Conseil de
l'Union européenne

Bruxelles, le 6 décembre 2024
(OR. en)

16527/24

CYBER 360
TELECOM 369
COSI 231
COPEN 535
CSDP/PSDC 854
DATAPROTECT 347
RECH 534
HYBRID 146
IPCR 72
JAI 1814
RELEX 1549
POLMIL 420

RÉSULTATS DES TRAVAUX

Origine:	Secrétariat général du Conseil
Destinataire:	délégations
Objet:	Conclusions du Conseil sur l'ENISA

Les délégations trouveront en annexe les conclusions du Conseil sur l'ENISA, approuvées par le Conseil lors de sa session tenue le 6 décembre 2024.

ANNEXE

Projet de conclusions du Conseil sur l'ENISA

LE CONSEIL DE L'UNION EUROPÉENNE,

1. SOULIGNE que les défis découlant du cyberespace mondial n'ont jamais été aussi complexes, diversifiés et graves qu'ils le sont aujourd'hui, en raison de la sophistication des cybermenaces qui se font jour, de l'évolution constante de l'environnement de sécurité et des tensions géopolitiques actuelles. Par conséquent, l'UE et ses États membres devraient poursuivre leurs efforts pour devenir plus résilients en vue de recenser et de relever efficacement les menaces et les défis actuels et émergents. INSISTE sur le fait que les travaux visant à accroître le niveau de cyberrésilience devraient se poursuivre selon une approche englobant l'ensemble de la société. SOULIGNE que, dans les années à venir, l'UE et ses États membres devraient se concentrer sur la bonne mise en œuvre d'initiatives législatives et non législatives qui sous-tendent toutes les mesures prises jusqu'à présent à cet égard et y contribuent.

2. RAPPELANT que la sécurité nationale reste du seul ressort de chaque État membre, PREND ACTE de ce que l'UE et ses États membres ont considérablement œuvré de concert ces dernières années à la mise en place du cadre institutionnel et des formes de collaboration nécessaires, tant au niveau national qu'au niveau de l'UE, dans le cyberdomaine. SALUE les diverses initiatives législatives et non législatives qui ont permis à l'UE et à ses États membres de se doter d'un cadre solide et robuste dans ce domaine, renforçant ainsi la cyberrésilience globale de l'Union. Ce cadre a évolué pour couvrir plusieurs aspects du cyberdomaine: la sécurité, la diplomatie, l'application de la loi et la défense. RELÈVE qu'un grand nombre d'acteurs, dont les autorités des États membres chargées de la cybersécurité, le groupe de coopération SRI, le réseau européen d'organisations de liaison en cas de crises de cybersécurité (UE-CyCLONe), le réseau de centres nationaux de coordination, le groupe européen de certification de cybersécurité (GECC), la Commission, le Service européen pour l'action extérieure (SEAE), l'Agence de l'Union européenne pour la cybersécurité (ENISA), le Centre de compétences européen en matière de cybersécurité, le CERT-UE, l'Agence européenne de défense (AED) et le Centre européen de lutte contre la cybercriminalité (EC3) d'Europol, font partie de l'écosystème de la cybersécurité de l'UE, chacun participant à la mise en œuvre du cadre de cybersécurité à l'échelle de l'Union.

3. CONSIDÈRE qu'au cours des vingt dernières années, l'ENISA s'est révélée être une entité extrêmement utile dans l'écosystème européen de cybersécurité, jouant un rôle crucial pour ce qui est de soutenir activement les États membres et les institutions, organes et organismes de l'UE dans l'élaboration et la mise en œuvre de politiques en matière de cybersécurité, dans le renforcement de leurs capacités et leur préparation, dans leur coopération ainsi que dans leur promotion de la sensibilisation et de la certification en matière de cybersécurité.

