II

(Actes non législatifs)

RECOMMANDATIONS

RECOMMANDATION (UE) 2021/1086 DE LA COMMISSION

du 23 juin 2021

sur la création d'une unité conjointe de cybersécurité

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 292,

considérant ce qui suit:

- (1) La cybersécurité est essentielle à la réussite de la transformation numérique de l'économie et de la société. L'Union européenne s'est engagée à des niveaux d'investissement sans précédent pour garantir la confiance des citoyens, des entreprises et des pouvoirs publics dans les outils numériques.
- (2) La pandémie de COVID-19 a accru l'importance de la connectivité et la dépendance de l'Europe à l'égard de réseaux et systèmes d'information stables et a montré la nécessité de protéger l'ensemble de la chaîne d'approvisionnement. La fiabilité et la sécurité des réseaux et des systèmes d'information sont particulièrement importantes pour les entités qui se trouvent en première ligne dans la lutte contre la pandémie, telles que les hôpitaux, les organismes médicaux et les fabricants de vaccins. La coordination des efforts déployés dans l'Union pour empêcher, détecter, décourager, prévenir, atténuer et contrer les cyberattaques les plus lourdes de conséquences contre ces entités pourrait éviter des pertes de vies humaines et prévenir les tentatives visant à compromettre la capacité de l'Union à vaincre la pandémie de la manière la plus rapide possible. En outre, le renforcement de la capacité de l'Union à lutter efficacement contre les cyberattaques contribue à faire progresser un cyberspace mondial, ouvert, stable et sûr.
- (3) Face à des menaces transfrontières en matière de cybersécurité et à la multiplication continue d'attaques plus complexes, omniprésentes et ciblées ⁽¹⁾, les institutions et acteurs compétents en matière de cybersécurité devraient accroître leur capacité à réagir à de telles menaces et attaques en exploitant les ressources existantes et en coordonnant mieux les efforts. Tous les acteurs concernés dans l'Union doivent être prêts à réagir collectivement et à échanger des informations en se fondant sur le «besoin de partager» plutôt que sur le «besoin d'en connaître».
- (4) Malgré les progrès importants réalisés grâce à la coopération entre les États membres en matière de cybersécurité, en particulier par l'intermédiaire du groupe de coopération SRI et du réseau des centres de réponse aux incidents de sécurité informatique (CSIRT) créé en vertu de la directive (UE) 2016/1148 du Parlement européen et du Conseil ⁽²⁾, il n'existe toujours pas de plateforme commune de l'Union où les informations recueillies dans différentes communautés de cybersécurité puissent être échangées de manière efficace et sûre et qui permette aux acteurs concernés de coordonner et de mobiliser les capacités opérationnelles. En conséquence, les menaces et incidents de cybersécurité risquent d'être traités de manière cloisonnée, ce qui limite l'efficacité et accroît la vulnérabilité. En outre, il manque au niveau de l'Union un canal de coopération technique et opérationnelle avec le secteur privé, tant en ce qui concerne le partage d'informations que le soutien à la réaction aux incidents.

⁽¹⁾ ENISA, Paysage des menaces 2020; Europol, Évaluation de la menace que représente la criminalité organisée sur l'internet (iOCTA) 2020.

⁽²⁾ Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).

- (5) Les cadres et structures existants ainsi que les ressources et l'expertise disponibles dans les États membres et les institutions, organes et organismes compétents de l'Union constituent une base solide pour apporter une réponse collective aux menaces, incidents et crises de cybersécurité ⁽³⁾. Cette architecture existante comprend, sur le plan opérationnel, le plan d'action pour une réaction coordonnée aux incidents et crises transfrontières de cybersécurité majeurs (ci-après le «plan d'action») ⁽⁴⁾, le réseau des CSIRT et le réseau européen pour la préparation et la gestion des crises cyber («UE-CyCLONE») ⁽⁵⁾, ainsi que le Centre européen de lutte contre la cybercriminalité (EC3) et la Force d'action anticybercriminalité européenne (J-CAT) de l'Agence de l'Union européenne pour la coopération des services répressifs (Europol), et le protocole de réaction d'urgence des services répressifs de l'Union. Le groupe de coopération SRI, le Centre de situation et de renseignement de l'Union («INTCEN») et la boîte à outils cyberdiplomatie ⁽⁶⁾ ainsi que les projets liés à la cyberdéfense lancés dans le cadre de la coopération structurée permanente (CSP) ⁽⁷⁾ contribuent également à la coopération stratégique et opérationnelle dans différentes communautés de cybersécurité. L'Agence de l'Union européenne pour la cybersécurité (ENISA), en vertu de son mandat renforcé, est chargée de soutenir la coopération opérationnelle ⁽⁸⁾ en ce qui concerne la cybersécurité des réseaux et des systèmes d'information, les utilisateurs de ces systèmes et d'autres personnes touchées par des menaces et incidents de cybersécurité. Grâce au dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR), l'Union est en mesure de coordonner sa réaction politique aux crises graves, y compris en cas de cyberattaques majeures.
- (6) Toutefois, il n'existe pas encore de mécanisme permettant d'exploiter les ressources existantes et d'assurer une assistance mutuelle dans l'ensemble des cybercommunautés chargées de la sécurité des réseaux et des systèmes d'information, de la lutte contre la cybercriminalité, de la cyberdiplomatie et, le cas échéant, de la cyberdéfense en cas de crise. Il n'existe pas non plus, au niveau de l'Union, de mécanisme global de coopération technique et opérationnelle entre toutes les communautés en matière de connaissance de la situation, de préparation et de réaction. En outre, Europol et l'INTCEN devraient permettre de parvenir à des synergies avec les services répressifs et les services de renseignement, respectivement.
- (7) La Commission, le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité (haut représentant), les États membres et les institutions, organes et organismes compétents de l'Union reconnaissent qu'il est important d'analyser les forces, les faiblesses, les lacunes et les doubles emplois de l'architecture actuelle de cybersécurité de l'Union qui a été créée ces dernières années. En consultation avec les États membres, la Commission, avec la participation du haut représentant, a élaboré le concept d'unité conjointe de cybersécurité à la suite de cette analyse et en tant qu'élément important de la stratégie pour l'union de la sécurité ⁽⁹⁾, de la stratégie numérique ⁽¹⁰⁾ et de la stratégie de cybersécurité ⁽¹¹⁾.

⁽³⁾ Le réseau européen pour la préparation et la gestion des crises cyber (UE-CyCLONE) a été créé par les États membres à la suite de la recommandation relative au plan d'action. Il s'agit d'un réseau d'experts nationaux en matière de gestion opérationnelle et de gestion des crises, que la Commission a proposé de codifier par la directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148 [COM(2020) 823 final, 2020/0359 (COD)], proposée en décembre 2020.

⁽⁴⁾ 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).

⁽⁵⁾ La présente recommandation tient compte du rapport d'intervention faisant suite à l'exercice de simulation Blue OLEx («Blueprint Operational Level Exercise») pour 2020, et notamment du résumé qu'a fait la présidence de la réflexion stratégique et politique sur l'unité conjointe de cybersécurité.

⁽⁶⁾ Conclusions du Conseil du 19 juin 2017 relatives à un cadre pour une réponse diplomatique conjointe de l'Union européenne face aux actes de cybermalveillance («boîte à outils cyberdiplomatie») (9916/17).

⁽⁷⁾ En particulier, le projet CSP intitulé «équipes d'intervention rapide en cas d'incident informatique et assistance mutuelle dans le domaine de la cybersécurité», coordonné par la Lituanie, et le projet CSP sur le «centre de coordination dans le domaine du cyber et de l'information», coordonné par l'Allemagne.

