COMMISSION
EUROPÉENNE

Strasbourg, le 18.4.2023
COM(2023) 207 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

Remédier à la pénurie de talents dans le secteur de la cybersécurité pour renforcer la compétitivité, la croissance et la résilience de l'UE («L'académie des compétences en matière de cybersécurité»)

Remédier à la pénurie de talents dans le secteur de la cybersécurité pour renforcer la compétitivité, la croissance et la résilience de l'UE

(«L'académie des compétences en matière de cybersécurité»)

1. Il est urgent de réduire les risques en remédiant à la pénurie et à l'insuffisance de compétences en matière de cybersécurité

La cybersécurité ne fait pas seulement partie de la sécurité des citoyens, des entreprises et des États membres. Elle constitue également une nécessité pour garantir la stabilité politique de l'UE, la solidité de ses démocraties et la prospérité de notre société et de nos entreprises. Le **paysage des menaces pour la cybersécurité** a beaucoup changé ces dernières années et une tendance préoccupante s'en dégage: les cyberattaques ciblent de plus en plus des infrastructures critiques militaires et civiles au sein de l'UE. Les acteurs de ces menaces renforcent leurs capacités et des menaces nouvelles, hybrides et émergentes, comme l'utilisation de robots et de techniques fondées sur l'intelligence artificielle, se font jour[1]. Il convient notamment de relever que les acteurs des menaces liées aux rançongiciels (*ransomwares*) infligent couramment des dommages considérables à des entités, aussi bien au niveau financier que du point de vue de leur réputation[2].

Un grand nombre d'incidents de cybersécurité touchent également des administrations publiques et des gouvernements des États membres, ainsi que des institutions, des organes et des organismes de l'Union européenne[3]. Les secteurs de la finance[4] et de la santé[5], qui constituent des piliers de la société et de l'économie, sont aussi régulièrement la cible de cyberattaques[6]. Les tensions géopolitiques liées à la guerre d'agression menée par la Russie contre l'Ukraine intensifient la menace en matière de cybersécurité[7] et sont susceptibles de déstabiliser notre société. La **sécurité** de l'UE ne saurait être garantie sans l'**atout le plus précieux de l'Union: sa population**. L'UE a besoin de toute urgence de professionnels possédant les aptitudes et les compétences nécessaires pour prévenir, détecter et décourager

[1] Paysage des menaces 2022 de l'ENISA – ENISA (europa.eu)

[2] Europol, évaluation de la menace que représente la criminalité organisée sur l'internet (iOCTA) 2021. Ces acteurs s'appuient sur le modèle de type rançongiciel en tant que service. Le coût annuel pour les entreprises a dépassé 18,4 milliards d'EUR en 2022 (Cybereason, rapport 2022, «Ransomwares - Le véritable impact économique»).

[3] Voir, par exemple, publication conjointe de l'ENISA et de la CERT-EU, JP-23-01 – Sustained activity by specific threat actors (Activité soutenue d'acteurs de menaces spécifiques), TLP:CLEAR, 15 février 2023.

[4] Voir, par exemple, en Allemagne, les cas de fraude par courrier électronique signalés du 1er juin 2021 au 31 mai 2022 dont 90 % étaient des hameçonnages financiers, ou l'attaque menée contre une entreprise du secteur financier, au cours de laquelle plus de 20 000 dispositifs de 125 pays ont été infectés, The State of IT Security in Germany in 2022 (L'état de la sécurité informatique en Allemagne en 2022), Bundesamt für Sicherheit in der Informationstechnik (BSI), 1er janvier 2023.

[5] Voir, par exemple, en France, les attaques par rançongiciels menées contre des établissements de santé publics, notamment l'attaque contre le Centre Hospitalier Sud Francilien, au cours de laquelle 11 Go de données à caractère personnel et médical, ainsi que des données relatives au personnel, ont été compromises et publiées en ligne par l'acteur de la menace, Panorama de la cybermenace 2022, Agence nationale de la sécurité des systèmes d'information (ANSSI), janvier 2023.

[6] Rapport de l'ENISA sur le paysage des menaces 2022.

[7] Voir aussi: CERT-EU – Russia's war on Ukraine: one year of cyber operations (Guerre de la Russie contre l'Ukraine: un an de cyberopérations) (europa.eu); Cyberopérations russes contre l'Ukraine: déclaration du haut représentant au nom de l'Union européenne, 10 mai 2022; Déclaration du haut représentant au nom de l'Union européenne sur les actes de cybermalveillance perpétrés par des pirates informatiques et des groupes de pirates informatiques dans le contexte de l'agression de la Russie contre l'Ukraine, 19 juillet 2022.

les cyberattaques, défendre l'UE, y compris ses infrastructures les plus critiques, contre ce type d'attaques et assurer sa **résilience**.

