurs de la cybersécurité, les entités cyberdiplomatiques et les services répressifs sont donc fondamentaux pour garantir

une compréhension complète du panorama des menaces et être en mesure de réagir de manière cohérente et coordonnée.

(22) Les crises génèrent une incertitude que les adversaires peuvent facilement exploiter pour diffuser la désinformation et semer la méfiance. Pour contrer cette situation, une communication publique claire et cohérente sur la situation et les mesures prises pour y remédier est essentielle. Une communication stratégique coordonnée peut également soutenir les mesures diplomatiques à l'égard des acteurs de menaces persistantes et l'élaboration d'un discours sur les menaces pesant sur l'Union, ses actions de dissuasion et la nécessité de promouvoir un comportement responsable des États dans le cyberespace.

(23) Pour une gestion efficace des crises, il est nécessaire de définir des solutions communes de communication sécurisées pour le domaine cyber et de les mettre en œuvre dans l'ensemble de l'Union, y compris, le cas échéant, pour l'échange d'informations classifiées de l'UE. À la demande du Conseil, la Commission et d'autres entités concernées de l'Union ont cartographié les outils de communication sécurisés existants et présenté les résultats en décembre 2022. Plusieurs actions distinctes sont actuellement menées par les entités de l'Union pour renforcer les capacités de communication sécurisées en cas de crise, qui nécessitent une meilleure coordination et un meilleur effet de levier. Il s'agit notamment de la mise en place d'un système de communications critiques de l'UE afin de renforcer la résilience des infrastructures de communications publiques contre des ingérences malveillantes et d'améliorer la coopération opérationnelle quotidienne, y compris par-delà les frontières.

(24) L'environnement de sécurité de l'Union exige une approche de la préparation civile et militaire «tous risques», pangouvernementale et englobant l'ensemble de la société. Les organismes militaires s'appuient sur des infrastructures critiques civiles, telles que les communications, l'énergie, la santé, les transports et la logistique. Par conséquent, et comme le souligne la politique de cyberdéfense de l'UE[18], la cybersécurité de l'UE nécessite une coopération et des synergies accrues entre les capacités de préparation et de réaction des réseaux civils et militaires, y compris en cas d'attaque armée. Les acteurs de la cybersécurité devraient œuvrer ensemble à l'élimination des cloisonnements institutionnels et opérationnels afin d'anticiper la menace de perturbations multisectorielles et pluridimensionnelles et d'y remédier, conformément aux principes qui [doivent être intégrés] dans la stratégie pour une union de la préparation. En outre, les actes de cybermalveillance jouent un rôle croissant dans des campagnes hybrides plus larges menées contre l'Union, ses États membres et ses partenaires stratégiques. Une coopération plus étroite entre l'Union et l'OTAN est donc nécessaire.

(25) Au sein de la communauté militaire, le futur Centre de coordination de l'UE en matière de cyberdéfense et la capacité unique d'analyse du renseignement (SIAC) au sein du service européen pour l'action extérieure, le réseau opérationnel d'équipes militaires d'intervention en cas d'urgence informatique de l'UE (MICNET) et la conférence des cybercommandants de l'UE, facilités par l'Agence européenne de défense (AED), ainsi que les projets pertinents relevant de la coopération structurée permanente (CSP), représentent des acteurs et des initiatives importants en ce qui concerne la coordination et la coopération en matière de préparation à la détection, à la

[18] La politique de cyberdéfense de l'UE; JOIN/2022/49 final.

dissuasion et à la défense contre les cybermenaces qui touchent l'Union et les États membres, ainsi qu'au rétablissement si elles se réalisent. Par conséquent, il convient d'encourager la coopération entre les acteurs civils et militaires, telle que la coopération entre EU-CyCLONe et la conférence des cybercommandants de l'UE, ainsi que la collaboration potentielle entre MICNET et le réseau des CSIRT.