⁽⁸⁾ L'article 7 du 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) n° 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15) exige de l'Agence qu'elle apporte son soutien à la coopération opérationnelle entre les États membres, les institutions, organes et organismes de l'Union, et entre les parties prenantes. Il s'agit notamment de soutenir les États membres en ce qui concerne la coopération opérationnelle au sein du réseau des CSIRT, de préparer à intervalles réguliers un rapport approfondi de situation technique en matière de cybersécurité de l'Union européenne sur les incidents et cybermenaces dans l'Union et de contribuer à l'élaboration d'une réaction concertée au niveau de l'Union et des États membres en cas d'incidents ou de crises transfrontières majeures. En outre, l'ENISA contribue à des actions de formation avec le Collège européen de sécurité et de défense (CESD).

⁽⁹⁾ Communication de la Commission au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions relative à la stratégie de l'UE pour l'union de la sécurité, COM(2020) 605 final.

⁽¹⁰⁾ Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Façonner l'avenir numérique de l'Europe, COM (2020) 67 final.

⁽¹¹⁾ Communication conjointe au Parlement européen et au Conseil — La stratégie de cybersécurité de l'UE pour la décennie numérique, JOIN(2020) 18 final.

- (8) En cas de crise, les États membres devraient pouvoir compter sur la solidarité de l'Union sous la forme d'une assistance coordonnée, notamment de la part de l'ensemble des quatre cybercommunautés, à savoir les communautés civile, diplomatique, répressive ⁽¹²⁾ et, le cas échéant, militaire du domaine de la cybersécurité. Le degré d'intervention des participants d'une ou de plusieurs communautés peut dépendre de la nature de l'incident ou de la crise majeur(e) à gérer et, par conséquent, du type de contre-mesures qui seront nécessaires pour y répondre. En cas de menace, d'incident ou de crise de cybersécurité, la disponibilité d'experts bien formés et d'équipements techniques constitue un atout essentiel qui peut contribuer à éviter de graves dommages et à assurer le rétablissement effectif des activités. Par conséquent, des capacités techniques et opérationnelles clairement répertoriées, principalement des experts et des équipements prêts à être déployés dans les États membres en cas de besoin, seront les éléments centraux de l'unité conjointe de cybersécurité. Au sein de cette plateforme, les participants occuperont une position unique pour développer et coordonner ces capacités par l'intermédiaire des équipes de réaction rapide de l'Union en matière de cybersécurité, tout en assurant des synergies appropriées avec les projets de cybersécurité existants menés dans le cadre de la CSP.
- (9) L'unité conjointe de cybersécurité fournit une plateforme virtuelle et physique et ne nécessite pas la création d'un corps autonome supplémentaire. Sa création ne devrait pas avoir d'incidence sur les compétences et les pouvoirs des autorités nationales de cybersécurité et des entités concernées de l'Union. L'unité conjointe de cybersécurité devrait être fondée sur des protocoles d'accord entre ses participants. Elle devrait s'appuyer sur des structures, des ressources et des capacités existantes et leur apporter une valeur ajoutée, constituant ainsi une plateforme pour une coopération opérationnelle et technique sécurisée et rapide entre les entités de l'Union et les autorités des États membres. Elle devrait également fédérer toutes les communautés du domaine de la cybersécurité, à savoir les communautés civile, répressive, diplomatique et militaire. Les participants à la plateforme devraient avoir un rôle opérationnel ou de soutien. Parmi les participants ayant un rôle opérationnel devraient figurer l'ENISA, Europol, l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'Union (CERT-UE), la Commission, le Service européen pour l'action extérieure (y compris l'INTCEN), le réseau des CSIRT et le réseau UE-CyCLONe. Les participants ayant un rôle de soutien devraient inclure l'Agence européenne de défense (AED), le (la) président(e) du groupe de coopération SRI, le (la) président(e) du groupe horizontal «Questions liées au cyberspace» du Conseil et un représentant des projets CSP concernés ⁽¹³⁾. Étant donné que les États membres disposent de capacités et de compétences opérationnelles pour faire face à des menaces, incidents et crises de cybersécurité majeurs, les participants à la plateforme devraient principalement s'appuyer sur leurs capacités, avec l'aide des entités compétentes de l'Union, pour atteindre leurs objectifs.
- (10) L'unité conjointe de cybersécurité devrait donner un nouvel élan au processus lancé en 2017 avec le plan d'action. Elle devrait continuer à rendre opérationnelle l'architecture prévue dans le plan d'action et franchir une étape décisive vers la mise en place d'un cadre européen de gestion des crises de cybersécurité, dans lequel les menaces et les risques seront recensés, atténués et traités de manière prompte et coordonnée. Ce faisant, l'unité conjointe de cybersécurité devrait aider l'Union à faire face aux menaces actuelles et imminentes.
- (11) En participant à l'unité conjointe de cybersécurité, les participants ayant un rôle opérationnel et ceux ayant un rôle de soutien devraient être en mesure de dialoguer avec un éventail plus large de parties prenantes, au titre du cadre de l'Union pour la réaction aux crises de cybersécurité. Tout en exerçant leurs fonctions dans les limites de leur mandat, les participants devraient bénéficier d'une meilleure préparation et d'une connaissance élargie de la situation englobant tous les aspects liés aux menaces et incidents de cybersécurité, et tirer parti d'une expertise supplémentaire en matière de cybersécurité. Par exemple, les participants devraient être régulièrement associés à des exercices intercommunautaires, se voir confier un rôle bien défini dans le plan de réaction aux crises de l'Union, rendre leurs actions plus visibles grâce à une communication publique partagée et conclure des accords de coopération opérationnelle avec le secteur privé. Parallèlement, la contribution à l'unité conjointe de cybersécurité devrait permettre aux participants de renforcer les réseaux existants, tels que le réseau des CSIRT et le réseau EU CyCLONe, en leur fournissant des outils sécurisés d'échange d'informations et de meilleures capacités de détection (centres des opérations de sécurité, «COS») et en leur permettant d'utiliser les capacités opérationnelles disponibles de l'Union.
- (12) Les participants à l'unité conjointe de cybersécurité devraient se concentrer sur la coopération technique et opérationnelle, y compris les opérations conjointes. Les participants devraient contribuer à cette coopération dans la mesure où leur mandat le permet. La coopération devrait s'appuyer sur les efforts déjà engagés et les compléter. En fonction du type de coopération envisagé, d'autres participants peuvent y prendre part.

⁽¹²⁾ Également compétente pour la coopération judiciaire.

⁽¹³⁾ Voir la note de bas de page 5. Le SEAE et l'AED, dans le cadre de leur rôle de gestion du secrétariat de la CSP, se concerteront avec les coordinateurs des projets CSP concernés.

