Conseil de
l'Union européenne

Bruxelles, le 22 mai 2023
(OR. en)

9618/23

COPS 269	**JAI 656**
POLMIL 123	**RELEX 639**
CYBER 130	**JAIEX 22**
HYBRID 31	**TELECOM 154**
EUMC 230	**IPCR 38**
CIVCOM 144	**PROCIV 35**
COPEN 162	**COTER 101**
COSI 103	**DISINFO 34**
DATAPROTECT 146	**CSC 252**
IND 256	**CSDP/PSDC 402**
RECH 191	**CFSP/PESC 748**

RÉSULTATS DES TRAVAUX

Origine:	Secrétariat général du Conseil
Destinataire:	délégations
Nº doc. préc.:	ST 9124/23 COPS 224 POLMIL 104 CYBER 113 HYBRID 20 EUMC 210 CIVCOM 111 COPEN 138 COSI 86 DATAPROTECT 129 IND 232 RECH 173 JAI 574 RELEX 563 JAIEX 16 TELECOM 135 IPCR 31 PROCIV 25 COTER 86 DISINFO 28 CSC 216 CSDP/PSDC 349 CFSP/PESC 674
Objet:	Conclusions du Conseil sur la politique de cyberdéfense de l'UE

Les délégations trouveront ci-joint les conclusions du Conseil sur la politique de cyberdéfense de l'UE, approuvées par le Conseil lors de sa session tenue le 22 mai 2023.

Conclusions du Conseil sur la politique de cyberdéfense de l'UE

1. Dans le prolongement du cadre stratégique de cyberdéfense de 2014 et de sa mise à jour de 2018, le Conseil se félicite de l'ambitieuse communication conjointe sur la politique de cyberdéfense de l'UE, qui vise à investir davantage dans nos forces armées modernes et interopérables, dans les technologies de rupture et dans les capacités de cyberdéfense de pointe, ainsi qu'à renforcer les partenariats pour relever les défis communs. Le cyberespace est devenu un domaine de concurrence stratégique, dans une période de dépendance croissante à l'égard des technologies numériques. Il est donc essentiel de maintenir un cyberespace ouvert, libre, stable et sécurisé. Le recours à des cyberopérations facilitant et accompagnant la guerre d'agression non provoquée et injustifiée menée par la Russie contre l'Ukraine nuit à la stabilité et à la sécurité mondiales, représente un risque important d'escalade et vient s'ajouter à la multiplication déjà importante des actes de cybermalveillance commis ces dernières années en dehors des conflits armés.

2. La guerre en Ukraine a créé un nouveau contexte stratégique et a confirmé la nécessité pour l'UE, ses États membres et leurs partenaires de renforcer encore la résilience de l'UE face aux cybermenaces et d'accroître notre cybersécurité et notre cyberdéfense communes contre les comportements malveillants et les actes d'agression dans le cyberespace. La communication conjointe sur la politique de cyberdéfense de l'UE témoigne de notre détermination à prendre des mesures immédiates et à long terme pour garantir la liberté d'action dans le cyberespace et à réagir face aux acteurs de la menace qui cherchent, entre autres, à envahir, perturber ou détruire les réseaux et les systèmes d'information de l'UE et de ses partenaires. Cette communication conjointe, qui vient compléter la stratégie de cybersécurité de l'UE et s'inscrit dans le droit fil de la boussole stratégique, constitue un élément important de l'approche globale de l'UE en matière de résilience, de réaction, de prévention des conflits, de coopération et de stabilité au sein du cyberespace. Dans ce contexte, le Conseil souligne que les réactions de l'UE, de ses États membres et de leurs partenaires doivent être appropriées et cohérentes, et il attend également avec intérêt la révision des lignes directrices pour la mise en œuvre de la boîte à outils cyberdiplomatique de l'UE, qui marquera une nouvelle étape essentielle dans l'évolution de la cyber posture de l'UE.