(26) La coopération avec les pays et organisations partenaires internationaux stratégiques en dehors de l'Union renforce les capacités de l'Union en matière de cybersécurité. En favorisant la coopération internationale, l'Union et ses partenaires peuvent garantir une appréciation commune de la situation et une cohérence dans la gestion des crises de cybersécurité ainsi qu'une posture cyber solide, contribuant ainsi à un cyberespace mondial, ouvert, stable, sûr et résilient. Cette coopération devrait reposer sur la confiance et l'objectif commun de protéger les infrastructures critiques et les services essentiels contre les cybermenaces, notamment en promouvant un comportement responsable des États dans le cyberespace fondé sur le cadre des Nations unies et en obligeant les acteurs de la menace à rendre compte de leur comportement irresponsable et illégal dans le cyberespace. Les mesures cyberdiplomatiques contribuent à la dissuasion et à la réaction aux actes de cybermalveillance et prévoient une coordination et une coopération avec les pays partenaires internationaux stratégiques,

A ADOPTÉ LA PRÉSENTE RECOMMANDATION:

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

(1) La présente recommandation 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 menaces hybrides pluridimensionnelles. La manière dont un incident peut se transformer en incident de grande ampleur et, par voie de conséquence, en crise au niveau de l'UE est illustrée et résumée à l'annexe I, y compris lorsqu'un tel incident coïncide avec d'autres menaces hybrides nécessitant une coordination des réponses nécessaires. Le cadre relatif à la gestion des crises de cybersécurité devrait permettre aux acteurs concernés au niveau de l'Union, y compris les entités et les réseaux, de comprendre comment interagir et utiliser au mieux les mécanismes existants énumérés à l'annexe II tout au long du cycle de vie de la gestion des crises. En outre, il formule des recommandations à ces acteurs au niveau de l'Union quant aux moyens d'améliorer l'efficacité des mécanismes existants.

(2) L'Union et ses États membres devraient suivre le schéma directeur en matière de cybersécurité dans la gestion d'une crise résultant d'un incident de cybersécurité majeur, tel que défini à l'article 6, point 7), de la directive (UE) 2022/2555, qui affecte le bon fonctionnement du marché intérieur ou présente des risques graves de sécurité et de sûreté publiques pour des entités ou des citoyens de plusieurs États membres ou de l'Union dans son ensemble («crise de cybersécurité»).

(3) Lorsqu'un incident de cybersécurité, détecté au niveau technique par un CSIRT ou un cyberpôle, entraîne une escalade dans le cadre des procédures internes du réseau des CSIRT, les informations appropriées devraient être partagées avec EU-CyCLONe conformément aux modalités procédurales pertinentes, qui devraient à son tour examiner s'il s'agit d'un incident majeur potentiel ou en cours au sens de l'article 6, point 7), de la directive (UE) 2022/2555. Il convient de déterminer si une crise de cybersécurité existe ou cesse d'exister à la suite de cet incident majeur,

conformément à la décision d'exécution (UE) 2018/1993, et notamment à ses articles 4 et 5.

(4) Conformément aux principes de proportionnalité, de subsidiarité, de complémentarité et de confidentialité des informations énoncés à l'annexe III, 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. Bien que le schéma directeur en matière de cybersécurité n'interfère pas avec la manière dont les entités définissent leurs procédures internes, chaque entité devrait définir clairement les interfaces utilisées pour travailler avec d'autres entités. Ces interfaces devraient faire l'objet d'un accord commun entre les entités concernées et être clairement documentées.

(5) Le schéma directeur en matière de cybersécurité devrait être appliqué en cohérence avec le schéma directeur pour les infrastructures critiques, en particulier en cas d'incidents affectant à la fois la résilience physique et la cybersécurité des infrastructures critiques[19]. Lorsqu'il existe des mesures sectorielles de gestion des crises couvrant les incidents de cybersécurité, ces mesures devraient être mises en œuvre de manière cohérente avec la présente recommandation.