- (13) La plateforme devrait rassembler des experts techniques et opérationnels de la gestion des crises provenant des États membres et des entités de l'Union, en vue de coordonner les réactions aux menaces, incidents et crises de cybersécurité en utilisant les capacités et l'expertise existantes. Les experts participant à l'unité conjointe de cybersécurité seront en mesure de surveiller et de protéger une surface d'exposition beaucoup plus vaste en utilisant la plateforme dans ses composantes tant physique que virtuelle. À cette fin, les participants devraient coordonner leurs efforts en cas d'incidents et de crises transfrontières, ainsi que la fourniture, via la plateforme, d'une assistance aux pays touchés par des incidents.
- (14) La mise sur pied de l'unité conjointe de cybersécurité passe par un processus progressif qui exploite et consolide les cadres et structures existants mentionnés dans la présente recommandation, notamment les mécanismes de collaboration mis en place dans le cadre des enceintes dirigées par les États membres (par exemple, le réseau des CSIRT, le réseau EU CyCLONe, le groupe horizontal «Questions liées au cyberspace» du Conseil, J-CAT et les projets CSP concernés) et, du côté des institutions organes et agences de l'Union, la coopération structurée entre l'ENISA et le CERT-UE et celle du groupe interinstitutionnel d'échange d'informations sur la cybersécurité. En outre, les cadres relatifs aux menaces hybrides, à la protection civile ⁽¹⁴⁾ et certains cadres sectoriels ⁽¹⁵⁾ devraient être associés de manière adéquate. De même, un lien structuré avec l'IPCR ⁽¹⁶⁾ devrait être créé. Cela permettra, en cas de crise, de transmettre rapidement et efficacement des informations aux décideurs politiques réunis au sein du Conseil.
- (15) La création de l'unité conjointe de cybersécurité devrait donc suivre un processus progressif et transparent, à mener à terme au cours des deux prochaines années. Les objectifs énoncés dans la présente recommandation devraient donc être atteints au moyen d'un processus en quatre étapes, tel que décrit à l'annexe de la présente recommandation. Un processus préparatoire, organisé et soutenu par l'ENISA, associant des participants ayant un rôle opérationnel et des participants ayant un rôle de soutien aux échelons de l'Union et des États membres, devrait être lancé aux deux premières étapes et être mené sous la conduite d'un groupe de travail à établir par la Commission. Les travaux préparatoires devraient être guidés par les principes d'engagement mutuel, d'inclusion et de recherche du consensus. Il convient d'encourager l'engagement de tous les participants, en permettant l'expression d'une pluralité de points de vue et positions et en s'efforçant de trouver des solutions qui recueillent le soutien le plus large possible. En fonction des besoins et à certaines conditions, le calendrier des différentes étapes indiquées dans la présente recommandation pourra être adapté.
- (16) Dans le cadre de la première étape, le processus préparatoire devrait commencer par l'identification des capacités opérationnelles de l'Union disponibles et par le lancement d'une évaluation des rôles et des responsabilités des participants au sein de la plateforme. La deuxième étape devrait inclure l'élaboration du plan de l'Union de réaction aux incidents et aux crises de cybersécurité, en cohérence avec le projet de recommandation ⁽¹⁷⁾ et le protocole de réaction d'urgence des services répressifs de l'UE, la mise en œuvre d'activités liées à la préparation et à la connaissance de la situation, en cohérence avec le règlement sur la cybersécurité et le règlement Europol ⁽¹⁸⁾, et la conclusion de l'évaluation des rôles et des responsabilités des participants au sein de la plateforme. Le groupe de travail devrait présenter les résultats de cette évaluation à la Commission et au haut représentant, qui transmettront ensuite ces résultats au Conseil. La Commission et le haut représentant devraient collaborer, dans le respect de leurs compétences respectives, afin d'élaborer un rapport conjoint sur la base de cette évaluation, et inviter le Conseil à approuver ce rapport sous la forme de conclusions du Conseil.
- (17) À la suite de cette approbation, l'unité conjointe de cybersécurité sera rendue opérationnelle, en vue de mener à bien les deux étapes restantes du processus. Dans le cadre de la troisième étape, les participants devraient être en mesure de déployer des équipes de réaction rapide de l'Union au sein de l'unité conjointe de cybersécurité, en suivant les procédures définies dans le plan de l'Union de réaction aux incidents et aux crises de cybersécurité, en tirant parti de la plateforme tant physique que virtuelle et en contribuant à divers aspects de la réaction aux incidents (depuis la communication publique jusqu'au rétablissement a posteriori). Enfin, dans le cadre de la quatrième étape, les parties prenantes du secteur privé, y compris les utilisateurs et les fournisseurs de solutions et de services de cybersécurité, seront invitées à contribuer à la plateforme, en permettant aux participants d'améliorer le partage d'informations et de renforcer la réponse coordonnée de l'Union face aux cybermenaces et incidents.

⁽¹⁴⁾ Dans ce contexte, l'unité conjointe de cybersécurité devrait établir des synergies avec le mécanisme de protection civile de l'UE (MPCU) afin d'améliorer la préparation et la réaction européennes en cas de catastrophes ou d'urgences multifformes présentant un enjeu de cybersécurité.

⁽¹⁵⁾ Notamment le cadre du secteur financier envisagé au titre du règlement (UE) 2021/xx du Parlement européen et du Conseil* [DORA].

⁽¹⁶⁾ Voir le considérant 5.

⁽¹⁷⁾ Voir la note de bas de page 3.

⁽¹⁸⁾ Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI (JO L 135 du 24.5.2016, p. 53).

- (18) À l'issue du processus en quatre étapes, les participants devraient établir un rapport d'activité sur les progrès accomplis dans la mise en œuvre des quatre étapes énoncées dans la recommandation, en indiquant les réalisations et les défis à relever, rapport qui devrait être présenté à la Commission et au haut représentant. Sur la base de ce rapport, la Commission et le haut représentant devraient effectuer une évaluation de ces résultats et tirer des conclusions pour l'avenir de l'unité conjointe de cybersécurité.
- (19) La Commission, l'ENISA, Europol et la CERT-UE devraient apporter un soutien administratif, financier et technique à l'unité conjointe de cybersécurité comme énoncé à la section IV de la présente recommandation, sous réserve des disponibilités budgétaires et humaines. Le renforcement des capacités opérationnelles de cybersécurité des institutions, organes et agences compétents de l'Union sera essentiel pour assurer une préparation efficace et la pérennité de l'unité conjointe de cybersécurité. La Commission entend veiller à ce que le règlement à venir sur des règles communes contraignantes en matière de cybersécurité applicables aux institutions, organes et agences de l'Union (octobre 2021) établisse la base juridique de cette contribution dans le cas de la CERT-UE.
- (20) Vu son mandat renforcé au titre du règlement (UE) 2019/881 (règlement sur la cybersécurité), l'ENISA se trouve dans une position privilégiée pour organiser et soutenir la préparation de l'unité conjointe de cybersécurité ainsi que pour contribuer à son entrée en service. Conformément aux dispositions du règlement sur la cybersécurité, l'ENISA met actuellement en place un bureau à Bruxelles à l'appui de sa coopération structurée avec la CERT-UE. Cette coopération structurée, qui prévoit notamment des bureaux adjacents, assure un cadre utile pour faciliter la création de l'unité conjointe de cybersécurité, notamment par la mise en place de son espace physique qui devrait être en cas de besoin mis à la disposition des participants ainsi que des institutions, organes et agences de l'Union compétents. La plateforme physique devrait être combinée à une plateforme virtuelle composée d'outils de collaboration et de partage sécurisé d'informations. Ces outils mobiliseront un vaste corpus d'informations recueillies par l'intermédiaire du cyber-bouclier européen ⁽¹⁹⁾, qui comprend les centres des opérations de sécurité (COS) et les centres d'échange et d'analyse d'informations (ISAC).
- (21) Le protocole de réaction d'urgence des services répressifs de l'UE pour les cyberattaques transfrontières majeures, adopté par le Conseil en 2018, confère un rôle central au Centre européen de lutte contre la cybercriminalité (EC3) ⁽²⁰⁾ dans le cadre du «plan d'action». Ce protocole permet aux services répressifs de l'Union, 24 h sur 24 et 7 jours sur 7, d'apporter une réponse aux attaques transfrontières majeures suspectées d'être malveillantes, grâce à une réaction et une évaluation rapides ainsi qu'au partage sécurisé et en temps utile d'informations critiques pour la coordination efficace des réactions face aux incidents transfrontières. Le protocole développe plus avant la collaboration avec les autres institutions de l'Union et les protocoles de crise à l'échelle de l'Union, ainsi que la coopération avec le secteur privé en cas de crise. Les services répressifs, avec le soutien d'Europol s'il y a lieu, devraient contribuer à l'unité conjointe de cybersécurité en prenant les mesures nécessaires tout au long du cycle d'investigation, conformément aux exigences du cadre de la justice pénale et des procédures de traitement applicables pour les preuves électroniques. Europol apporte un soutien opérationnel et facilite la coopération opérationnelle contre les cybermenaces depuis le lancement de l'EC3 en 2013. Europol devrait soutenir la plateforme conformément à son mandat et à l'approche des activités de police fondée sur le renseignement en tirant parti de tous les types d'expertise, produits, outils et services internes pertinents en réponse à l'incident ou à la crise.
- (22) La directive 2013/40/UE relative aux attaques contre les systèmes d'information impose également aux États membres de veiller à ce qu'ils disposent d'un point de contact national opérationnel disponible 24 heures par jour et sept jours par semaine aux fins de l'échange d'informations relatives aux infractions définies dans cette directive. Le réseau de points de contact nationaux opérationnels devrait également contribuer à l'unité conjointe de cybersécurité en assurant la participation des autorités répressives des États membres, le cas échéant.
- (23) La communauté de cyberdiplomatie de l'Union contribue à promouvoir et à protéger un cyberspace mondial ouvert, stable et sûr et à prévenir et décourager les actes de cybermalveillance à cet égard. En 2017, l'Union a établi un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance («boîte à outils cyberdiplomatie»). Ce cadre s'inscrit dans le contexte plus large de la politique de cyberdiplomatie de l'Union. Il contribue à la prévention des conflits et à une plus grande stabilité des relations internationales. Il permet à l'Union et aux États membres, en coopération avec les partenaires internationaux le cas échéant, à utiliser toutes les mesures relevant de la politique étrangère et de sécurité commune (PESC), conformément aux procédures respectives pour leur réalisation, à encourager la coopération, à atténuer les menaces et à influencer sur les comportements malveillants actuels et potentiels dans le cyberspace. La communauté de cyberdiplomatie devrait coopérer dans le cadre de l'unité conjointe de cybersécurité et fournir un soutien en utilisant tout l'éventail des mesures diplomatiques, notamment en ce qui concerne la communication publique et la coopération avec les pays tiers en cas de crise.