3. Le Conseil insiste sur le fait que les cyberattaques perpétrées récemment contre des infrastructures critiques européennes, l'évolution rapide du paysage des cybermenaces et le rythme soutenu du développement technologique démontrent en outre qu'il est nécessaire de renforcer la coordination et la coopération civilo-militaires, mais il précise qu'il n'existe aucune hiérarchie entre la sphère civile et la sphère militaire.
La politique de cyberdéfense de l'UE permet à cette dernière et à ses États membres de renforcer leur capacité de protection, de détection, de défense et de dissuasion, en utilisant de manière appropriée tout l'éventail des moyens défensifs dont disposent les sphères civile et militaire pour assurer la sécurité et la défense générales de l'UE, conformément au droit international, y compris le droit relatif aux droits de l'homme et le droit international humanitaire.

4. Si la sécurité nationale, y compris dans le domaine cyber, reste de la seule responsabilité de chaque État membre, comme indiqué à l'article 4, paragraphe 2, du TUE, le Conseil souligne, dans le même temps, qu'il est nécessaire d'investir massivement, à titre individuel et collectif, dans le renforcement de la résilience et dans le déploiement de tout l'éventail des capacités défensives de cyberdéfense, ainsi qu'en tirant parti des cadres de coopération et des incitations financières de l'UE. Le Conseil insiste sur la poursuite nécessaire du renforcement des actions que mènent les États membres ainsi que les institutions, organes et organismes de l'UE pour protéger l'Union, ses citoyens, les institutions, organes et organismes de l'UE et les missions et opérations de PSDC dans le cyberespace. Il attire en outre l'attention sur le fait qu'il importe d'assurer la résilience de l'UE au sein du cyberespace en développant les capacités de cyberdéfense et en intensifiant la coopération avec un écosystème privé fiable.

I. **Agir ensemble pour renforcer la cyberdéfense**

5. Le Conseil réaffirme qu'un processus progressif, transparent et inclusif est essentiel pour le renforcement de la confiance, lequel est indispensable pour la poursuite de la mise en place d'un cadre européen de gestion des crises en matière de cybersécurité, conformément à la feuille de route pour la gestion des crises de cybersécurité élaborée au sein du Conseil. Le Conseil rappelle qu'il est nécessaire de continuer à améliorer notre capacité de protection, de détection, de défense et de dissuasion face aux cyberattaques grâce à une meilleure appréciation de la situation, au développement des capacités, à la formation, à l'organisation d'exercices et à une résilience accrue ainsi qu'en réagissant fermement, par tous les moyens appropriés, aux cyberattaques visant l'UE, ses États membres ainsi que ses institutions, organes et organismes et les missions et opérations de PSDC. Dans ce cadre, le Conseil encourage le haut représentant et la Commission à réduire la complexité dans le domaine cyber, à éviter les doubles emplois inutiles et à assurer une coopération et des synergies avec les initiatives existantes. Il convient de renforcer la coopération et la coordination entre les acteurs de la cyberdéfense au sein de l'UE et des États membres, entre la sphère militaire et la sphère civile ainsi qu'entre un écosystème public et un écosystème privé fiable. Dans ce contexte, les États membres sont encouragés à examiner et renforcer plus avant les mécanismes nationaux de coordination civilo-militaire, à faciliter l'échange volontaire commun d'informations, à partager les enseignements tirés, à contribuer à l'élaboration de normes interopérables, à mener des évaluations des risques et à établir des scénarios de risque, ainsi qu'à organiser des exercices conjoints, en particulier au niveau européen, dans le plein respect des dispositions de la directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (SRI 2).

6. Conscient des efforts déployés pour continuer à renforcer la résilience de l'Union au moyen de la directive SRI 2 et de la directive sur la résilience des entités critiques (CER), le Conseil répète sa recommandation relative à une approche coordonnée de l'Union pour renforcer la résilience des infrastructures critiques[1]. Il préconise des mesures visant à renforcer plus avant la résilience des entités, infrastructures, produits et services numériques critiques, tout en précisant que la bonne mise en œuvre de la directive SRI 2 demeure l'élément le plus important. Bien qu'il s'agisse principalement d'une responsabilité civile, cela contribue également à renforcer la cyberdéfense. Dans ce contexte, les institutions, organes et organismes de l'UE ainsi que les États membres sont encouragés à soutenir la poursuite du développement et le déploiement des mécanismes de coordination nouveaux et existants au niveau de l'Union, les analyses et évaluations des risques et les scénarios de risques, l'échange volontaire commun d'informations et les exercices communs, en veillant à ce que soit apportée une valeur ajoutée et en évitant les doubles emplois inutiles avec les initiatives existantes.