La pénurie de talents dans le secteur de la cybersécurité constitue une entrave supplémentaire à la **compétitivité** et à la **croissance** de l'Europe, qui dépendent fortement de la mise au point et de l'adoption de technologies numériques stratégiques (par exemple, l'intelligence artificielle, la 5G et l'informatique en nuage). L'UE a besoin d'une main-d'œuvre qualifiée dans le domaine de la cybersécurité pour rester en mesure de fournir des technologies de pointe essentielles dans un contexte mondial.

Afin d'anticiper ces menaces qui évoluent et d'y répondre et pour favoriser sa compétitivité, l'UE a considérablement fait progresser la politique de cybersécurité de l'UE au cours des dernières années; un certain nombre d'initiatives ont ainsi été adoptées, comme la stratégie de cybersécurité de l'UE pour la décennie numérique[8], la directive révisée sur la sécurité des réseaux et des systèmes d'information (directive SRI 2)[9], la législation sectorielle de l'UE sur la cybersécurité[10], la politique de cyberdéfense de l'UE[11], le règlement sur la cyberrésilience[12] et le règlement sur la cybersolidarité, que la Commission propose parallèlement à la présente communication. Toutefois, sans les personnes qualifiées nécessaires pour leur mise en œuvre, ces actes législatifs n'atteindront pas leurs objectifs. Si les connaissances élémentaires de la population générale en matière de cybersécurité sont abordées dans le cadre d'initiatives visant à soutenir le développement des compétences générales nécessaires pour participer à la société[13], il est essentiel de disposer d'une main-d'œuvre compétente, tant dans le secteur public que dans le secteur privé, aux niveaux national et de l'UE, y compris au sein des organismes de normalisation, **afin de satisfaire aux exigences juridiques et politiques en matière de cybersécurité**.

La sécurité et la compétitivité de l'UE dépendent donc de l'existence d'une main-d'œuvre professionnelle qualifiée dans le secteur de la cybersécurité. Or l'UE connaît une pénurie très importante de professionnels qualifiés en cybersécurité, ce qui l'expose, de même que ses États membres, ses entreprises et ses citoyens, à un risque d'incidents de cybersécurité. En 2022, il manquait **entre 260 000**[14] **et 500 000**[15] professionnels dans le secteur de la

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

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

[10] Notamment, pour le secteur financier, le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011 (règlement DORA).

[11] Communication au Parlement européen et au Conseil – La politique de cyberdéfense de l'UE, JOIN(2022) 49 final.

[12] Proposition de règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020 [COM(2022) 454 final].

[13] Parmi les initiatives pertinentes traitant des compétences numériques générales de la population: l'objectif de porter à 80 % le pourcentage de la population disposant de compétences numériques de base d'ici à 2030, fixé dans le cadre du plan d'action sur le socle européen des droits sociaux et de la boussole numérique; le plan d'action en matière d'éducation numérique 2021-2027; l'outil du cadre de compétences numériques; ou la proposition de recommandation du Conseil relative à l'amélioration de l'offre de compétences numériques dans le domaine de l'éducation et de la formation.

[14] (ISC)² dans Assessing Cyber Skills on the basis of the ECSF (Évaluation des compétences informatiques sur la base de l'ECSF), webinaire de l'ENISA, 16 février 2023.

[15] Selon l'Organisation européenne pour la cybersécurité (ECSO), comme indiqué dans la communication au Parlement européen et au Conseil – La politique de cyberdéfense de l'UE, JOIN(2022) 49 final.

cybersécurité au sein de l'Union européenne, alors que les besoins en main-d'œuvre de l'UE dans le domaine de la cybersécurité étaient estimés à 883 000 professionnels[16], ce qui tend à indiquer un décalage entre les compétences disponibles et celles requises par le marché du travail. La main-d'œuvre dans le domaine de la cybersécurité souffre en outre d'une méprise associée à son image technique et ne parvient toujours pas attirer les **femmes**, qui représentent 20 % des diplômés dans ce domaine[17] et 19 % des spécialistes des technologies de l'information et de la télécommunication (TIC) [18]. Afin de remédier à ce problème, le **programme d'action de l'Europe pour la décennie numérique à l'horizon 2030**[19] a fixé comme objectif d'augmenter de 20 millions le nombre de spécialistes des TIC d'ici à 2030, en parvenant en même temps à une parité entre les hommes et les femmes. En outre, la mise en œuvre de la nouvelle politique de l'UE nécessite une main-d'œuvre correctement formée et suffisante. À titre d'exemple, plus de 42 % des cadres supérieurs en informatique dans le secteur des services financiers ont souligné que le manque de compétences et de savoir-faire en matière de cybersécurité constituait un problème majeur auquel leur entreprise était confrontée s'agissant de cyberdéfense et de gestion des incidents de cybersécurité[20], alors qu'ils vont devoir mettre en œuvre la législation sectorielle en matière de cybersécurité, notamment le règlement sur la résilience opérationnelle numérique du secteur financier (règlement DORA).