⁽¹⁹⁾ JOIN/2020/18 final, section 1.2.

⁽²⁰⁾ Institué par le règlement (UE) 2016/794.

- (24) Conformément au cadre du plan d'action, le haut représentant, y compris par l'intermédiaire de l'INTCEN, devrait contribuer à l'unité conjointe de cybersécurité en apportant une connaissance de la situation continue et partagée, fondée sur le renseignement, des menaces existantes et émergentes, y compris la nécessaire connaissance stratégique de la situation face à un événement donné.
- (25) Au sein de la communauté de cyberdéfense, l'Union et les États membres visent à renforcer les capacités de cyberdéfense et à accroître encore les synergies, la coordination et la coopération entre les institutions, organes et agences compétents de l'Union, ainsi qu'avec les États membres et entre eux, notamment en ce qui concerne les missions et opérations relevant de la politique de sécurité et de défense commune (PSDC). Le fonctionnement de cette communauté repose sur une gouvernance intergouvernementale au niveau de l'Union, sur des structures nationales de commandement militaire et sur des capacités et moyens militaires ou à double usage. Compte tenu de la nature particulière de cette communauté, les interfaces spécifiques mises en place avec l'unité conjointe de cybersécurité devraient permettre le partage d'informations avec la communauté de cyberdéfense, ⁽²¹⁾.
- (26) La coopération structurée permanente (CSP) est un cadre juridique introduit par le traité de Lisbonne ⁽²²⁾ et établi en 2017 dans le cadre de l'Union. La coopération structurée a conduit à la mise en place d'un certain nombre de projets CSP dans le domaine du cyberspace, contribuant ainsi à la réalisation de l'engagement n° 11 ⁽²³⁾ consistant à «intensifier les efforts de coopération en matière de cyberdéfense, notamment en ce qui concerne le partage d'informations, la formation et le soutien opérationnel». Le secrétariat de la CSP est assuré par le SEAE, conjointement avec l'État-major de l'Union et l'AED. Il sert de point de contact unique, dans le cadre de l'Union, pour toutes les questions relevant de la CSP, y compris les fonctions de soutien et de coordination liées aux projets CSP (par exemple, l'évaluation des nouvelles propositions de projets, la préparation des rapports d'avancement des projets, etc.). Les représentants des projets CSP pertinents devraient soutenir l'unité conjointe de cybersécurité, notamment en ce qui concerne la connaissance de la situation et l'état de préparation.
- (27) Par l'intermédiaire de l'unité conjointe de cybersécurité, les participants devraient intégrer de manière adéquate les parties prenantes du secteur privé, notamment les fournisseurs et les utilisateurs de solutions et de services de cybersécurité, afin de soutenir le cadre européen de gestion des crises en matière de cybersécurité, en tenant dûment compte du cadre juridique relatif au partage des données et à la sécurité des informations. Les fournisseurs de cybersécurité devraient contribuer à l'initiative en partageant des renseignements sur les menaces et en fournissant des analystes CERT afin d'accroître rapidement la capacité de réaction de l'unité face à des crises et attaques majeures. Les utilisateurs de biens et services de cybersécurité, principalement ceux qui relèvent du champ d'application de la directive SRI, devraient pouvoir obtenir de l'aide et des conseils par l'intermédiaire de canaux structurés, qui font actuellement défaut et qui seront liés aux centres d'échange et d'analyse d'informations (ISAC) au niveau de l'Union ⁽²⁴⁾. La plateforme pourrait également contribuer à renforcer la coopération avec les partenaires internationaux.
- (28) Pour acquérir et conserver la connaissance de la situation, il faut disposer de capacités de tout premier ordre en matière de détection et de prévention des intrusions. L'unité conjointe de cybersécurité devrait s'appuyer sur un réseau de pointe capable d'analyser les menaces et incidents malveillants susceptibles d'avoir une incidence sur les principaux systèmes de communication et d'information dans l'ensemble de l'Union. Cette unité devrait donc être alimentée, entre autres, par des connaissances sur les menaces extraites des réseaux de communication suivis par les COS nationaux, sectoriels et transfrontaliers pour permettre aux participants de mieux évaluer le paysage de la menace dans l'Union.
- (29) Afin de faciliter l'échange d'informations opérationnelles, y compris, éventuellement, de documents confidentiels, la plateforme devrait faire appel à des canaux de communication suffisamment sécurisés. Ces canaux pourraient également s'appuyer sur les infrastructures existantes, telles que l'application de réseau d'échange sécurisé d'informations (SIENA) utilisée par Europol et les services répressifs. Comme annoncé dans la stratégie de cybersécurité, les outils utilisés par les institutions, organes et agences de l'Union devraient respecter les règles en matière de sécurité de l'information que la Commission proposera prochainement.

⁽²¹⁾ Notamment par l'intermédiaire de la représentation du SEAE, afin de permettre une participation appropriée de la communauté de cyberdéfense, sur la base de contributions nationales volontaires.

⁽²²⁾ Article 42, paragraphe 6, article 46 et protocole n° 10 du TUE.

⁽²³⁾ Chacun des États membres participant à la CSP prend 20 engagements individuels, répartis sur cinq objectifs clés énoncés à l'article 2 du protocole n° 10 sur la CSP annexé au TUE.