RECOMMANDATIONS GÉNÉRALES

4. INVITE la Commission à mettre à profit **l'évaluation du règlement sur la cybersécurité** pour voir comment en tirer parti pour simplifier l'écosystème complexe de la cybersécurité, de manière à renforcer l'efficacité et la bonne utilisation des ressources. Par conséquent, INVITE la Commission à veiller à ce que le mandat de l'ENISA visant à soutenir les États membres et les institutions, organes et organismes de l'Union soit ciblé et clairement défini, et assorti d'objectifs stratégiques concrets et de tâches hiérarchisées, en plus d'une répartition plus précise des tâches et des compétences par rapport aux autres acteurs. À cet égard, INVITE la Commission à examiner et renforcer encore le rôle de l'ENISA pour ce qui est de soutenir la coopération opérationnelle menée au niveau de l'UE et entre les États membres pour renforcer la cyberrésilience, en tenant compte des compétences des États membres dans ce domaine. En outre, INVITE la Commission à renforcer le rôle consultatif joué par l'ENISA pour ce qui est de fournir des orientations et des recommandations spécialisées et fondées sur des données probantes, en ce qui concerne la mise en œuvre des initiatives législatives et non législatives actuelles et futures de l'Union, tout en garantissant un cadre cohérent de l'UE en matière de cybersécurité.

5. Dans le même esprit, ENCOURAGE la Commission à envisager de rationaliser le rôle de l'ENISA en ce qui concerne les tâches qui ne sont pas au cœur de sa mission. MET EN AVANT le fait que **les responsabilités** de l'ENISA **ont été considérablement élargies** par des initiatives législatives récentes, notamment la directive SRI 2, le règlement sur la cyberrésilience et le règlement sur la cybersolidarité. Tout en NOTANT que l'ENISA a reçu des ressources supplémentaires à la suite de certaines de ces initiatives, SOULIGNE que l'élargissement des responsabilités de l'Agence et la complexité croissante des menaces et des défis dans le cyberdomaine ont donné lieu à une augmentation considérable de ses tâches, qui devrait se traduire par des **ressources adéquates** – humaines, financières et techniques – afin de permettre pleinement à l'ENISA d'exécuter toutes les tâches relevant de sa compétence, sans préjuger de la négociation du cadre financier pluriannuel. À cette fin, INVITE la Commission à hiérarchiser les mesures et à accorder la priorité aux tâches visant à aider les États membres à renforcer leur cyberrésilience, leur coopération opérationnelle ainsi que l'élaboration et la mise en œuvre du droit de l'Union lors de l'élaboration du projet de budget général de l'Union.

SOUTIEN DE L'ENISA À L'ÉLABORATION ET À LA MISE EN ŒUVRE DES POLITIQUES

6. RAPPELLE qu'en vertu du cadre juridique actuel en matière de cybersécurité, l'ENISA a plusieurs responsabilités essentielles en matière de soutien et de conseil dans l'ensemble de l'Union. SE FÉLICITE du rôle joué à cet égard par l'ENISA pour ce qui est de prêter **assistance aux États membres** en ce qui concerne la bonne mise en œuvre d'initiatives législatives et non législatives. INVITE l'ENISA, en étroite coopération avec le groupe de coopération SRI et la Commission, à continuer de fournir des informations et des analyses générales sur l'environnement juridique actuel en matière de cybersécurité. ENCOURAGE l'ENISA à partager et à promouvoir activement les orientations techniques et les bonnes pratiques de manière régulière et structurée pour aider les États membres à mettre en œuvre la politique et la législation en matière de cybersécurité.

7. RECONNAÎT le rôle essentiel joué par l'ENISA dans l'élaboration de **schémas européens de certification de cybersécurité**, qui sous-tendent la confiance placée dans les produits, services et processus TIC, et les services de sécurité gérés, à la lumière de la modification ciblée qui doit être apportée prochainement au règlement sur la cybersécurité. SOULIGNE que les États membres et l'industrie sont préoccupés par la longueur du processus de sélection, d'élaboration et d'adoption des schémas de certification de cybersécurité; par conséquent, INVITE INSTAMMENT la Commission à saisir l'occasion qu'offre l'évaluation du règlement sur la cybersécurité pour trouver des moyens d'adopter une approche plus souple, plus transparente, plus rapide et fondée sur les risques pour l'élaboration de schémas de certification de cybersécurité de l'UE, tout en SOULIGNANT le rôle important que jouent les États membres dans le processus. Par ailleurs, INSISTE sur le fait qu'il importe d'attribuer explicitement la responsabilité de la maintenance de chaque schéma de certification. En outre, RAPPELLE que l'ENISA devrait consulter en temps utile toutes les parties prenantes concernées au moyen d'un processus formel, ouvert, transparent et inclusif lors de l'élaboration de schémas candidats et que la Commission devrait procéder à des consultations ouvertes, transparentes et inclusives lors de l'évaluation de l'efficacité et de l'utilisation des schémas adoptés. ENCOURAGE l'ENISA à renforcer encore la collaboration avec la communauté de la protection des données, en particulier le comité européen de la protection des données, le cas échéant, et les autorités nationales compétentes, en accordant une attention particulière à la promotion des synergies dans le cadre de l'élaboration de futurs schémas européens de certification de cybersécurité.