II: Se préparer à une crise de cybersécurité au niveau de l'Union

(a) Appréciation de la situation et partage d'informations

(6) Des données vérifiées et fiables, y compris les tendances en matière d'incidents, de tactiques, de techniques et de procédures, et les vulnérabilités activement exploitées devraient servir de base à une appréciation commune de la situation du panorama des cybermenaces par les États membres et les entités de l'Union. Ces connaissances partagées devraient être utilisées par les États membres et les entités de l'Union pour anticiper les cyberattaques, s'y préparer et les détecter, conformément à leurs domaines de responsabilité respectifs. Cette appréciation commune de la situation devrait:

(a) s'appliquer à tous les secteurs critiques énumérés dans la directive (UE) 2022/2555, en particulier les communications, les infrastructures numériques, l'énergie, les transports, la finance, l'espace et la santé, et également s'appliquer, par l'intermédiaire du CERT-UE, aux réseaux et systèmes des entités de l'Union conformément au règlement (UE/Euratom) 2023/2841;

(b) reposer sur des ensembles de données de haute qualité, diversifiés et intégrés, qui sont collectés, traités et partagés en temps réel;

(c) être prise en considération dans le rapport conjoint de l'UE sur la cybersécurité (JCAR) et dans d'autres produits pertinents;

(d) tenir compte des menaces hybrides connexes, y compris les activités de manipulation de l'information et d'ingérence menées depuis l'étranger et la désinformation;

(e) soutenir les actions à court terme et les mesures de réaction, ainsi que contribuer à la planification des politiques à long terme dans le contexte de la préparation et de la dissuasion;

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

(f) [lien vers d'autres évaluations des risques et des menaces produites régulièrement et renforcées par la stratégie pour une union de la préparation afin de garantir des synergies et une simplification des obligations de déclaration qui incombent aux États membres.]

(7) 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 les membres;

(c) tirer pleinement parti des outils disponibles pour le partage d'informations.

(8) Les États membres et les entités concernées de l'Union devraient améliorer les moyens de se coordonner et de coopérer avec le secteur privé, y compris les communautés et les fabricants de logiciels libres, afin d'améliorer le partage d'informations, en s'appuyant sur les centres d'échange et d'analyse d'informations existants au niveau de l'UE et au niveau national, de renforcer les capacités en matière de cybersécurité et de réagir aux incidents de cybersécurité, y compris au moyen de tables rondes avec EU-CyCLONe et le réseau des CSIRT.

(9) Les États membres et les entités concernées de l'Union pourraient choisir, afin de faire progresser la coopération et de renforcer la confiance, et en s'appuyant sur les accords de partage d'informations en matière de cybersécurité de la directive (UE) 2022/2555 et les dispositions du règlement (UE) 2025/38 relatives aux cyberpôles, de créer des groupes collaboratifs volontaires fondés sur le besoin d'en connaître lorsqu'il existe des préoccupations communes, telles que la dissuasion, la détection ou la réaction concernant un type particulier de menace auquel chaque État membre ou entité est confronté dans sa situation spécifique. Tout groupement de ce type devrait respecter le mandat des acteurs concernés, ainsi que les structures déjà établies. Ces groupes collaboratifs pourraient faire appel aux entités de l'Union pour faciliter leur coopération, y compris au moyen d'infrastructures appropriées.

(10) Les États membres, par l'intermédiaire du groupe de coopération SRI institué par la directive (UE) 2022/2555, devraient, dans un délai de douze mois à compter de l'adoption du schéma directeur en matière de cybersécurité, élaborer une taxinomie commune en ce qui concerne la gestion des crises de cybersécurité et fournir un guide sur le traitement et l'échange sécurisés d'informations relatives aux incidents et crises de cybersécurité, y compris une section consacrée à la détermination du niveau de confidentialité de ces informations (catégorisation).

(11) Lorsqu'ils déterminent le niveau de confidentialité des informations disponibles, les États membres et les entités concernées de l'Union devraient tenir compte de l'incidence potentielle que la surclassification peut avoir sur l'échange volontaire d'informations et l'appréciation commune de la situation. Lorsqu'ils partagent des informations non classifiées, 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 EU-CyCLONe.

b) Exercices communs

(12) Les États membres et les entités concernées de l'Union devraient mettre au point un cycle continu efficace d'exercices de cybersécurité afin de se préparer aux crises de cybersécurité et d'améliorer l'efficacité organisationnelle. Ces exercices devraient se fonder sur les scénarios élaborés sur la base d'évaluations des risques coordonnées

au niveau de l'UE, y compris celles concernant les crises multisectorielles. Le cycle continu d'exercices de cybersécurité devrait tenir compte du MPCU et d'autres mécanismes de réaction aux crises au niveau de l'Union. Il devrait garantir que les enseignements tirés des exercices sont effectivement mis en œuvre.