⁽²⁴⁾ Parmi les exemples notables d'ISAC existants qui pourraient être associés à ce partage figurent le centre européen d'échange et d'analyse d'informations dans le domaine de l'énergie (EE-ISAC) ou le centre européen d'échange et d'analyse d'informations financières (FI-ISAC).

- (30) La Commission soutiendra, principalement par l'intermédiaire du programme pour une Europe numérique, les investissements nécessaires à la mise en place de la plateforme, tant dans ses composantes physique que virtuelle, à l'établissement et au maintien de canaux de communication et de capacités de formation sécurisés, ainsi qu'au développement et au déploiement de capacités de détection. En outre, le Fonds européen de la défense pourrait contribuer à financer les technologies et les capacités essentielles en matière de cyberdéfense, ce qui renforcerait la préparation nationale en matière de cyberdéfense.

A ADOPTÉ LA PRÉSENTE RECOMMANDATION:

I. OBJET DE LA PRÉSENTE RECOMMANDATION

1. La présente recommandation vise à recenser les actions nécessaires pour coordonner les efforts déployés par l'Union afin d'empêcher, de détecter, de décourager, de dissuader les incidents et crises de cybersécurité majeurs, d'en atténuer les effets et de réagir. Pour ce faire, la présente recommandation définit également le processus, les étapes et le calendrier que les États membres et les institutions, organes et agences de l'Union compétents devraient suivre en ce qui concerne la création et le développement de cette plateforme.
2. Les États membres et les institutions, organes et agences de l'Union compétents devraient veiller, en cas d'incidents et de crises de cybersécurité majeurs, à coordonner leurs efforts par l'intermédiaire d'une unité conjointe de cybersécurité fournissant une assistance mutuelle ⁽²⁵⁾ grâce à l'expertise des États membres et des institutions, organes et organismes compétents de l'Union. L'unité conjointe de cybersécurité devrait également permettre aux participants de coopérer avec le secteur privé.

II. DÉFINITIONS

3. Aux fins de la présente recommandation, on entend par:
 - a) «plan de l'UE concernant la réaction aux incidents et crises de cybersécurité», un ensemble de rôles, de modalités et de procédures conduisant à l'achèvement du cadre de l'Union européenne pour la réaction aux crises de cybersécurité décrit au point 1) de la recommandation de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs («plan d'action»);
 - b) «communautés de cybersécurité», les groupes collaboratifs de la société civile, des services répressifs, de la diplomatie et de la défense représentant à la fois les États membres et les institutions, organes et organismes compétents de l'Union, qui échangent des informations en vue de la réalisation d'objectifs, d'intérêts et de missions communs en matière de cybersécurité;
 - c) «participants du secteur privé», les représentants d'entités du secteur privé qui fournissent ou utilisent des solutions ⁽²⁶⁾ et services ⁽²⁷⁾ de cybersécurité;
 - d) «incident majeur», un incident au sens de l'article 4, paragraphe 7, de la directive (UE) 2016/1148 ayant une incidence significative dans au moins deux États membres;
 - e) «rapport intégré de l'UE sur la situation en matière de cybersécurité», un rapport rassemblant les contributions des participants à l'unité conjointe de cybersécurité, sur la base du rapport de situation technique en matière de cybersécurité de l'Union européenne défini à l'article 7, paragraphe 6, du règlement (UE) 2019/881;
 - f) «équipe de réaction rapide de l'UE en matière de cybersécurité»: une équipe composée de spécialistes de la cybersécurité reconnus, issus notamment des CSIRT des États membres, qui, avec le soutien de l'ENISA, de la CERT-UE et d'Europol, est prête à aider à distance les participants touchés par des incidents et des crises majeurs;
 - g) «protocole d'accord»: un accord entre participants exposant les modalités de coopération requises, y compris une définition des moyens et des procédures nécessaires à la mise en place et à la mobilisation des équipes de réaction rapide de l'UE en matière de cybersécurité, ainsi qu'à la fourniture d'une assistance mutuelle.

⁽²⁵⁾ Conformément à l'approche et aux principes énoncés dans la directive (UE) 2016/1148 et dans l'article 222 du TFUE. Sans préjudice de l'article 42, paragraphe 7, du traité sur l'Union européenne.

⁽²⁶⁾ Y compris les éditeurs de logiciels.

⁽²⁷⁾ Y compris le renseignement sur les menaces.

III. OBJECTIF DE L'UNITÉ CONJOINTE DE CYBERSÉCURITÉ

4. Les États membres et les institutions, organes et organismes compétents de l'Union devraient garantir une **réaction coordonnée de l'Union** en cas d'incidents ou de crises de cybersécurité majeurs, ainsi que le rétablissement des activités. En particulier, cette réaction devrait être assurée entre les participants ayant un rôle opérationnel, notamment l'ENISA, Europol, la CERT-UE, la Commission, le Service européen pour l'action extérieure (y compris l'INTCEN), le réseau des CSIRT, le réseau UE-CyCLONe, et les participants ayant un rôle de soutien, notamment le (la) président(e) du groupe de coopération SRI, le (la) président(e) du groupe horizontal «Questions liées au cyberspace» du Conseil, l'Agence européenne de défense et un représentant des projets CSP concernés ⁽²⁸⁾. Les participants ayant un rôle opérationnel devraient être en mesure de mobiliser rapidement et efficacement des ressources opérationnelles pour l'assistance mutuelle au sein de l'unité conjointe de cybersécurité. À cette fin, les mécanismes d'assistance mutuelle devraient être coordonnés au sein de l'unité conjointe de cybersécurité, en fonction de la demande d'un ou de plusieurs États membres.
5. Afin de permettre une réaction coordonnée efficace, les participants ayant un rôle opérationnel et les participants ayant un rôle de soutien mentionnés au point 4) devraient être en mesure d'échanger leurs meilleures pratiques, d'assurer une **connaissance de la situation partagée** en continu et de garantir le nécessaire **état de préparation**, dans la mesure autorisée par leurs mandats. Ces participants devraient tenir compte des processus existants et de l'expertise des différentes communautés de cybersécurité.