7. Dans la perspective de la poursuite du renforcement de la confiance, de la consolidation de la coopération et de la facilitation de l'échange d'informations en temps utile sur les cyberincidents importants et de grande ampleur affectant les systèmes de défense, le Conseil se félicite de l'initiative visant à continuer de développer la Conférence des cybercommandeurs de l'UE, qui sera organisée par chaque présidence du Conseil de l'UE, avec le concours de l'Agence européenne de défense (AED) et la participation du Service européen pour l'action extérieure (SEAE). Le Conseil encourage tous les États membres à participer à ces réunions. Afin de renforcer la résilience de l'UE face aux incidents de cybersécurité majeurs, le Conseil invite le réseau européen d'organisations de liaison en cas de crises de cybersécurité (UE – CyCLONe) et la Conférence des cybercommandeurs de l'UE à recenser les pistes envisageables pour coopérer et bénéficier d'une démarche conjointe militaire et civile.

---

[1] Proposition de recommandation du Conseil relative à une approche coordonnée de l'Union pour renforcer la résilience des infrastructures critiques (COM/2022/551 final).

8. En vue de favoriser une réaction plus ferme et mieux coordonnée au niveau de l'UE, le Conseil salue la mise en place du réseau opérationnel de l'UE d'équipes militaires d'intervention en cas d'urgence informatique (MICNET) et s'attend à ce que la capacité opérationnelle initiale de ce réseau soit atteinte d'ici mi-2024 afin d'améliorer le partage d'informations techniques sur les cyberincidents affectant les systèmes de défense entre les États membres participants. Le Conseil encourage tous les États membres à participer au réseau MICNET afin d'en garantir l'efficacité. En outre, le Conseil invite les États membres à s'inspirer des enseignements tirés du réseau des centres de réponse aux incidents de sécurité informatiques (CSIRT) et encourage vivement la création d'un mécanisme efficace de coopération et de coordination entre les deux réseaux en temps opportun, dans le plein respect des mécanismes de gouvernance et des groupes cibles de chaque entité.

9. Compte tenu de l'augmentation des actes de cybermalveillance d'acteurs étatiques et non étatiques ciblant les missions et opérations menées par l'UE dans le cadre de la PSDC, le Conseil invite l'UE et ses États membres à renforcer leurs capacités afin de protéger et sécuriser les missions et opérations de PSDC. À cet égard, le Conseil se félicite des objectifs visant à faire progresser la protection des réseaux et structures militaires de l'UE, conformément, entre autres, à la vision et à la stratégie militaires de l'UE sur le cyberespace en tant que domaine d'opérations[2].

[2] EEAS(2021) 706 REV4.

10. Le Conseil rappelle ses conclusions de mai 2022[3] et la nécessité d'investir dans notre assistance mutuelle au titre de l'article 42, paragraphe 7, du TUE, ainsi que de la clause de solidarité figurant à l'article 222 du TFUE. Le Conseil souligne qu'il importe de continuer à approfondir la compréhension commune qu'ont l'UE et ses États membres de la mise en œuvre de l'article 42, paragraphe 7, y compris dans le cadre de scénarios complexes comportant une cyberattaque, conformément aux principes pertinents du droit international. Il se félicite qu'il soit possible d'obtenir, à la demande explicite du ou des États membres concernés, un soutien de l'UE en cas de cyberattaque, sans préjudice du caractère spécifique de la politique de sécurité et de défense de certains États membres.

11. Le Conseil relève les progrès réalisés dans le cadre du projet mis sur pied au titre de la CSP intitulé "Équipes d'intervention rapide en cas d'incident informatique et assistance mutuelle dans le domaine de la cybersécurité" (CRRT) et précise qu'il est prêt à agir sur demande pour répondre aux besoins des États membres et de l'UE, à l'appui des missions et opérations de PSDC, et à apporter une assistance aux partenaires de l'UE. Le Conseil se félicite de la poursuite du développement des capacités des CRRT au titre de la CSP, des équipes nationales d'intervention en cas d'incident informatique et, le cas échéant, des capacités supplémentaires d'intervention en cas d'incidents, telles que les futures équipes d'intervention rapide en cas de menaces hybrides prévues dans la boussole stratégique, y compris par la facilitation de leur coordination et de leur coopération au niveau de l'UE.