8. Afin d'éviter la charge administrative inutile qui pourrait résulter d'un cadre complexe en matière de communication d'informations, INVITE l'ENISA, en coopération avec la Commission, à poursuivre les échanges avec les États membres sur les modalités pratiques, la simplification et la rationalisation de la procédure de communication d'informations. RAPPELLE, en outre, avoir invité la Commission à élaborer, avec le soutien de l'ENISA et d'autres entités concernées de l'UE, une cartographie des obligations pertinentes en matière de communication d'informations énoncées dans les différents actes législatifs de l'UE concernant le cyberdomaine et le numérique. RAPPELLE que l'échange d'informations entre l'ENISA et les États membres repose sur une relation de confiance, dans le cadre de laquelle la sécurité et la confidentialité sont garanties conformément au règlement sur la cybersécurité et aux règles et protocoles pertinents et devraient être limitées à ce qui est nécessaire et proportionné à la finalité de l'échange. INSISTE sur la nécessité de traiter les données et les informations avec toute la diligence requise.

9. SOULIGNE que l'ENISA est responsable de la mise en place et du maintien de **la plateforme unique de communication d'informations au titre du règlement sur la cyberrésilience**, qui aura une valeur ajoutée opérationnelle concrète, en particulier pour les vulnérabilités activement exploitées et les incidents graves ayant une incidence sur la sécurité des produits comportant des éléments numériques. Compte tenu du large champ d'application de cette législation horizontale, la plateforme unique de communication d'informations devrait être un outil efficace et sécurisé pour faciliter le partage d'informations entre les CSIRT nationaux et l'ENISA. Par conséquent, DEMANDE INSTAMMENT à l'ENISA, en plus d'allouer des ressources humaines suffisantes, d'accélérer la mise en place de la plateforme en tant que priorité absolue afin qu'elle puisse être prête dans le délai fixé dans le règlement sur la cyberrésilience.

10. EST CONSCIENT du rôle de l'ENISA dans la création d'une **base de données européenne sur les vulnérabilités**, qui vise à améliorer la transparence en ce qui concerne la divulgation des vulnérabilités, tout en garantissant le traitement approprié des données sensibles. Compte tenu de l'expiration du délai de transposition de la directive SRI 2, INVITE INSTAMMENT l'ENISA à redoubler d'efforts partout où cela est nécessaire pour assurer le bon fonctionnement de cette base de données. INVITE parallèlement le groupe de coopération SRI, avec l'aide de l'ENISA, à mieux faire connaître les orientations, les politiques et les procédures relatives à la divulgation des vulnérabilités.

11. MESURE les avantages de l'**action de soutien à la cybersécurité** menée par l'ENISA, qui fonctionne comme un ensemble de services de cybersécurité mis à la disposition des États membres pour compléter leurs efforts, ainsi que l'expérience acquise par l'ENISA dans sa mise en œuvre. À cet égard, SOULIGNE que l'ENISA devrait jouer un rôle central dans l'administration et le fonctionnement de la réserve de cybersécurité de l'UE. INVITE l'ENISA à commencer de répertorier les services nécessaires et leur disponibilité dès l'entrée en vigueur du règlement sur la cybersolidarité, afin de faire en sorte que la réserve de cybersécurité de l'UE soit aussi utile et adaptée aux besoins des utilisateurs que possible dans tous les États membres. INVITE l'ENISA, une fois que cette mission lui aura été confiée, à associer les États membres, notamment en recueillant des contributions sur les critères requis et en fournissant des informations sur les appels d'offres à venir, à un stade précoce du processus de mise en place de la réserve de cybersécurité de l'UE. INVITE l'ENISA, une fois que cette mission lui aura été confiée, à veiller à ce que le processus de sélection des fournisseurs de confiance de services de sécurité gérés soit transparent, ouvert et équitable et permette la participation de fournisseurs de tous les États membres, quelle que soit leur taille. En outre, RAPPELLE que l'ENISA est tenue de publier dans les meilleurs délais les lignes directrices en matière d'interopérabilité pour les cyberpôles transfrontières.