IV. DÉFINITION DU FONCTIONNEMENT DE L'UNITÉ CONJOINTE DE CYBERSÉCURITÉ

6. Les États membres et les institutions, organes et organismes compétents de l'Union, s'appuyant sur la contribution de l'ENISA conformément à l'article 7, paragraphe 7, du règlement (UE) 2019/881, devraient garantir une **réaction coordonnée** en cas d'incidents ou de crises de cybersécurité majeurs, ainsi que le rétablissement des activités, en assurant:
 - a) la mise en place, la formation, la mise à l'essai et le déploiement coordonné d'**équipes de réaction rapide de l'Union en matière de cybersécurité**, en tirant parti de l'article 7, paragraphe 4, du règlement (UE) 2019/881 et des articles 3 et 4 du règlement (UE) 2016/794;
 - b) le déploiement coordonné d'une **plateforme virtuelle et physique**, en tirant parti de la coopération structurée de l'ENISA et de la CERT-UE consacrée à l'article 7, paragraphe 4, du règlement (UE) 2019/881, qui devrait servir d'infrastructure de soutien à la coopération technique et opérationnelle entre les participants et rassembler le personnel compétent et d'autres ressources provenant des participants;
 - c) la création et la tenue à jour d'un inventaire des **capacités opérationnelles et techniques disponibles dans l'Union** parmi l'ensemble des communautés de cybersécurité ⁽²⁹⁾, qui sont prêtes à être déployées en cas d'incidents ou de crises de cybersécurité majeurs.
 - d) la communication de rapports à la Commission et au haut représentant sur l'expérience acquise dans le cadre des **activités de coopération opérationnelle en matière de cybersécurité** au sein des communautés de cybersécurité et entre celles-ci.
7. Les États membres et les institutions, organes et organismes compétents de l'Union devraient faire en sorte que l'unité conjointe de cybersécurité assure, entre les communautés de cybersécurité et au sein de celles-ci, une **connaissance de la situation** partagée en continu et un **état de préparation** pour faire face aux crises facilitées par les cybertechnologies, en poursuivant les objectifs énoncés à l'article 7 du règlement (UE) 2019/881 et à l'article 3 du règlement (UE) 2016/794. À cette fin, les États membres et les institutions, organes et organismes compétents de l'Union, conformément au règlement (UE) 2019/881 et au règlement (UE) 2016/794, devraient favoriser la mise en œuvre des opérations de **soutien** suivantes:
 - a) l'élaboration du **rapport de situation intégré en matière de cybersécurité de l'UE**, en recueillant et en analysant l'ensemble des informations pertinentes et des éléments du renseignement concernant les menaces;
 - b) l'utilisation d'**outils** adéquats et sécurisés, conformément à l'article 7, paragraphe 1, du règlement (UE) 2019/881, pour l'échange rapide d'informations entre les participants et avec d'autres entités;
 - c) l'**échange des informations et de l'expertise** nécessaires pour préparer l'Union à gérer les incidents et crises majeurs facilités par les cybertechnologies, avec le soutien de l'ENISA, comme prévu à l'article 7, paragraphe 2, du règlement (UE) 2019/881;
 - d) l'adoption et la mise à l'essai de **plans nationaux de réaction aux incidents et crises de cybersécurité** ⁽³⁰⁾, conformément à l'article 7, paragraphes 2, 5 et 7, du règlement (UE) 2019/881;

⁽²⁸⁾ Centre de coordination dans le domaine du cyber et de l'information (CIDCC) et «Équipes d'intervention rapide en cas d'incident informatique et assistance mutuelle dans le domaine de la cybersécurité» (CRRT).

⁽²⁹⁾ Y compris, s'il y a lieu, la communauté de cyberdéfense.

⁽³⁰⁾ Proposés en vertu de l'article 7, paragraphe 3 de la proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148, COM(2020) 823 final, 2020/0359 (COD).

- e) l'élaboration, la gestion et la mise à l'essai, y compris au moyen d'exercices et de formations intercommunautaires, du **plan de l'UE concernant la réaction aux incidents et aux crises de cybersécurité**, conformément à la recommandation «plan d'action» et en s'appuyant sur l'article 7, paragraphe 3, de la proposition de la Commission relative à une révision de la directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union ⁽³¹⁾;
 - f) l'assistance à offrir aux participants pour la conclusion d'accords d'échange d'informations, ainsi que d'accords de coopération opérationnelle avec des **entités du secteur privé** fournissant, entre autres, des services de renseignement sur les menaces et de réaction aux incidents, avec le soutien de l'ENISA, comme prévu à l'article 7, paragraphe 1, du règlement (UE) 2019/881;
 - g) la mise en place de synergies structurées avec les **capacités de surveillance et de détection** nationales, sectorielles et transfrontières, en particulier avec les centres des opérations de sécurité;
 - h) l'assistance à offrir aux participants pour la **gestion** des incidents et crises majeurs, conformément au rôle de soutien de l'ENISA tel que prévu à l'article 7 du règlement (UE) 2019/881. Il s'agit notamment de contribuer à une connaissance partagée de la situation, de soutenir l'action diplomatique, l'imputation de la responsabilité politique ainsi que l'imputation de responsabilités dans le contexte d'enquêtes pénales, y compris par l'intermédiaire d'Europol ⁽³²⁾, d'harmoniser la communication publique et de faciliter le rétablissement des activités après un incident.
8. Afin de mettre en œuvre les points 6) et 7), les États membres et les institutions, organes et organismes compétents de l'Union devraient prévoir:
- a) la définition des aspects organisationnels de l'unité conjointe de cybersécurité, ainsi que les **rôles et responsabilités** des participants ayant un rôle opérationnel et des participants ayant un rôle de soutien au sein de la plateforme, permettant le bon fonctionnement de la plateforme dans le respect des éléments et principes énoncés à l'annexe de la présente recommandation;
 - b) la conclusion de **protocoles d'accord** fixant les nécessaires modalités de la coopération entre les participants mentionnés au point 4).
9. Conformément à l'article 7 du règlement (UE) 2019/881, l'ENISA devrait assurer la coordination entre les États membres et les institutions, organes et organismes compétents de l'Union, ainsi que le soutien de ceux-ci, au sein de l'unité conjointe de cybersécurité, notamment en faisant office de secrétariat, en organisant les réunions et en contribuant à la mise en œuvre des actions au niveau des États membres et au niveau de l'Union. L'ENISA devrait mettre en place à la fois une plateforme virtuelle sécurisée et un espace physique pour accueillir les réunions et faciliter les actions de mise en œuvre nécessaires.

V. CRÉATION DE L'UNITÉ CONJOINTE DE CYBERSÉCURITÉ

10. Les États membres et les institutions, organes et organismes compétents de l'Union devraient veiller à ce que l'unité conjointe de cybersécurité entre dans sa phase opérationnelle à compter du **30 juin 2022**. D'ici là, les participants ayant un rôle opérationnel devraient mettre à disposition des capacités opérationnelles et des experts susceptibles de constituer la base des équipes de réaction rapide de l'Union en matière de cybersécurité. Les plans relatifs à la plateforme physique et virtuelle devraient être bien avancés.
11. Les États membres et les institutions, organes et organismes compétents de l'Union devraient contribuer au fonctionnement de l'unité conjointe de cybersécurité et veiller à ce que sa mise en œuvre soit pleinement achevée le **30 juin 2023**. Pour ce faire, il convient de suivre quatre étapes successives, qui viseront à mener à bien les activités suivantes:
- a) Étape 1 — Analyser les aspects organisationnels de l'unité conjointe de cybersécurité et recenser les capacités opérationnelles de l'Union disponibles au plus tard le **31 décembre 2021**;
 - b) Étape 2 — Préparer les plans de réaction aux incidents et aux crises et déployer les activités conjointes de préparation au plus tard le **30 juin 2022**;
 - c) Étape 3 — Rendre l'unité conjointe de cybersécurité opérationnelle au plus tard le **31 décembre 2022**;
 - d) Étape 4 — Étendre la coopération au sein de l'unité conjointe de cybersécurité aux entités du secteur privé et rendre compte des progrès accomplis au plus tard le **30 juin 2023**.

Des actions plus détaillées à entreprendre dans le cadre des quatre étapes successives sont exposées dans l'annexe de la présente recommandation.

⁽³¹⁾ COM(2020) 823 final.

⁽³²⁾ Conformément au règlement (UE) 2016/794.