Les employeurs à la recherche d'une main-d'œuvre déjà formée et expérimentée se montrent réticents à investir dans le capital humain, ce qui constitue également un frein sur le marché du travail[21]. Cette pénurie concerne tous les types d'entreprises, y compris les petites et moyennes entreprises (**PME**), qui représentent 99 % de l'ensemble des entreprises de l'UE[22]. Le problème est aussi de taille pour les **administrations publiques** qui sont fortement touchées, surtout par des incidents de cybersécurité[23].

Dès lors que la sécurité et la compétitivité de l'UE sont en jeu, il est urgent de remédier à la pénurie de talents professionnels dans le secteur de la cybersécurité de l'UE.

2. L'absence de synergies et d'actions coordonnées pour remédier à la pénurie de compétences dans le secteur de la cybersécurité

Les initiatives d'entités publiques et privées se multiplient aux niveaux européen et national pour remédier à la pénurie qui frappe le marché du travail en matière de cybersécurité. Ces initiatives sont toutefois isolées et n'ont jusqu'à présent pas atteint la masse critique nécessaire pour avoir une réelle incidence.

---

[16] (ISC)² dans Assessing Cyber Skills on the basis of the ECSF (Évaluation des compétences informatiques sur la base de l'ECSF), webinaire de l'ENISA, 16 février 2023.

[17] Base de données sur l'enseignement supérieur en matière de cybersécurité (CyberHEAD).

[18] Seuls 19 % des spécialistes des TIC au sein de l'UE sont des femmes. Indice relatif à l'économie et à la société numériques (DESI) 2022 |Façonner l'avenir numérique de l'Europe (europa.eu). Aucun chiffre n'est disponible en ce qui concerne la main-d'œuvre féminine de l'Union dans le domaine de la cybersécurité.

[19] Décision (UE) 2022/2481 du Parlement européen et du Conseil du 14 décembre 2022 établissant le programme d'action pour la décennie numérique à l'horizon 2030, qui met en place un mécanisme de suivi et de coopération pour atteindre les objectifs communs de la transformation numérique de l'Europe définis dans la boussole numérique pour2030, y compris le domaine des compétences.

[20] S-RM Cyber Security Insights Report 2022 (Rapport du S-RM sur la cybersécurité 2022).

[21] «Cybersecurity Skills Development in the EU» (Développement des compétences en matière de cybersécurité dans l'UE), ENISA, décembre 2019.

[22] Définition de PME (europa.eu).

[23] Paysage des menaces 2022 de l'ENISA – ENISA (europa.eu).

Tout d'abord, force est de constater que la composition de la main-d'œuvre de l'UE dans le domaine de la cybersécurité et des compétences associées est actuellement mal comprise, alors que des profils d'emploi comparables dans le secteur de la cybersécurité devraient impliquer le même ensemble de compétences. L'utilisation encore insuffisante, par les acteurs concernés, d'un **cadre de référence européen commun pour les professionnels de la cybersécurité** se traduit par l'absence d'un outil de communication entre les employeurs, les éducateurs et les décideurs politiques, ainsi que par l'incapacité à effectuer des mesures et à évaluer les failles du marché du travail en matière de cybersécurité. Elle empêche également de concevoir des programmes d'éducation et de formation et de créer des parcours de carrière adaptés aux besoins des politiques et du marché pour les personnes qui souhaitent accéder à la profession. Le **perfectionnement et la reconversion professionnels** de la main-d'œuvre reposent en grande partie sur des formations et des certificats en matière de cybersécurité, en général proposés par des prestataires privés. Il n'est toutefois pas évident, pour la main-d'œuvre, d'obtenir un aperçu de la qualité des formations en cybersécurité proposées et des certificats délivrés à leur issue.

Si l'éducation, la formation et la création de parcours de carrière sont nécessaires pour améliorer l'offre sur le marché du travail, le rôle de la **demande** dans la formation de sa main-d'œuvre et dans l'adaptation à son évolution est actuellement sous-estimé. L'industrie et les employeurs publics manquent de forums et d'espaces communs leur permettant de mettre en commun leurs idées sur la meilleure manière de former la main-d'œuvre et d'examiner comment **mieux évaluer les compétences**, notamment au cours du processus de recrutement. Les **compétences techniques** les plus demandées peuvent être liées à la cybersécurité[24], comme le développement de logiciels ou l'informatique en nuage[25], mais les **compétences transversales** ne sont toujours pas prises en considération, sans que cela se justifie. L'esprit critique et l'analyse, la résolution de problèmes et l'autogestion constituent des groupes de compétences très recherchées par les employeurs[26] et de plus en plus importantes à l'horizon 2025[27].

Il existe déjà de nombreuses initiatives d'investissement public et privé dans les compétences en matière de cybersécurité, bénéficiant d'un important **soutien financier** de l'UE octroyé au titre de différents instruments[28]. La pénurie constante des compétences au sein de l'UE soulève toutefois des questions quant à leur visibilité et à leur incidence et semble indiquer qu'elles ne correspondent peut-être pas systématiquement aux besoins du marché, qui doivent être recensés de toute urgence au niveau de l'UE. En outre, la multiplication des sources de financement favorise les doubles emplois, ce qui empêche ces initiatives de prendre de l'ampleur et d'avoir un impact réel. De plus, les initiatives qui ont besoin d'un investissement ne parviennent pas toujours à cerner les sources les plus susceptibles de répondre à leurs besoins.