(13) Les acteurs concernés de l'Union pourraient mener des exercices de moindre envergure pour tester leurs interactions et leurs interfaces en cas d'escalade des incidents de cybersécurité.

(14) Les services de la Commission, le SEAE et l'ENISA sont invités à organiser un exercice visant à tester le schéma directeur en matière de cybersécurité dans un délai de 18 mois à compter de l'adoption du schéma directeur, en associant tous les acteurs concernés, y compris le secteur privé.

c) Capacités de résolution DNS

(15) Les États membres, les entités concernées de l'Union ainsi que les entités privées telles que les opérateurs d'infrastructures critiques devraient renforcer leur stratégie de diversification de la résolution DNS, comprenant l'utilisation d'au moins une infrastructure DNS basée dans l'Union, telle que DNS4EU, afin de garantir une résolution DNS fiable en cas de crise majeure. L'ENISA et EU-CyCLONe devraient élaborer et mettre à disposition des lignes directrices en matière de relais d'urgence qui définissent les étapes du passage à une infrastructure DNS basée dans l'Union en cas de défaillance d'autres services DNS, garantissant ainsi la continuité des services critiques en cas de crise.

(16) En outre, les cyberpôles nationaux et les cyberpôles transfrontières devraient partager des informations pertinentes sur les menaces avec ces infrastructures DNS basées dans l'Union afin de les aider à assurer un niveau élevé de protection contre les menaces spécifiques à l'Union et, partant, à accroître encore les capacités de détection et d'atténuation des menaces propres à l'Union.

(17) Afin de renforcer de manière générale la sécurité et la disponibilité des infrastructures internet critiques, y compris en cas de crise, les États membres devraient encourager activement la participation de tous les acteurs concernés – y compris ceux qui ne sont pas directement visés par la directive SRI 2 – au sein du forum multipartite mandaté, chargé de recenser les meilleures normes et meilleures techniques de déploiement disponibles pour les mesures de sécurité essentielles des réseaux. En outre, les États membres devraient envisager de participer au forum et adopter eux-mêmes les lignes directrices recommandées.

d) Ressources

(18) Les États membres devraient utiliser pleinement les ressources financières disponibles pour la cybersécurité prévues par les programmes pertinents de l'Union.

III: Détection d'un incident susceptible d'évoluer vers une crise de cybersécurité

(19) Pour faire face à la complexité croissante des incidents de cybersécurité et aux défis grandissants liés à leur détection, les entités tant publiques que privées devraient mettre en œuvre des stratégies de détection éclairées sur l'ensemble de leurs infrastructures numériques, afin de recenser les éventuels prépositionnements qui pourraient être exploités ultérieurement à des fins de perturbation. Lorsque des opérations dissimulées sont détectées, les entités devraient partager de manière proactive les informations pertinentes avec leurs partenaires, bien avant que les situations ne deviennent des crises.

(20) Tous les acteurs devraient apporter leur contribution, conformément à leurs mandats respectifs et sur la base de l'approche «tous risques», en communiquant aux réseaux concernés des informations indiquant une crise de cybersécurité potentielle.

(21) Le réseau des CSIRT et 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.

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

(23) Les cyberpôles transfrontières, déjà établis ou devant être mis en place en vertu du règlement (UE) 2025/38, devraient apporter leur contribution en fournissant des informations pertinentes aux mécanismes au niveau de l'Union en cas d'incident de cybersécurité majeur potentiel ou en cours sur la base de l'approche «tous risques», y compris les dommages physiques causés aux infrastructures critiques qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou traitées ou des services offerts par les réseaux et systèmes d'information ou accessibles par l'intermédiaire de ceux-ci.

(24) Lorsqu'un incident de cybersécurité potentiel ou majeur ayant une incidence multisectorielle est détecté:

(a) la Commission devrait faciliter le flux d'informations nécessaires entre les points de contact pour les mécanismes de crise horizontaux et sectoriels pertinents au niveau de l'Union énumérés à l'annexe II et EU-CyCLONe;

(b) les entités concernées de l'Union devraient aider EU-CyCLONe à évaluer les conséquences pour les secteurs et la population.