[3] Conclusions du Conseil sur la mise en place d'une posture cyber de l'Union européenne, 23 mai 2022 (9364/22).

12. Le Conseil salue les travaux menés dans le cadre du projet CSP de Centre de coordination dans le domaine du cyber et de l'information (CIDCC), qui vise à fournir des capacités militaires pour collecter et analyser les informations pertinentes en vue d'obtenir un tableau opérationnel commun du cyberespace. Le Conseil accueille également avec satisfaction la proposition visant à intégrer la validation du concept, s'il se révèle efficace en tant que centre de coordination de l'information, à partir de 2025, dans un Centre de coordination de l'UE en matière de cyberdéfense (EUCDCC), ce qui améliorera la coordination et l'appréciation de la situation, en particulier pour les commandants des missions et opérations de PSDC de l'UE, ainsi que le renforcement de l'architecture globale de commandement et de contrôle de l'UE. Le Conseil invite le haut représentant à présenter un concept et une feuille de route pour la mise en place de l'EUCDCC, en tirant les enseignements d'entités internationales similaires, en déterminant les ressources nécessaires, en évitant les doubles emplois inutiles et en recherchant la complémentarité avec le cadre global de l'UE en matière de cybersécurité.

13. Le Conseil souligne l'importance que revêt la coopération stratégique en matière de renseignement sur les cybermenaces et les actes de cybermalveillance, et invite les États membres, par l'intermédiaire de leurs autorités compétentes, à continuer de contribuer aux travaux menés par le Centre de situation et du renseignement de l'UE, la direction "Renseignement" de l'EMUE et les États membres dans le cadre de la capacité unique d'analyse du renseignement (SIAC). Le Conseil précise en outre qu'il importe de renforcer nos capacités de cyberrenseignement afin d'améliorer notre résilience et nos réactions dans le domaine cyber et d'apporter un soutien efficace à nos missions et opérations civiles et militaires relevant de la PSDC, ainsi qu'à nos forces armées et aux capacités de la SIAC dans le domaine cyber, sur la base de contributions volontaires des États membres en matière de renseignement et sans préjudice des compétences de ces derniers.

14. Le Conseil prend acte de l'existence du centre d'analyse et de situation de la Commission européenne dans le domaine du cyber, qui vise à améliorer l'appréciation de la situation par la Commission. Le Conseil souligne qu'il importe d'établir une coopération mutuellement bénéfique entre ce centre et les autres institutions, organes et organismes de l'UE, en particulier l'ENISA et la CERT-UE. Il précise qu'il convient d'assurer une coopération étroite avec les réseaux de coopération de l'UE lors du développement de l'appréciation de la situation, et de respecter la confidentialité. Le Conseil note qu'il est nécessaire de renforcer l'appréciation commune de la situation au niveau de l'UE et de poursuivre le développement du cadre de l'UE pour la réaction aux crises de cybersécurité, tout en évitant les doubles emplois inutiles.

15. Le Conseil rappelle que l'éducation, la formation et les exercices dans le domaine cyber sont essentiels pour garantir la préparation et l'efficacité, et se félicite des activités nationales ainsi que de celles menées par l'UE par l'intermédiaire du Collège européen de sécurité et de défense (CESD), de l'AED, de l'ENISA, de même que des projets en cours dans le cadre de la CSP, tels que les Fédérations de plateformes de simulation cyber et l'Académie et plateforme d'innovation de l'UE dans le domaine du cyber (CAIH). En vue d'une intensification encore plus grande de ces efforts, le Conseil attend avec intérêt la mise en place du projet-cadre CyDef-X de l'AED visant à synchroniser et à soutenir les exercices de cyberdéfense. Le Conseil encourage l'AED à examiner, en étroite coopération avec les États membres et le SEAE, la manière dont le projet CyDef-X pourrait continuer à soutenir des exercices tels que l'exercice Cyber Phalanx, y compris en ce qui concerne l'assistance mutuelle au titre de l'article 42, paragraphe 7, du TUE et de la clause de solidarité figurant à l'article 222 du TFUE, ainsi qu'avec la Commission et l'ENISA pour ce qui est des exercices civils. En outre, le Conseil encourage l'utilisation et la poursuite du développement, dans le cadre du projet CyDef-X, des environnements existants de test et d'exercices dans le domaine de la cyberdéfense, tels que les Fédérations de plateformes de simulation cyber. Le Conseil souligne qu'il importe, afin de garantir un processus décisionnel souple et efficace en cas de crise de cybersécurité, d'organiser régulièrement des exercices de simulation sur table pour le niveau décisionnel des États membres.