Les **parties prenantes** s'efforcent de traiter la question complexe et multidimensionnelle de la pénurie de compétences dans le secteur de la cybersécurité. L'Agence de l'Union

[24] LinkedIn 2023 Most In-Demand Skills: Learn the Skills Companies Need Most (Les compétences les plus demandées sur LinkedIn en 2023: découvrez les compétences dont les entreprises ont le plus besoin).

[25] Rapport 2022 de l'ISACA sur l'état de la cybersécurité.

[26] Comme l'outil du CEDEFOP: Skills-OVATE | CEDEFOP (europa.eu).

[27] The Future of Jobs Report (rapport sur l'avenir de l'emploi), octobre 2020, Forum économique mondial.

[28] Par exemple: Alliance pour les compétences en cybersécurité – Une nouvelle vision pour l'Europe – projet REWIRE (initiative financée par le programme Erasmus+); les projets soutenant le Centre de compétences européen en matière de cybersécurité [ECHO, CONCORDIA, CyberSec4Europe, SPARTA (projet financé par Horizon 2020), projet Cybersecpro (financé au titre du programme pour une Europe numérique)].

européenne pour la cybersécurité (ENISA) a mis au point des instruments liés aux profils de rôle ou à l'enseignement supérieur[29], le Centre de compétences européen en matière de cybersécurité (ECCC)[30] étudie la question des compétences en matière de cybersécurité au sein d'un groupe de travail spécifique, le Collège européen de sécurité et de défense (CESD) travaille sur les compétences en matière de cybersécurité de la main-d'œuvre civile et militaire dans le cadre de la politique de sécurité et de défense commune[31], des organisations privées cherchent à résoudre le problème[32], le secteur de la certification en matière de cybersécurité élabore actuellement une feuille de route et des formations axées sur la pénurie de compétences[33]. Les États membres essaient également d'apporter des solutions au problème dans le cadre d'initiatives diverses allant de la réglementation[34] à la création d'académies de compétences en matière de cybersécurité[35] ou de campus cyber[36], en passant par des centres d'excellence en matière de cybercriminalité[37], ou encore par des partenariats public-privé[38]. Cependant, les efforts de toutes ces parties prenantes manquent souvent de coordination et de synergies et n'ont pas encore eu une incidence substantielle sur le marché du travail, comme le montre la pénurie croissante de main-d'œuvre dans le domaine de la cybersécurité au sein de l'UE. Il est également nécessaire d'accroître les synergies entre les cybercommunautés, étant donné que les compétences nécessaires pour faire respecter la cybersécurité, lutter contre la **cybercriminalité** ou élaborer des réponses en matière de **cyberdéfense** sont souvent de même nature.

Enfin, l'UE dispose actuellement de moyens limités pour évaluer l'**état et l'évolution du marché du travail en matière de cybersécurité** et des compétences de sa main-d'œuvre. Les États membres et les institutions, organes et organismes de l'Union européenne s'appuient sur des données recueillies par des entités privées ou sur un ensemble plus large de données collectées au sein de l'UE, notamment par Eurostat[39] et le Centre européen pour le développement de la formation professionnelle (CEDEFOP)[40] sur les professionnels des TIC. En d'autres termes, l'UE a une vision partielle et fragmentée de ses besoins, ce qui l'empêche de consolider une vision agrégée de l'état du marché du travail en matière de cybersécurité.

3. Réponse coordonnée à l'échelle de l'UE: l'académie des compétences en matière de cybersécurité

[29] Notamment: le cadre européen de compétences en matière de cybersécurité (ECSF); la base de données sur l'enseignement supérieur en cybersécurité (CyberHEAD); la Cyber Exercise Platform (plateforme de cyberexercice) (CEP); le défi européen de la cybersécurité; le mois européen de la cybersécurité.

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

[31] Notamment la plateforme de formation, d'entraînement, d'exercices et d'évaluation (ETEE) dans le domaine du cyber.

[32] Par exemple, le groupe de travail 5 de l'Organisation européenne pour la cybersécurité (ESCO) sur «l'éducation, la formation, la sensibilisation, les plateformes de simulation cyber, les facteurs humains»; l'organisation DIGITALEUROPE.

[33] Par exemple, l'institut SANS, (ISC)², ISACA.

[34] Par exemple, dans les stratégies nationales en matière d'éducation ou de cybersécurité.

[35] Par exemple, la C-Academy au Portugal.

[36] Par exemple, les campus cyber en France.

[37] Par exemple, le Centre lituanien d'excellence en matière de cybercriminalité pour la formation, la recherche et l'éducation en Lituanie (L3CE).