12. Dans le cadre des deux premières étapes, l'ENISA devrait organiser et soutenir la préparation de l'unité conjointe de cybersécurité. Les services de la Commission devraient mettre sur pied un groupe de travail rassemblant les participants ayant un rôle opérationnel et les participants ayant un rôle de soutien pour mener à bien ce travail préparatoire. Les services de la Commission devraient nommer un représentant en tant que coprésident du groupe de travail et devraient inviter à exercer les fonctions de coprésident un représentant désigné par le haut représentant, chacun contribuant aux points de l'ordre du jour conformément à leurs compétences respectives, et un représentant choisi par les États membres.
13. À la fin de l'étape 2, le groupe de travail devrait conclure son analyse des aspects organisationnels de l'unité conjointe de cybersécurité et des rôles et responsabilités des participants ayant un rôle opérationnel au sein de cette plateforme. Le groupe de travail devrait présenter les résultats de son analyse à la Commission et au haut représentant. La Commission et le haut représentant devraient ensuite partager cette analyse avec le Conseil. La Commission et le haut représentant devraient élaborer un rapport conjoint sur la base de cette analyse et inviter le Conseil à approuver ce rapport sous la forme de conclusions du Conseil.
14. L'unité conjointe de cybersécurité devrait être opérationnelle à partir de l'étape 3.
15. L'ENISA et la Commission devraient veiller à l'utilisation des ressources disponibles dans le cadre des programmes de financement de l'Union, principalement le programme pour une Europe numérique, conformément aux règles applicables concernant l'établissement des programmes de travail respectifs, pour doter les participants à l'unité conjointe de cybersécurité de capacités supplémentaires en matière de formation, de communication et d'infrastructures sécurisées de partage d'informations permettant l'échange d'informations classifiées, y compris entre les communautés.

VI. RÉEXAMEN

16. Les États membres devraient coopérer avec la Commission et le haut représentant, dans le respect de leurs compétences respectives, afin d'évaluer l'efficacité et l'efficacité de l'unité conjointe de cybersécurité au plus tard le **30 juin 2025**, en vue de tirer des conclusions concernant l'avenir de cette unité conjointe. Cette évaluation devrait tenir compte de la mise en œuvre des quatre étapes susmentionnées.

Fait à Bruxelles, le 23 juin 2021.

Par la Commission
Thierry BRETON
Membre de la Commission

ANNEXE

Étapes en vue de la création de l'unité conjointe de cybersécurité

La présente annexe décrit plus en détail les actions clés et les actions de soutien nécessaires pour mettre en place l'unité conjointe de cybersécurité et la rendre opérationnelle.

1. *Étape 1 — Analyse des aspects organisationnels de l'unité conjointe de cybersécurité et recensement des capacités opérationnelles de l'Union disponibles*

ACTIONS CLÉS

Les participants ayant un rôle opérationnel à l'unité conjointe de cybersécurité, réunis au sein d'un groupe de travail mis en place par la Commission et assistés par l'ENISA, devraient recueillir des informations sur les capacités opérationnelles existantes, et notamment dresser une liste des professionnels reconnus disponibles avec une indication de leur expertise pertinente, des outils, fonctions et actifs disponibles pour gérer les incidents, des portefeuilles de formations et d'exercices disponibles et des produits d'analyse d'informations et de renseignement existants. Sur la base de ces informations, les participants ayant un rôle opérationnel devraient établir **une liste des capacités opérationnelles de l'Union disponibles** et prêtes à être déployées en cas d'incidents ou de crises de cybersécurité, notamment par l'intermédiaire d'équipes de réaction rapide de l'Union en matière de cybersécurité.

Le groupe de travail devrait lancer une analyse des **aspects organisationnels** de l'unité conjointe de cybersécurité **et des rôles et responsabilités des participants ayant un rôle opérationnel au sein de cette plateforme**.

Afin d'obtenir une vue d'ensemble des capacités et de convenir des procédures, les actions clés et, dans la mesure du possible, les actions de soutien menées dans le cadre de l'étape 1 devraient être achevées le **31 décembre 2021 au plus tard [6 mois après l'adoption]**.

2. *Étape 2 — Préparation des plans de réaction aux incidents et aux crises et déploiement d'activités conjointes de préparation*

ACTIONS CLÉS

Les participants ayant un rôle opérationnel réunis au sein du groupe de travail, en concertation avec les participants ayant un rôle de soutien, devraient élaborer le **plan de l'UE concernant la réaction aux incidents et aux crises de cybersécurité** sur la base des plans nationaux de réaction aux incidents et aux crises de cybersécurité. Le plan de l'UE concernant la réaction aux incidents et aux crises de cybersécurité devrait inclure des objectifs en matière de préparation de l'Union, des procédures déterminées et des canaux d'échange d'informations sécurisés, y compris les modalités de traitement des informations, ainsi que des critères d'activation du mécanisme d'assistance mutuelle sur la base d'une classification des incidents (taxonomie) convenue et de la liste des capacités de l'Union disponibles.

À la fin de l'étape 2, le groupe de travail devrait conclure son analyse des aspects organisationnels de l'unité conjointe de cybersécurité et des rôles et responsabilités des participants ayant un rôle opérationnel au sein de cette plateforme. Le groupe de travail devrait présenter les résultats de son analyse à la Commission et au haut représentant. La Commission et le haut représentant devraient partager cette analyse avec le Conseil. La Commission et le haut représentant devraient collaborer, dans le respect de leurs compétences respectives, afin d'élaborer un rapport conjoint sur la base de cette analyse et inviter le Conseil à approuver ce rapport sous la forme de conclusions du Conseil.

ACTIONS DE SOUTIEN

Le plan de l'UE concernant la réaction aux incidents et aux crises de cybersécurité devrait s'appuyer sur les principaux éléments des plans nationaux de réaction aux incidents et aux crises de cybersécurité. Conformément à la proposition de la Commission de directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148 ⁽¹⁾, chaque État membre devrait adopter un plan national de réaction aux incidents et aux crises de cybersécurité. Les plans nationaux, qui peuvent éventuellement faire l'objet d'un examen par les pairs, devraient définir des objectifs et des modalités pour la gestion des incidents et des crises de cybersécurité majeurs. Les plans nationaux devraient aborder, en particulier, les points suivants:

- a) les objectifs des mesures et activités nationales de préparation;
- b) les rôles et responsabilités des autorités nationales compétentes au niveau national;
- c) les procédures de gestion de crise et les canaux d'échange d'informations au niveau national;
- d) le recensement des mesures de préparation, y compris les exercices et les activités de formation;
- e) l'identification des infrastructures et parties prenantes des secteurs public et privé impliquées;
- f) les procédures et modalités nationales entre les autorités et organismes nationaux compétents, y compris ceux qui sont responsables de toutes les cybercommunautés, pour garantir, d'une part, la participation effective des États membres à la gestion coordonnée des incidents et des crises de cybersécurité majeurs au niveau de l'Union et, d'autre part, leur soutien à cette gestion.

Sur la base des contributions fournies par les États membres et les institutions, organes et agences de l'Union, les participants ayant un rôle opérationnel devraient exécuter les actions de soutien suivantes dans le cadre de l'unité conjointe de cybersécurité:

- a) établir le premier rapport intégré de situation de l'Union en s'appuyant sur les plans nationaux de réaction aux incidents et aux crises de cybersécurité;

⁽¹⁾ COM(2020) 823 final, 2020/0359 (COD), Bruxelles, le 16.12.2020.

- b) mettre en place des capacités de communication et des outils sécurisés de partage d'informations;
- c) faciliter l'adoption de protocoles relatifs à l'assistance mutuelle parmi les participants;
- d) organiser des exercices et des formations intercommunautaires pour les experts figurant sur la liste des capacités opérationnelles de l'Union disponibles;
- e) élaborer un plan pluriannuel de coordination des exercices.

Le cas échéant, les participants ayant un rôle opérationnel devraient consulter les participants ayant un rôle de soutien. L'ENISA, avec le soutien de la Commission, d'Europol et de la CERT-UE, devrait permettre le partage d'informations en mettant en place des capacités de communication et des outils sécurisés de partage d'informations.

Afin de garantir que les plans nécessaires sont élaborés et que les activités conjointes commencent à être déployées, les actions clés et, dans la mesure du possible, les actions de soutien menées dans le cadre de l'étape 2 devraient être achevées le **30 juin 2022 au plus tard [6 mois après la fin de l'étape 1]**.