16. Le Conseil prend note de la proposition de législation en matière de cybersolidarité et de l'intention de renforcer les capacités de détection des menaces et incidents de cybersécurité dans l'UE et de réaction à ceux-ci. Il souligne que les propositions dans ce domaine ne peuvent être efficaces que si elles sont conformes aux cadres et aux besoins des États membres en matière de gestion des crises. Le Conseil souligne qu'il importe de tester les infrastructures critiques pour détecter les vulnérabilités potentielles, lorsque cela est jugé bénéfique, en tant que compétence nationale, en tenant compte des analyses de risques disponibles au niveau de l'UE.

17. Le Conseil prend note de la proposition de la Commission visant à mettre en place un mécanisme d'urgence en matière de cybersécurité, qui pourrait soutenir la disponibilité de services de cybersécurité émanant de prestataires de confiance privés pour aider les États membres à leur demande en cas d'incidents de cybersécurité majeurs, tout en insistant sur le fait qu'il est nécessaire de développer un secteur européen de la cybersécurité avec le concours du Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité, en tant que pilier essentiel pour rendre ce mécanisme opérationnel. Le Conseil attire l'attention sur le rôle essentiel que joue chaque État membre dans le suivi et l'évaluation de ses besoins nationaux.

II. **Sécuriser l'écosystème de la défense de l'UE**

18. Le Conseil rappelle qu'il encourage les États membres à poursuivre le développement de leurs propres capacités à mener des opérations de cyberdéfense, y compris, le cas échéant, des mesures défensives proactives de protection, détection, défense et dissuasion face aux cyberattaques. Étant donné que la directive SRI 2 ne s'applique pas aux entités de l'administration publique qui exercent leurs activités dans le domaine de la défense, le Conseil invite l'AED, avec le soutien de la Commission et du SEAE, le cas échéant, à aider les États membres à élaborer des recommandations volontaires juridiquement non contraignantes inspirées de la directive SRI 2 afin d'accroître la cybersécurité au sein de la communauté de la défense, et invite tous les États membres à participer activement à cet effort. Ces recommandations devraient tenir compte des efforts similaires entrepris dans d'autres cadres.

19. Comme indiqué dans la boussole stratégique, la capacité d'action de l'UE dépend de son aptitude à réduire ses dépendances stratégiques dans le cadre de toutes ses capacités de cyberdéfense et de ses chaînes d'approvisionnement, ainsi qu'à développer et à maîtriser des technologies de cyberdéfense de rupture. Il s'agit notamment de renforcer la base industrielle et technologique de défense européenne (BITDE) dans l'ensemble de l'UE, ainsi que sa capacité à coopérer avec des partenaires partageant les mêmes valeurs à travers le monde, sur une base réciproque pour obtenir des avantages mutuels. Le Conseil appelle dès lors les secteurs de la cybersécurité et de la cyberdéfense à coopérer étroitement afin de créer des synergies dans le but de développer et de fournir des capacités de cyberdéfense couvrant la totalité du spectre. Le Conseil invite la Commission, en étroite collaboration avec le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité, le cas échéant, à continuer de soutenir la mise en place d'une base industrielle et technologique européenne de cyberdéfense forte, souple, compétitive au niveau mondial et innovante, comprenant des petites et moyennes entreprises (PME), au moyen de nouveaux investissements et de mesures stratégiques.