[38] Par exemple, le Plan Compétences Cybersécurité de Microsoft.

[39] ICT specialists in employment - Statistics Explained (spécialistes des TIC en activité - statistiques expliquées) (europa.eu)

[40] Comme l'outil du CEDEFOP: Skills-OVATE | CEDEFOP (europa.eu).

3.1.L'objectif

Afin de relever le défi consistant à apporter une solution au problème des compétences en matière de cybersécurité et à remédier à la pénurie sur le marché du travail, la Commission propose, dans le contexte de l'Année européenne des compétences, de mettre en place une **académie des compétences en matière de cybersécurité**, comme l'a annoncé la présidente de la Commission européenne dans sa lettre d'intention sur l'état de l'Union 2022[41, 42].

L'académie des compétences en matière de cybersécurité (ci-après l'«académie») vise à créer un **point d'entrée unique et des synergies** pour les offres d'éducation et de formation en matière de cybersécurité ainsi que des possibilités de financement et des actions spécifiques en vue de soutenir le développement des compétences dans ce secteur. Elle permettra d'étendre la portée des initiatives des parties prenantes afin d'atteindre la masse critique qui aura une incidence sur le marché du travail, y compris pour la défense. Ces activités seraient alignées sur des objectifs communs et des indicateurs clés de performance afin d'avoir un effet plus important.

L'académie mettra l'accent sur le renforcement des compétences des **professionnels de la cybersécurité**. Les activités de l'académie permettront d'orienter les politiques de l'UE en matière de cybersécurité, de même que l'éducation et l'apprentissage tout au long de la vie. Cette initiative vient compléter les deux recommandations du Conseil relatives à l'éducation et aux compétences numériques que la Commission propose simultanément à la présente communication[43].

L'académie reposera sur quatre piliers: 1) favoriser l'**acquisition de connaissances par l'éducation et la formation** en travaillant à l'élaboration d'un cadre commun pour les profils de rôle en matière de cybersécurité et les compétences associées, améliorer l'offre d'éducation et de formation au niveau européen afin de répondre aux besoins, proposer des parcours de carrière et apporter de la visibilité et de la clarté sur les formations et les certifications en matière de cybersécurité dans le but de renforcer l'offre de main-d'œuvre; 2) assurer une meilleure canalisation et une plus grande visibilité des **possibilités de financement** disponibles pour les activités liées aux compétences afin de maximiser leurs résultats; 3) inviter les parties prenantes à **prendre des mesures**; et 4) définir des indicateurs afin de **suivre l'évolution du marché** et de pouvoir évaluer l'efficacité de leurs actions.

Pour sa mise en œuvre, l'académie bénéficiera d'un financement de 10 millions d'EUR au titre du programme pour une Europe numérique[44].

3.2.La gouvernance de l'académie

À terme, afin de fournir une infrastructure servant de **point d'entrée unique** pour favoriser la coopération entre les universités, les prestataires de formation et l'industrie, où l'offre et la demande dans l'écosystème de la cybersécurité de l'UE pourraient se rencontrer et se former, l'académie pourrait prendre la forme d'un **consortium pour une infrastructure numérique**

[41] Lettre d'intention sur l'état de l'Union 2022 adressée à la présidente Roberta Metsola et au premier ministre Petr Fiala.

[42] Communication au Parlement européen et au Conseil – La politique de cyberdéfense de l'UE, JOIN(2022) 49 final.

[43] Propositions de recommandations du Conseil sur les principaux facteurs favorisant la réussite de l'éducation et de la formation numériques et sur l'amélioration de l'offre de compétences numériques dans le domaine de l'éducation et de la formation.

[44] Règlement (UE) 2021/694 du Parlement européen et du Conseil du 29 avril 2021 établissant le programme pour une Europe numérique et abrogeant la décision (UE) 2015/2240.

européenne (EDIC)[45]. Cet instrument permettrait aux États membres d'œuvrer ensemble pour remédier à la pénurie de compétences dans le secteur de la cybersécurité, de travailler en étroite collaboration avec la Commission, l'ENISA et le Centre de compétences européen en matière de cybersécurité (ECCC), conformément à leurs mandats et compétences, et d'associer toutes les parties prenantes concernées, mais aussi d'orienter des investissements européens, nationaux et privés vers un objectif commun. À cette fin, les États membres intéressés sont encouragés à présenter à la Commission, au plus tard le 30 mai 2023, une notification préalable de leur future demande de création d'un EDIC. Grâce à cette notification préalable volontaire, la Commission devrait pouvoir formuler des observations précoces sur le projet de demande de création d'un EDIC, ce qui permettra de le développer ultérieurement et de le présenter formellement de manière plus rapide. Tout au long du processus et dans la mesure requise par les États membres, la Commission, qui agit en tant qu'accélérateur de projets multinationaux, facilitera la préparation de la demande de création d'EDIC. Après l'évaluation positive de la demande par la Commission et l'approbation du comité du programme pour la décennie numérique, la Commission publiera une décision établissant l'EDIC et contribuera ensuite à coordonner la mise en œuvre de l'EDIC[46].