IV: Réagir à une crise de cybersécurité au niveau de l'Union

(25) En cas de crise de cybersécurité établie au titre de l'IPCR, tous les acteurs devraient réagir en étroite coordination avec d'autres entités qui répondent aux menaces hybrides plus larges dans le cadre d'une approche pangouvernementale, comme suit:

(a) le ou les États membres concernés et le réseau des CSIRT devraient coopérer pour rétablir rapidement les systèmes compromis, en garantissant une perturbation opérationnelle minimale;

(b) EU-CyCLONe, en coopération avec le réseau des CSIRT, devrait fournir des informations claires au niveau politique sur l'impact, les conséquences possibles et les mesures de réaction à l'incident et de retour à la normale, y compris en contribuant au rapport de connaissance et d'analyse intégrées de la situation (ISAA) dans le cadre de l'IPCR;

(c) la Commission, en coopération avec le haut représentant, le cas échéant, devrait assurer la cohérence et la coordination entre les réactions à la crise et les actions de réaction connexes au niveau de l'Union, en particulier les mécanismes sectoriels pertinents de gestion des crises au niveau de l'Union énumérés à l'annexe II, et en ce qui concerne la demande d'assistance par l'intermédiaire du MPCU;

(d) la présidence du Conseil devrait envisager d'inviter le président d'EU-CyCLONe à des tables rondes informelles et à d'autres réunions pertinentes du Conseil dans le cadre de l'IPCR;

(e) le Conseil, soutenu par EU-CyCLONe et les entités concernées de l'Union, devrait coordonner les efforts de communication publique, y compris pour veiller à ce que la situation de crise ne soit pas utilisée pour diffuser des informations inexactes;

(f) le haut représentant, en étroite coopération avec la Commission et d'autres entités concernées de l'Union, devrait soutenir la prise de décision au sein du Conseil, y compris au moyen d'analyses et de rapports, sur le recours à d'éventuelles mesures dans le cadre de la boîte à outils cyberdiplomatique. 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;

(g) la Commission, le haut représentant et les États membres devraient également utiliser plus efficacement des outils économiques tels que les interdictions commerciales afin de mieux prévenir et décourager les actes de cybermalveillance persistants commis par des acteurs étatiques, et d'y réagir.

(26) Lorsqu'un utilisateur des services fournis par la réserve de cybersécurité de l'UE[20] demande des services à la réserve de cybersécurité de l'Union conformément à l'article 15 du règlement (UE) 2025/38, et sans préjudice de tout acte d'exécution futur au titre dudit règlement:

(a) les services doivent être déployés dans les 24 heures qui suivent la demande;

(b) la Commission et le haut représentant devraient assurer la coordination avec des mesures supplémentaires, conformément à la boîte à outils hybride[21] en cas d'actes de cybermalveillance qui s'inscrivent dans le cadre d'une campagne hybride plus large;

(c) en cas d'acte de cybermalveillance revêtant une dimension militaire, l'État membre demandeur devrait informer la Conférence des cybercommandants de l'UE de sa demande.

(27) En cas d'incident de cybersécurité majeur affectant le bon fonctionnement des services spatiaux essentiels pour la sécurité de l'Union ou de ses États membres, EU-CyCLONe devrait informer le haut représentant en vue de coordonner une éventuelle réaction avec l'architecture de réaction aux menaces spatiales établie conformément à la décision (PESC) 2021/698 du Conseil.

---

[20] La réserve de cybersécurité de l'Union est un mécanisme qui se compose de services fournis par des fournisseurs de services de sécurité gérés de confiance visant, sur demande, à soutenir les mesures de réaction et à amorcer le rétablissement en cas d'incidents de cybersécurité importants, d'incidents de cybersécurité majeurs ou d'incidents de cybersécurité assimilés à des incidents majeurs touchant des États membres, des institutions, organes ou organismes de l'Union ou des pays tiers associés au programme pour une Europe numérique.

[21] 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.

V: Rétablissement après une crise de cybersécurité

(28) 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 exercices menés, 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.