20. Compte tenu de l'importance que revêtent l'interopérabilité et la communauté de conception des capacités de cyberdéfense, y compris en ce qui concerne le développement collaboratif de capacités de cyberdéfense de nouvelle génération, le Conseil invite l'AED et l'état-major de l'UE à s'employer à mettre au point un ensemble d'exigences de l'UE en matière d'interopérabilité dans le domaine de la cyberdéfense, qui s'appuieraient sur les principes, processus et normes existants établis en particulier dans le cadre de l'Organisation du traité de l'Atlantique Nord (OTAN) et seraient compatibles avec ceux-ci. En outre, le Conseil invite les États membres à examiner, dans le cadre du Comité européen de normalisation de la défense, si des normes volontaires spécifiques pour les systèmes de défense pourraient être requises, en étroite coopération avec toutes les parties prenantes concernées, y compris les organisations européennes de normalisation et l'OTAN, le cas échéant.

21. Le Conseil salue les efforts réalisés par la Commission pour présenter un plan visant à promouvoir l'utilisation des normes existantes pour les utilisations civiles en matière de cybersécurité et de cyberdéfense, ainsi que l'élaboration de nouvelles normes volontaires. Il souligne qu'il est nécessaire, le cas échéant, d'harmoniser les normes de cybersécurité et de cyberdéfense. Le Conseil est conscient que de telles normes volontaires pourraient être utiles pour les secteurs de la cybersécurité et de la cyberdéfense de l'UE et recommande une collaboration plus étroite entre les organismes de normalisation des domaines civil et de la défense.

22. Le Conseil préconise l'élaboration rapide de recommandations fondées sur la cartographie des outils de communication sécurisée existants dans le domaine cyber, réalisée par la Commission et les institutions compétentes. Dans la mesure du possible, les recommandations devraient être alignées sur les initiatives existantes en matière de partage d'informations et devraient également tenir compte des risques que posent les technologies émergentes et de rupture pour les méthodes de chiffrement actuelles.

23. Par ailleurs, le Conseil se félicite des premiers travaux menés sur l'analyse des risques et les scénarios de risques en cours d'élaboration par la Commission, le haut représentant et le groupe de coopération SRI en ce qui concerne, dans un premier temps, les secteurs de l'énergie et des télécommunications, à la demande du Conseil. Le Conseil prend acte du fait que des analyses ciblées des risques en matière de cybersécurité pour les infrastructures et les réseaux de communication au sein de l'UE sont également en préparation. Le Conseil réaffirme qu'il est de la plus haute importance de parvenir à une compréhension commune des incidences possibles des cyberincidents entre les États membres, mais aussi entre les institutions, organes et organismes de l'UE. Par conséquent, le Conseil invite les acteurs précités à veiller à ce que les analyses de risques, les scénarios de risques et les recommandations ultérieures soient pris en compte lors de la définition et de la hiérarchisation des mesures et du soutien au niveau de l'UE et, le cas échéant, au niveau national. Il préconise en outre que les scénarios de risque soient pris en considération par tous les acteurs concernés dans les processus d'analyse des risques, ainsi que lors de la mise au point d'exercices de cybersécurité.

III. **Investir dans les capacités de cyberdéfense**

24. Le Conseil encourage les États membres à accroître leurs investissements en vue de mettre en place, maintenir et continuer à développer des capacités de cyberdéfense interopérables. Il soutient l'élaboration d'un ensemble d'engagements volontaires visant à poursuivre le développement des capacités nationales de cyberdéfense, en ayant à l'esprit les efforts similaires entrepris dans d'autres cadres.

25. Le Conseil invite les États membres et l'AED à saisir l'occasion offerte par la révision du plan de développement des capacités pour fixer un niveau d'ambition élevé en ce qui concerne le développement de la cyberdéfense collaborative au niveau de l'UE. Il encourage en outre les États membres à s'appuyer sur l'ensemble actualisé de priorités et sur leurs engagements au titre de la CSP pour augmenter leur niveau de participation à des projets collaboratifs de développement des capacités de cyberdéfense de l'UE, compte tenu de l'avantage direct que présentent les projets collaboratifs au niveau de l'UE pour soutenir le développement des capacités nationales de cyberdéfense.