Entre-temps, et pendant la mise en place formelle de l'EDIC, la Commission créera un point d'entrée unique virtuel en renforçant sa **plateforme des compétences et des emplois numériques**[47] avec le soutien du projet de communauté européenne en matière de cybersécurité (ECCO)[48].

L'**ENISA** contribuera à la mise en œuvre de l'académie conformément aux objectifs de l'agence[49], notamment en ce qui concerne l'assistance dans le domaine de l'éducation et de la formation en matière de cybersécurité, et en tenant compte des obligations d'information qui lui incombent au titre de la directive SRI 2[50]. L'**ECCC** travaillera dans le respect de son programme stratégique pour soutenir la mise en œuvre de l'académie des compétences en matière de cybersécurité. Il mettra notamment en œuvre le troisième objectif stratégique (cybersécurité) du programme pour une Europe numérique. Il bénéficiera du soutien de la Commission et des États membres, par l'intermédiaire des **centres nationaux de coordination**. Le **groupe de coopération** institué en vertu de la directive SRI 2[51] sera sollicité le cas échéant. Enfin, il sera nécessaire de s'allier à l'**industrie** et au **monde universitaire** pour atteindre l'objectif de l'académie de remédier à la pénurie de compétences dans le secteur de la cybersécurité.

---

[45] Les EDIC ont été établis aux articles 13 et suivants de la décision (UE) 2022/2481 du Parlement européen et du Conseil du 14 décembre 2022 établissant le programme d'action pour la décennie numérique à l'horizon 2030.

[46] Ibidem, article 12

[47] Accueil | Digital Skills and Jobs Platform (Plateforme des compétences et des emplois numériques) (europa.eu)

[48] Voir Centre et réseau européens de compétences en matière de cybersécurité: nouveau projet financé par l'UE pour soutenir la cybercommunauté (europa.eu). En décembre 2022, la Commission européenne a signé un contrat de 3 millions d'EUR afin de soutenir la cybercommunauté de l'UE dans le cadre du Centre de compétences européen en matière de cybersécurité. Ce projet contribuera à la réalisation des objectifs de l'UE axés sur le renforcement des communautés et des compétences dans les domaines de la recherche et de l'innovation en matière de cybersécurité, du recours à la cybersécurité et de la base industrielle en la matière.

[49] «L'ENISA soutient le renforcement des capacités et contribue à l'état de préparation au sein de l'Union en aidant les institutions, organes et organismes de l'Union, ainsi que les États membres et les parties prenantes des secteurs public et privé, […] et à développer des aptitudes et des compétences dans le domaine de la cybersécurité.» Article 4, paragraphe 3, du règlement sur la cybersécurité.

[50] Article 18 de la directive SRI 2.

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

4. Acquisition de connaissances et formation: établir une approche commune de l'UE en matière de formation à la cybersécurité

Dans le cadre du pilier de l'académie des compétences en matière de cybersécurité sur l'acquisition de connaissances et la formation, une approche structurée sera mise au point dans le but clairement énoncé d'accroître le **nombre** de personnes disposant de compétences en matière de cybersécurité au sein de l'UE, afin de mieux axer les formations sur les **besoins du marché** et de donner de la visibilité aux **parcours de carrière**.

4.1. Utiliser le même langage: une approche commune des profils de rôle en matière de cybersécurité et des compétences associées

L'ENISA a déjà entrepris de définir les profils de rôle des professionnels de la cybersécurité dans le cadre européen de compétences en matière de cybersécurité (**ECSF**)[52]. L'académie devrait s'en inspirer pour définir et évaluer les compétences pertinentes, suivre l'évolution de la pénurie de compétences et fournir des indications sur les nouveaux besoins. Pour chaque rôle en matière de cybersécurité figurant dans l'ECSF, un ensemble de compétences applicables, issues du référentiel européen des compétences informatiques[53] est intégré dans la description du profil[54].

L'ENISA passera donc en revue l'ECSF et **déterminera l'évolution des besoins et des insuffisances en matière de compétences** au niveau de la main-d'œuvre dans le domaine de la cybersécurité, notamment au moyen d'outils avancés (par exemple, l'intelligence artificielle, les mégadonnées[55] et l'exploration de données). À cette fin, l'ENISA travaillera sous le pilotage de l'EDIC, dès que celui-ci sera établi, et de l'ECCC, avec l'appui des centres nationaux de coordination, de la Commission, du projet ECCO et des acteurs du marché[56]. En ce qui concerne la main-d'œuvre de la cyberdéfense, l'ENISA tiendra dûment compte du travail réalisé par le CESD. De même, dans le domaine de la lutte contre la cybercriminalité, l'ENISA prendra en considération les activités menées par l'Agence de l'UE pour la formation des services répressifs (CEPOL) et Europol dans la mise en place d'une analyse des besoins de formation opérationnelle[57] sur les cyberattaques.