12. Souligne qu'il est essentiel de **suivre les tendances concernant les technologies émergentes** dans un domaine en évolution rapide comme le domaine cyber afin de maintenir et renforcer encore notre posture cyber. EST CONSCIENT du travail accompli par l'ENISA pour attirer l'attention du public sur les risques et les possibilités que représentent des technologies telles que l'intelligence artificielle et l'informatique quantique, facilitant ainsi une meilleure compréhension des défis actuels. ENCOURAGE l'ENISA à contribuer davantage à ces tâches, à préconiser activement la mise en œuvre de ses recommandations, ainsi qu'à conseiller le Centre de compétences européen en matière de cybersécurité et à collaborer avec lui, le cas échéant.

SOUTIEN DE L'ENISA AUX ÉTATS MEMBRES POUR RENFORCER LA CYBERRÉSILIENCE ET LA COOPÉRATION OPÉRATIONNELLE

13. SOULIGNE que l'ENISA joue un rôle important en tant que **secrétariat des deux réseaux de cybercoopération au niveau de l'UE pilotés par les États membres que sont le réseau des CSIRT et le réseau UE-CyCLONe.** INSISTE SUR la précieuse participation de l'ENISA au groupe de coordination SRI, notamment par son engagement actif et ses contributions techniques aux différents axes de travail. ENCOURAGE l'ENISA à continuer à l'avenir de soutenir le fonctionnement et la coopération de ces réseaux, étant donné qu'ils fournissent aux États membres des canaux déterminants de collaboration à différents niveaux.

14. RÉAFFIRME la nécessité d'améliorer l'**appréciation commune de la situation** au niveau de l'UE, qui contribue à la posture cyber de l'UE, en ce qui concerne la détection et la prévention des incidents de cybersécurité et la réponse qui y est apportée. SOULIGNE à cet égard l'importance des activités de prospective, des rapports réguliers et des évaluations de la menace réalisés par l'ENISA, qui contribuent tous à améliorer l'appréciation de la situation. ENCOURAGE l'ENISA à travailler en étroite coopération avec les États membres afin de contribuer à développer l'appréciation de la situation au niveau de l'UE. Dans ce contexte, MESURE le rôle important joué par l'ENISA, en collaboration avec le CERT-UE et Europol, dans le soutien apporté au Conseil au moyen de notes d'information sur la situation dans le cadre de la boîte à outils cyberdiplomatique complétant l'appréciation de la situation fournie par la capacité unique d'analyse du renseignement (SIAC), et SOULIGNE la nécessité de dresser un tableau complet des menaces émanant de différentes sources, y compris le secteur privé. ENCOURAGE à cet égard un développement accru de la coopération de l'ENISA avec le SEAE, et en particulier avec l'INTCEN, dans le plein respect de leurs mandats respectifs.

15. SOULIGNE que le centre d'analyse et de situation de la Commission en matière de cybersécurité remplit une fonction interne au sein de la Commission et est soutenu par sa collaboration avec l'ENISA et le CERT-UE. Afin de créer un potentiel de synergies maximum et de réduire la complexité au sein de l'écosystème de cybersécurité de l'UE, INVITE la Commission à tenir compte des résultats de l'évaluation du règlement sur la cybersécurité ainsi que des discussions sur l'évaluation du plan d'action pour la cybersécurité afin de rationaliser les tâches du centre d'analyse et de situation de la Commission en matière de cybersécurité et les tâches de l'ENISA qui y sont liées. INCITE la Commission à éviter toute duplication inutile des tâches, tout en préservant le rôle central de l'ENISA de par sa contribution au développement d'une appréciation commune de la situation au niveau de l'Union, en soutien aux États membres, dans le respect de leurs compétences nationales.

16. INSISTE SUR le fait qu'élaborer une appréciation commune de la situation est une condition préalable à une gestion rapide et efficace des crises dans l'ensemble de l'Union. PRÉCISE que, au niveau de l'Union, divers acteurs clés participent à la **réponse apportée aux incidents de cybersécurité de grande ampleur** et que, lorsque de tels incidents se produisent, la coopération efficace entre les États membres repose principalement sur le réseau des CSIRT et sur UE-CyCLONe. L'ENISA joue un rôle important dans la gestion des crises de cybersécurité en tant que secrétariat du réseau des CSIRT et d'UE-CyCLONe. INVITE la Commission à utiliser l'évaluation du plan d'action pour la cybersécurité pour tenir dûment compte des tâches et responsabilités supplémentaires en termes de contribution à l'élaboration d'une réponse concertée aux incidents ou aux crises de cybersécurité transfrontières de grande ampleur, ainsi que du rôle confié à l'ENISA en tant que secrétariat du réseau CSIRT et d'UE-CyCLONe et par la législation récente en matière de cybersécurité.