26. Le Conseil salue les efforts de recherche collaborative menés au niveau de l'UE pour étudier les applications possibles, dans les systèmes liés à la défense, des technologies émergentes et de rupture, et il note également qu'il convient de veiller à ce que ces évolutions technologiques soient rapidement intégrées dans les capacités existantes et futures. Il encourage les États membres et l'industrie de l'UE à utiliser au mieux les possibilités de recherche collaborative au niveau de l'UE, par exemple dans le cadre de l'AED, des projets en cours au titre de la CSP, tels que l'Académie et plateforme d'innovation de l'UE dans le domaine du cyber (CAIH), ainsi que dans le cadre du Fonds européen de la défense et, le cas échéant, d'Horizon Europe et du programme pour une Europe numérique pour les projets à double usage. En outre, le Conseil se félicite de la mobilisation des cadres spécifiques pour soutenir l'innovation en matière de défense en utilisant les apports du domaine civil, notamment le programme de l'UE pour l'innovation dans le domaine de la défense et le pôle d'innovation dans le domaine de la défense. Par ailleurs, le Conseil encourage le Centre de compétences européen en matière de cybersécurité et l'AED à élaborer un arrangement de travail visant à faciliter l'échange d'informations entre leurs services respectifs sur les priorités en ce qui concerne les technologies civiles, à double usage et de défense, en vue de créer des synergies et d'éviter les doubles emplois.

27. Le Conseil prend note avec satisfaction de l'intention de la Commission d'élaborer, en coopération avec l'AED et le Centre de compétences européen en matière de cybersécurité conformément à leurs mandats respectifs, avec les États membres et en concertation avec les parties prenantes concernées telles que l'industrie, une feuille de route technologique pour les cybertechnologies critiques qui, en recensant les cybertechnologies critiques et en cartographiant les évolutions technologiques et les dépendances stratégiques, offre les moyens de réduire ces dernières, afin de favoriser l'autonomie stratégique et la souveraineté technologique de l'UE, tout en maintenant une économie ouverte. Le Conseil note que la feuille de route technologique pour les cybertechnologies critiques peut guider le choix des priorités stratégiques pour les instruments de financement de l'UE, tout en respectant les modalités respectives mises en place pour ces instruments. Il rappelle que l'UE devrait mener une politique industrielle européenne ambitieuse et volontariste afin de créer un environnement durable, attrayant et compétitif pour les entreprises, qui puisse également permettre aux entités européennes dans le domaine cyber de se développer.

28. Le Conseil se félicite qu'il soit prévu de combler l'important déficit de compétences en matière de cybersécurité par l'attrait de nouveaux professionnels, dont des femmes, par la reconversion et le perfectionnement professionnels, ainsi que par l'investissement dans des formations et des exercices et l'organisation de formations et d'exercices visant à constituer une main-d'œuvre diversifiée et inclusive dans le domaine cyber. Conscient des défis auxquels est confrontée l'UE en ce qui concerne le capital humain dans le domaine de la cybersécurité et de la cyberdéfense, le Conseil salue l'initiative de l'Académie européenne des compétences cyber, qui pourrait également être bénéfique pour les travailleurs du secteur de la cyberdéfense.

29. Le Conseil invite les États membres à échanger des informations sur les bonnes pratiques afin de former des professionnels qualifiés en matière de cybersécurité, en exploitant les synergies entre les initiatives menées dans les domaines militaire, civil et répressif, et demande au CESD, avec le concours et l'expertise de l'AED et de l'ENISA, d'examiner les moyens d'intensifier l'échange de bonnes pratiques et d'approfondir les synergies entre les sphères militaire et civile en ce qui concerne la formation et le développement de compétences de défense dans le domaine cyber.

30. Le Conseil souligne l'importance que revêt une compréhension commune de la composition de la main-d'œuvre dans le domaine de la cybersécurité et des compétences associées afin de recenser les lacunes sur le marché du travail dans le domaine de la cybersécurité et de les combler, et précise qu'il convient d'associer toutes les parties prenantes, y compris les États membres et l'industrie. Le Conseil est conscient du fait que la mise en place d'indicateurs permettant d'observer le marché du travail dans le domaine de la cybersécurité aiderait à recenser les besoins de compétences en matière de cybersécurité et à orienter les fonds de manière adéquate, tout en contribuant à satisfaire aux obligations liées aux politiques, notamment celles découlant de la directive SRI 2. Il salue la proposition relative à un cadre de certification des compétences en matière de cyberdéfense et invite le haut représentant, en sa qualité de directeur du CESD, à faire progresser ce dossier, en coopération avec le SEAE, la Commission et les États membres, en tirant parti des initiatives civiles.