VI: Communications sécurisées

(29) Sur la base de la cartographie des outils de communication sécurisés existants[22], la Commission, le haut représentant, EU-CyCLONe, le réseau des CSIRT et les entités concernées de l'Union devraient convenir, d'ici fin 2026, d'un ensemble interopérable de solutions de communication sécurisées pour les acteurs concernés de l'Union. Ces solutions devraient couvrir l'ensemble des modes de communication requis (voix, données, vidéoconférence, messagerie, collaboration, partage et consultation de documents). Les solutions devraient prendre en considération des principes clés tels que les intérêts de l'Union en matière de sécurité, la souveraineté technologique et la confidentialité, ainsi que des caractéristiques telles que la facilité d'utilisation, la sécurité dès la conception, la certification par les organismes européens chargés de la sécurité de l'information, le chiffrement de bout en bout, l'authentification, la disponibilité et la cryptographie post-quantique. Les solutions devraient répondre à des exigences communément définies en matière de protection des informations sensibles non classifiées et comprendre des outils pour l'échange d'informations classifiées RESTREINT UE/EU RESTRICTED.

(30) Sur cette base, les acteurs au niveau de l'Union devraient utiliser des solutions fondées sur le protocole Matrix pour la communication en temps réel. 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, 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 ces outils.

(31) 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.

(32) À moyen terme, 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. Ces mécanismes devraient respecter le rôle de chaque partie et éviter toute ingérence dans les opérations en cours. La Commission travaille avec les États membres à la mise en place du système de communication critique de l'UE, qui devrait relier d'ici à 2030 les réseaux de communication des services répressifs et de la protection civile dans l'ensemble de l'espace Schengen, de sorte que les équipements de communication critiques puissent être utilisés sur le territoire d'autres États membres. Le système de communication critique de l'UE peut donc également bénéficier de la réponse conjointe avec les cybercommunautés concernées. Ce système devrait intégrer des

[22] HWPCI WK 862/23.

communications de sauvegarde au moyen, par exemple, de communications par satellite.

VII: Coordination des crises de cybersécurité avec les acteurs militaires

(33) EU-CyCLONe et la conférence des cybercommandants de l'UE, MICNET et le réseau des CSIRT, ainsi qu'un futur Centre de coordination de l'UE en matière de cyberdéfense et ses homologues civils de l'Union, devraient coopérer afin de parvenir à une appréciation commune de la situation par les acteurs civils et militaires.

(34) L'Union, compte tenu des accords existants tels que l'accord technique CERT-UE/OTAN de 2016, devrait s'efforcer d'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. À cette fin, l'Union devrait étudier les moyens d'améliorer les capacités de partage d'informations avec l'OTAN, y compris par d'éventuelles interconnexions entre leurs systèmes d'information et de communication respectifs.

(35) Lorsqu'un État membre, dans le contexte d'un incident de cybersécurité, utilise des initiatives pertinentes en matière de défense, telles que les CRRT de la CSP ou d'autres initiatives pertinentes, telles que les équipes d'intervention rapide de l'UE en cas de menaces hybrides, il devrait en informer EU-CyCLONe ainsi que la conférence des cybercommandants de l'UE.

VIII: Coopération avec les partenaires stratégiques

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

(a) lorsqu'un incident pertinent est détecté, faciliter le flux d'informations nécessaires avec les partenaires stratégiques;

(b) renforcer la coordination avec les partenaires stratégiques en ce qui concerne la réaction aux activités de cybermalveillance durables menées par des acteurs de menaces persistantes, notamment lors de l'utilisation de la boîte à outils cyberdiplomatique, conformément à ses orientations d'application.

(37) 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 de cyberincidents potentiels ou majeurs.

(38) Dans le cadre du cycle continu d'exercices visé à la section II, les services de la Commission et le SEAE devraient envisager d'organiser un exercice conjoint du personnel afin de tester la coopération entre les composantes civile et militaire en cas d'incident de cybersécurité majeur touchant des États membres de l'Union et des alliés de l'OTAN, y compris lorsque les articles 4 ou 5 du traité de l'OTAN sont déclenchés ou sont susceptibles de l'être.

(39) Compte tenu de l'exposition des pays candidats et du potentiel des incidents de cybersécurité survenant dans le voisinage de l'Union, il convient d'envisager des exercices conjoints associant les pays candidats.

Fait à Bruxelles, le

Par le Conseil

Le président