L'ECSF sera régulièrement complété et réexaminé dans le cadre de l'académie sur un cycle de deux ans. En outre, la Commission et le Service européen pour l'action extérieure contribueront à définir des profils spécifiques et des compétences associées pour les secteurs

---

[52] Cadre européen de compétences en matière de cybersécurité (ECSF) – ENISA (europa.eu). L'ECSF soutient la détermination et l'articulation des tâches, des compétences, des aptitudes et des connaissances associées aux rôles des professionnels européens de la cybersécurité. Il regroupe tous les rôles liés à la cybersécurité dans des profils, qui font l'objet d'une analyse distincte dans le détail de leurs responsabilités, compétences, synergies et interdépendances correspondantes.

[53] Référentiel européen des compétences informatiques (e-CF) |. Esco (europa.eu). L'e-CF fournit des liens cohérents dans le contexte des certifications en matière de TIC et d'autres cadres pertinents pour le secteur, notamment DigComp.

[54] Voir à cet égard le Manuel de l'utilisateur – Cadre européen de compétences en matière de cybersécurité (ECSF) – septembre 2022.

[55] Voir, par exemple, l'outil Skills-OVATE, mis au point par le Cedefop.

[56] L'agence s'appuiera également sur les résultats d'autres projets financés par l'UE [par exemple, REWIRE, Data Space For Skills (DS4S), CyberSecPro, Concordia] et sur des méthodes issues d'initiatives comparables [par exemple, «Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom and United States» (Création d'une main-d'œuvre qualifiée dans le domaine de la cybersécurité dans cinq pays: contributions de l'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis), rapport de l'OCDE publié le 21 mars 2023] afin de garantir à l'avenir une vision actualisée des besoins dans un environnement où la demande ne cesse d'évoluer.

[57] CEPOL Operational Training Needs Assessment (analyse des besoins de formation opérationnelle) (OTNA).

en fonction des besoins, avec le soutien d'agences et d'organismes de l'UE, comme le CESD [58], Europol et le CEPOL[59].

Des liens seront également établis entre l'ECSF et les instruments pertinents de la politique de l'emploi de l'UE[60]. Les profils d'emploi de l'ECSF ainsi que les compétences liées à l'emploi seront notamment intégrés dans la **classification de l'ESCO**. Cette démarche améliorera la classification et les liens entre les professions et les compétences dans le domaine de la cybersécurité, ce qui facilitera le perfectionnement et la reconversion professionnels et permettra de soutenir la mise en adéquation de l'offre et de la demande d'emploi et la mobilité transfrontalière.

4.2. Favoriser la coopération pour concevoir des programmes d'éducation et de formation en matière de cybersécurité

Dès que l'EDIC sera mis en place, l'académie devrait recevoir le soutien des États membres pour devenir un **lieu de référence en Europe en matière de conception et d'offre de formations dans le domaine de la cybersécurité** traitant des compétences les plus demandées et proposer à des jeunes pousses et des PME ainsi qu'à des administrations publiques des formations sur le tas et des possibilités de stages dans des entreprises innovantes en matière de cybersécurité et dans des centres de compétences en cybersécurité. L'EDIC devrait collaborer avec toutes les parties prenantes concernées, y compris l'industrie, afin de mettre au point ces types de formation, et s'appuyer sur des projets comme **CyberSecPro**[61], qui est financé dans le cadre du programme pour une Europe numérique et qui réunit 17 établissements d'enseignement supérieur et 13 entreprises de sécurité de 16 États membres afin de constituer une pratique exemplaire pour tous les programmes de formation en matière de cybersécurité.

L'académie collaborera avec toutes les parties prenantes concernées afin d'**inciter les jeunes générations** à embrasser des carrières dans le domaine de la cybersécurité. Conformément à la proposition de recommandation du Conseil relative à l'amélioration de l'offre de compétences numériques dans le domaine de l'éducation et de la formation, les États membres devraient établir et renforcer des mesures visant à recruter et à former des enseignants et des formateurs spécialisés et faciliter l'acquisition de compétences en matière de cybersécurité, notamment au moyen de stages d'apprentissage. Il convient d'encourager l'intégration de la cybersécurité dans les programmes d'éducation et de formation, tout en veillant à assurer leur accessibilité, à développer l'offre d'**apprentissages** et de stages, à favoriser des approches innovantes comme des «jeux sérieux» et des plateformes partagées de simulation , à organiser des semaines d'immersion à des postes dans le secteur de la cybersécurité et à expliquer les profils de rôle non techniques. Il y a lieu également de soutenir la participation des groupes difficiles à atteindre, comme les jeunes handicapés, les

[58] Voir à cet égard la communication au Parlement européen et au Conseil – La politique de cyberdéfense de l'UE, JOIN(2022) 49 final.

[59] À cet égard, une attention particulière sera accordée aux travaux effectués sur le Cybercrime Training Competency Framework (cadre de compétences de formation à la cybercriminalité) (TCF) en cours d'élaboration.