IV. **Établir des partenariats pour relever les défis communs**

31. Le Conseil invite le haut représentant et la Commission à renforcer et à faire progresser leur coopération et à réfléchir à des partenariats mutuellement bénéfiques et adaptés en ce qui concerne les politiques de cyberdéfense, y compris aux fins du renforcement des capacités de cyberdéfense par l'intermédiaire de la facilité européenne pour la paix (FEP). À cette fin, la cyberdéfense devrait figurer parmi les points examinés lors des dialogues et des consultations de l'UE dans le domaine cyber, ainsi que dans le cadre des consultations globales en matière de sécurité et de défense avec les partenaires. En outre, les dialogues et la collaboration avec le secteur privé devraient être renforcés. Le Conseil souligne que la collaboration internationale concernant les normes et la certification en matière de cybersécurité serait bénéfique pour l'industrie européenne. Il se félicite donc de l'engagement pris par la Commission d'en faire un élément essentiel des dialogues menés par l'UE dans le domaine cyber avec les pays tiers et les organisations internationales.

32. Le Conseil met en avant l'importance que revêt la coopération internationale pour prévenir ou réduire les risques de conflit dans le cyberespace, en particulier par la poursuite de l'élaboration et la mise en œuvre de mesures de confiance à l'échelon régional et international, y compris au niveau des Nations unies, et en continuant à encourager le recours aux mesures de confiance existantes dans le domaine cyber, notamment dans le cadre de l'Organisation pour la sécurité et la coopération en Europe (OSCE), y compris en période de tensions internationales.

    L'UE et ses États membres soulignent que le droit international en vigueur s'applique dans le cyberespace et qu'il importe de poursuivre les efforts visant à faire respecter et promouvoir le cadre des Nations unies pour le comportement responsable des États et à œuvrer à sa mise en œuvre, y compris par la mise en place du programme d'action pour un comportement responsable des États dans le cyberespace.

33. Dans le droit fil des déclarations conjointes relatives à la coopération entre l'UE et l'OTAN, le Conseil invite le haut représentant, y compris en sa qualité de chef de l'AED, et la Commission à continuer à renforcer, à approfondir et à élargir le partenariat dans le domaine cyber avec 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. Tout en tenant compte du fait qu'il est nécessaire de déployer des efforts complémentaires et coordonnés avec la participation la plus large possible des États membres qui ne font pas partie de l'OTAN et d'éviter les doubles emplois inutiles, le Conseil préconise l'établissement de liens aux niveaux pertinents entre l'UE et l'OTAN en ce qui concerne la formation, l'éducation, l'appréciation de la situation, les exercices et les plateformes de R&D, et de rechercher des synergies potentielles entre les engagements volontaires respectifs pour le développement des capacités nationales de cyberdéfense et les cadres de gestion des crises, la protection des infrastructures critiques et l'amélioration des échanges sur l'appréciation de la situation, la coordination des réactions aux cyberactivités malveillantes ainsi que les efforts de renforcement des capacités dans les pays tiers. Cela comprend l'arrangement technique entre la capacité OTAN de réaction aux incidents informatiques (NCIRC) et l'équipe d'intervention en cas d'urgence informatique (CERT-UE), ainsi qu'un dialogue politique renforcé sur les questions de cyberdéfense à tous les niveaux.

V. **Conclusion**

34. Dans le prolongement de ses conclusions sur la politique de cyberdéfense de l'UE, le Conseil invite le haut représentant et la Commission à élaborer, en vue de son approbation par les États membres, un plan de mise en œuvre de cette politique au plus tard au cours du deuxième trimestre de 2023. Il invite également les États membres à indiquer sur une base volontaire leur ambition et leurs actions en matière de cyberdéfense dans le cadre de la politique de cyberdéfense de l'UE et à tirer pleinement parti des recommandations et engagements volontaires juridiquement non contraignants pour intensifier leurs efforts nationaux et multinationaux en matière de cyberdéfense afin de maximiser les effets à l'échelle de l'UE. Le haut représentant, la Commission et les États membres sont invités à rendre compte et à débattre chaque année des progrès accomplis dans la mise en œuvre des éléments de la communication conjointe et de son plan de mise en œuvre à partir du deuxième trimestre de 2024.