3. Étape 3 — *Rendre l'unité conjointe de cybersécurité opérationnelle*

ACTIONS CLÉS

Après l'approbation par le Conseil des conclusions de la Commission sur le rapport élaboré dans le cadre de l'étape 2, les participants ayant un rôle opérationnel devraient coordonner le déploiement d'**équipes de réaction rapide de l'Union en matière de cybersécurité** au sein de l'unité conjointe de cybersécurité et mettre en place une **plateforme physique** permettant aux équipes de mener des activités techniques et opérationnelles. Sur la base des travaux préparatoires réalisés dans le cadre de l'étape 2, les participants devraient finaliser le plan de l'UE concernant la réaction aux incidents et aux crises de cybersécurité. Les participants ayant un rôle opérationnel devraient veiller à ce que les experts et les capacités figurant sur la liste des capacités opérationnelles de l'Union disponibles soient prêts à contribuer aux activités des équipes de réaction rapide de l'Union en matière de cybersécurité.

Afin de mettre en œuvre le plan de l'UE concernant la réaction aux incidents et aux crises de cybersécurité, les participants devraient établir un programme de travail annuel.

ACTIONS DE SOUTIEN

La communauté de cyberdiplomatie peut s'appuyer sur l'unité conjointe de cybersécurité pour coordonner les actions de communication publique. La plateforme peut permettre aux participants de contribuer à l'imputation de la responsabilité politique ainsi qu'à l'imputation de responsabilités au titre du cadre de la justice pénale utilisé par les services de police et judiciaires. Elle peut en outre faciliter la relance et permettre des synergies structurées avec les capacités nationales et transfrontières de surveillance et de détection.

Afin de rendre l'unité conjointe de cybersécurité opérationnelle, les actions clés et, dans la mesure du possible, les actions de soutien menées dans le cadre de l'étape 3 devraient être achevées le **31 décembre 2022 au plus tard [6 mois après la fin de l'étape 2]**.

4. Étape 4 — *Étendre la coopération au sein de l'unité conjointe de cybersécurité aux entités du secteur privé et rendre compte des progrès accomplis*

ACTION CLÉ

Les participants à l'unité conjointe de cybersécurité devraient élaborer **un rapport d'activité sur les progrès accomplis dans la mise en œuvre des quatre étapes énoncées dans la recommandation, qui décrit les réalisations et les défis rencontrés**. Ce rapport devrait inclure des informations statistiques sur les activités de coopération opérationnelle menées tout au long des quatre étapes. Le rapport devrait être présenté à la Commission et au haut représentant.

ACTIONS DE SOUTIEN

Afin d'étendre les capacités et les informations dont disposent les équipes de réaction rapide de l'Union en matière de cybersécurité, les participants devraient veiller à ce que l'unité conjointe de cybersécurité contribue à la conclusion **d'accords de partage d'informations et de coopération opérationnelle entre les participants et les entités du secteur privé** fournissant, entre autres, des services de renseignement sur les menaces et de réaction aux incidents. Ils devraient également veiller, entre autres, à ce que l'unité conjointe de cybersécurité encourage un dialogue régulier et des activités de partage d'informations sur les menaces et les vulnérabilités avec les utilisateurs de solutions de cybersécurité, principalement celles relevant du champ d'application de la directive SRI ou recueillies par les **centres d'échange et d'analyse d'informations (ISAC) au niveau de l'Union**.

Les États membres devraient aider les entités actives sur leur territoire, en particulier celles relevant du champ d'application de la directive SRI, à avoir accès aux dialogues entre les secteurs public et privé et les ISAC au niveau de l'Union, et à y contribuer.

Afin de garantir une participation adéquate du secteur privé, les actions clés et, dans la mesure du possible, les actions de soutien menées dans le cadre de l'étape 4 devraient être achevées le **30 juin 2023 au plus tard [6 mois après la fin de l'étape 3]**.

COMMENT MOBILISER RAPIDEMENT LES CAPACITÉS OPÉRATIONNELLES DE L'UNION?

QUI MET À DISPOSITION LES CAPACITÉS: Participants ayant un rôle opérationnel

QUI GÈRE LES CAPACITÉS: Participants, au sein de l'unité conjointe de cybersécurité, conformément aux rôles et responsabilités convenus

Étape	Objectif	Tâche	Action clé	Action de soutien
Étape 1 — Recenser 31 décembre 2021 au plus tard [6 mois après l'adoption]	PRÉPARATION	Recenser les capacités	Les participants ayant un rôle opérationnel établissent une liste des capacités opérationnelles de l'Union disponibles.	
Étape 2 — Préparer 30 juin 2022 au plus tard [6 mois après la fin de l'étape 1]	PRÉPARATION	Définir des procédures et modalités pertinentes pour activer les capacités en cas de besoin	Les participants ayant un rôle opérationnel élaborent le plan de l'UE concernant la réaction aux incidents et aux crises de cybersécurité (cadre de l'UE pour la réaction aux crises de cybersécurité en vertu du plan d'action) sur la base des plans nationaux adoptés.	Les participants ayant un rôle opérationnel élaborent des rapports intégrés de situation en matière de cybersécurité de l'Union sur la base du rapport de situation technique en matière de cybersécurité de l'Union.
	PRÉPARATION	Capacités en matière d'exercices		Les participants organisent des exercices et formations conjoints (intercommunautaires). Les participants travaillent sur un plan pluriannuel de coordination des exercices.
	CONNAISSANCE DE LA SITUATION	Mettre en place des outils pour partager les informations et les demandes de soutien		Les participants mettent en place un partage d'informations sécurisé et rapide
L'UCC EST OPÉRATIONNELLE Sur la base des travaux préparatoires menés par les participants dans le cadre d'un groupe de travail que la Commission mettra en place				
Étape 3 — Déployer 31 décembre 2022 au plus tard [6 mois après la fin de l'étape 2]	PRÉPARATION	Adopter des procédures, modalités et protocoles d'accord pertinents pour activer les capacités en cas de besoin	Les participants ayant un rôle opérationnel finalisent le plan de l'UE concernant la réaction aux incidents et aux crises de cybersécurité et déterminent sa mise en œuvre au moyen de programmes de travail annuels.	Les participants soutiennent la mise en place de capacités nationales et transfrontières de surveillance et de détection, y compris la mise en place des COS
	RÉACTION COORDONNÉE	Déployer des capacités en cas de besoin	Les participants ayant un rôle opérationnel coordonnent les équipes opérationnelles de réaction rapide de l'Union en matière de cybersécurité par l'intermédiaire de la plateforme virtuelle et physique de l'UCC à Bruxelles.	Les participants coordonnent les actions de communication publique et contribuent à l'imputation de la responsabilité politique ainsi qu'à l'imputation de responsabilités dans le cadre de la justice pénale

<p>Étape 4 — Étendre et rendre compte</p> <p>30 juin 2023 au plus tard [6 mois après la fin de l'étape 3]</p>	<p>CONNAISSANCE DE LA SITUATION</p>	<p>Garantir l'évolutivité en associant le secteur privé afin de répondre aux besoins émergents</p>	<p>Les participants présentent un rapport d'activité sur les progrès accomplis, qui décrit les réalisations et les défis rencontrés et qui s'appuie sur des informations statistiques.</p>	<p>Les participants concluent des accords de partage d'informations, ainsi que des accords de coopération opérationnelle avec des fournisseurs de services de cybersécurité.</p>
	<p>RÉACTION COORDONNÉE</p>			<p>Les participants concluent des accords de partage d'informations avec des utilisateurs de services de cybersécurité, principalement des entités relevant du champ d'application de la directive SRI et les ISAC au niveau de l'Union.</p>