17. SOULIGNE qu'il importe d'organiser régulièrement des **exercices de cybersécurité** qui renforcent considérablement la préparation de l'UE à réagir aux incidents et aux crises. EST CONSCIENT que l'ENISA a acquis dans ce domaine une expérience précieuse et étendue en soutien aux États membres. MESURE le rôle important joué par l'ENISA dans les phases de planification, de préparation, d'exécution et d'évaluation des exercices de cybersécurité, et SOULIGNE qu'elle devrait demeurer l'un des acteurs centraux au niveau de l'UE, en gardant à l'esprit que ces exercices devraient être menés en s'appuyant sur des cadres structurés et une terminologie commune. INVITE l'ENISA, le réseau des CSIRT et UE-CyCLONe à faire le meilleur usage possible des exercices réguliers existants pour tester et améliorer le cadre de l'UE pour la réaction aux crises, et à exploiter au mieux les enseignements tirés.

COOPÉRATION DE L'ENISA AVEC D'AUTRES ACTEURS DE L'ÉCOSYSTÈME DE CYBERSÉCURITÉ

18. RÉAFFIRME qu'en raison de la nature horizontale de la cybersécurité, la **collaboration entre tous les acteurs au niveau des États membres et de l'Union** est essentielle, et INSISTE dès lors sur le fait que le renforcement de la cyberrésilience globale au niveau européen nécessite également une coopération entre l'ENISA et d'autres entités compétentes dans le domaine cyber.

19. SOULIGNE qu'il importe pour la cyberrésilience globale au niveau de l'UE, à laquelle le CERT-UE contribue de manière déterminante, que les institutions, organes et organismes de l'UE restent capables d'assurer leur cybersécurité. SE FÉLICITE à cet égard de la coopération structurée établie entre le CERT-UE et l'ENISA et les ENCOURAGE à continuer de coopérer étroitement à l'avenir.

20. Grâce à l'autonomie financière qu'il a acquise, le Centre de compétences européen en matière de cybersécurité contribuera de manière significative au développement d'un écosystème européen de cybersécurité solide en matière de recherche, d'industrie et de technologie, regroupant des compétences pour le développement de la main-d'œuvre conformément à son mandat. ENCOURAGE l'ENISA et le Centre de compétences européen en matière de cybersécurité à poursuivre leur étroite coopération, en particulier en ce qui concerne les besoins et les priorités en matière de recherche et d'innovation, ainsi que les cyber-compétences, afin d'accroître la compétitivité du secteur de la cybersécurité de l'Union. INVITE la Commission à examiner comment optimiser encore les synergies dans le fonctionnement de l'ENISA et du Centre de compétences européen en matière de cybersécurité et comment mieux rationaliser les activités conformément à leur mandat respectif.

21. SOULIGNE que la communication régulière d'informations actualisées concernant le paysage des menaces contribue à mieux repérer les mesures et les outils nécessaires pour lutter efficacement contre la cybercriminalité. INSISTE SUR la valeur ajoutée des rapports d'évaluation conjointe de la cybersécurité (JCAR) de l'UE, qui sont le résultat de la collaboration entre l'ENISA, l'EC3 d'Europol et le CERT-UE, et qui ont déjà apporté une contribution précieuse pour relever les différents défis, parmi lesquels la lutte contre la cybercriminalité. INVITE l'ENISA et Europol à continuer de collaborer de manière structurée à l'avenir.

22. RAPPELLE que la cyberdéfense constitue une part importante et en constante évolution de la lutte contre les menaces émanant du cyberespace. INSISTE sur la nécessité pour l'ENISA de dialoguer avec le SEAE et la Commission dans les cas où l'ENISA a un rôle à jouer pour soutenir la mise en œuvre de la politique de cyberdéfense de l'UE, en étroite coopération avec l'AED, le Centre de compétences européen en matière de cybersécurité et la communauté de cyberdéfense. SOULIGNE le rôle de l'ENISA en tant qu'agence civile. INSISTE SUR le fait qu'il importe d'approfondir et de rationaliser la coopération civilo-militaire dans le domaine cyber au sein de l'UE et de procéder notamment à une répartition claire des rôles et des responsabilités entre les deux communautés et entre l'UE et l'OTAN, en respectant pleinement les principes d'inclusivité, de réciprocité, d'ouverture mutuelle et de transparence, ainsi que l'autonomie décisionnelle des deux organisations. ENCOURAGE l'ENISA à poursuivre les arrangements de travail avec l'Agence de communication et d'information de l'OTAN (NCIA).

23. ENCOURAGE l'UE à continuer de promouvoir nos valeurs communes et nos efforts conjoints dans les enceintes mondiales afin de préserver un cyberespace libre, mondial, ouvert et sûr. INSISTE SUR le fait que, de par leur nature transfrontière, les menaces et incidents de cybersécurité doivent faire l'objet d'une collaboration forte et efficace, non seulement au niveau de l'Union, mais aussi **avec les organisations et partenaires internationaux**. FAIT OBSERVER que l'engagement international de l'ENISA devrait se concentrer sur les partenaires stratégiques et les pays candidats à l'adhésion à l'UE, conformément à la politique étrangère et de sécurité commune de l'UE. RAPPELLE que, dans le cadre de cet engagement international, l'ENISA devrait agir conformément au mandat qui lui a été confié et aux dispositions du règlement sur la cybersécurité en la matière. EST CONSCIENT de la nécessité de clarifier, selon les procédures applicables, l'engagement international de l'ENISA, en veillant notamment à ce que son conseil d'administration soit dûment informé, et en temps utile, des activités qui découlent de cet engagement. ENCOURAGE l'ENISA à participer aux structures de coopération internationale pertinentes en matière de cybersécurité, y compris à des organisations telles que l'OTAN et l'OSCE.

24. RAPPELLE que l'UE et ses États membres ont souvent mis en évidence des lacunes sur le plan des **compétences en matière de cybersécurité**. RAPPELLE que la Commission et l'ENISA ont mis en place un cadre large et global pour fournir des orientations à toutes les parties prenantes, et notamment le cadre européen des compétences en matière de cybersécurité, la communication sur une académie des compétences en matière de cybersécurité et la conférence européenne sur les compétences en matière de cybersécurité, organisée chaque année, et ENCOURAGE la Commission et l'ENISA à s'appuyer sur ces initiatives en accordant une attention particulière aux discussions en cours sur le consortium pour une infrastructure numérique européenne (EDIC). À cette fin, INVITE la Commission à se concerter avec les États membres intéressés par la mise en place d'un EDIC. PREND ACTE du fait que l'ENISA et le Centre de compétences européen en matière de cybersécurité sont tous deux chargés de promouvoir les compétences dans l'ensemble de l'Union. INVITE l'ENISA à soutenir en priorité les efforts des États membres en matière de compétences et d'éducation, à sensibiliser davantage le grand public et à collaborer avec le Centre de compétences européen en matière de cybersécurité, le cas échéant.

25. PREND NOTE du fait que l'ENISA a développé ces dernières années une **coopération avec le secteur privé**. RAPPELLE que, étant donné que le secteur privé surveille en permanence le paysage des cybermenaces, les informations qu'il recueille pourraient contribuer à améliorer l'appréciation commune de la situation. ENCOURAGE par conséquent l'ENISA à renforcer la coopération avec le secteur privé, en étroite collaboration avec les États membres et dans l'ensemble des entités de l'UE.

26. INVITE la Commission et l'ENISA à envisager comment renforcer la collaboration entre l'ENISA et les organismes européens de **normalisation**. SOULIGNE la nécessité pour l'ENISA d'accroître son expertise concernant la normalisation européenne en matière de cybersécurité, notamment en assurant un suivi des activités de normalisation et en y participant.

27. DEMANDE INSTAMMENT à la Commission et à l'ENISA d'examiner comment optimiser encore le fonctionnement du cadre de cybersécurité de l'Union, en tenant compte des recommandations et des propositions formulées dans les présentes conclusions. La coopération continue, la hiérarchisation des tâches et des ressources ainsi que la simplification du paysage complexe de la cybersécurité constitueront des éléments essentiels pour relever les défis actuels et futurs.