[60] Comme la classification européenne des aptitudes, compétences, certifications et professions (ESCO), Europass, le réseau européen de coopération des services de l'emploi (EURES).

[61] CyberSecPro permettra, par exemple, de réaliser une analyse des programmes, des cours et des écoles d'été en matière de cybersécurité proposés dans les universités ainsi que des tableaux de notation utilisés dans le système européen de transfert et d'accumulation de crédits (ECTS), d'assurer la participation de plus de 530 stagiaires sur une période de trois ans et de former des personnes externes de différents secteurs et industries.

jeunes vivant dans des zones reculées ou rurales et les jeunes issus d'autres groupes minoritaires, à ces possibilités d'apprentissage en matière de cybersécurité.

La Commission continuera de soutenir le développement des microcertifications et des programmes d'enseignement et de formation professionnels. En particulier, des **programmes communs de licence et de master, des cours ou des modules communs susceptibles de déboucher sur des microcertifications** et des **programmes intensifs hybrides**[62] sur tous les sujets, y compris **la cybersécurité**, continueront d'être financés au titre du programme Erasmus+. Un soutien sera également apporté à la poursuite du déploiement de l'**initiative «universités européennes»**[63] et des **centres d'excellence professionnelle**[64] afin d'encourager une plus grande coopération entre l'enseignement supérieur et les établissements d'enseignement et de formation professionnels concernés dans toute l'Europe. Les programmes de financement de l'UE, y compris Erasmus+ et le programme pour une Europe numérique, contribueront à cet objectif de renforcement de la coopération, tout comme les fonds de l'UE en faveur du développement de **comptes de formation individuels**[65].

Dans le but de faciliter la coopération, au niveau national, des universités et des prestataires de formations sur les compétences en matière de cybersécurité avec les employeurs des secteurs privé et public et de favoriser des synergies entre les secteurs public et privé, les centres nationaux de coordination sont invités à étudier la possibilité de créer des **campus cyber** au sein des États membres. Les campus cyber offriraient des pôles d'excellence au niveau national pour la communauté en matière de cybersécurité et l'académie faciliterait leur mise en réseau ainsi que la coordination de leurs activités.

L'ENISA renforcera également son offre de formation en matière de cybersécurité en procédant à l'alignement de **son catalogue de cours**[66] sur les profils de l'ECSF et en élaborant des modules de formation par profil, ce qui pourrait améliorer les offres de formation des États membres. L'ENISA élargira aussi son **programme de «formation des formateurs»**[67], afin de mieux cibler les besoins professionnels des institutions, des organes et des organismes de l'Union européenne, ainsi que les autorités publiques et les **opérateurs critiques publics et privés** des États membres dans le champ d'application de la directive SRI 2.

En outre, d'autres organismes et organes de l'UE renforceront leur offre de formation en matière de cybersécurité. À titre d'exemple, grâce à la mise en œuvre de la politique de l'UE en matière de cyberdéfense, le **CESD** mettra au point une nouvelle série de cours sur la cybersécurité et alignera certains de ses cours actuels sur l'ECSF. Ces cours conduiront à la certification des acquis d'apprentissage[68]. En collaboration avec la Commission, le CESD étudiera la possibilité d'intégrer les certificats dans le portefeuille numérique EUeID Wallet.

---

[62] Les programmes intensifs hybrides combinent l'apprentissage en ligne avec un séjour de mobilité physique de courte durée.

[63] Initiative «universités européennes» | Espace européen de l'éducation (europa.eu).

[64] Centres d'excellence professionnelle | Erasmus+ (europa.eu).

[65] Conformément à la recommandation du Conseil du 16 juin 2022 relative aux comptes de formation individuels.

[66] Cours de formation – ENISA (europa.eu).

[67] Programme de «formation des formateurs» – ENISA (europa.eu).

[68] Conformément à l'article 20, paragraphe 4, de la décision (PESC) 2020/1515 du Conseil du 19 octobre 2020 instituant un Collège européen de sécurité et de défense, et abrogeant la décision (PESC) 2016/2382.

Le CESD examinera plus en détail la possibilité d'évaluer les mécanismes en matière de compétences à l'aune desquels les certificats seront délivrés. De même, dans le domaine de la lutte contre la cybercriminalité, on cherchera à établir des liens étroits avec l'**académie de lutte contre la cybercriminalité du CEPOL**[69] afin de favoriser les synergies et les complémentarités dans la conception et la mise en œuvre des programmes de formation.

4.3.Créer des synergies et donner de la visibilité aux formations et à la certification en matière de cybersécurité dans les États membres

L'académie devrait aborder la question de la visibilité et des synergies relatives à la formation et à la certification. Ce serait à l'avantage des cybercommunautés de la société civile, de la défense, des services répressifs et de la diplomatie, étant donné que tous ces secteurs ont souvent besoin d'une même expertise, fondée sur des programmes d'études et des acquis d'apprentissage similaires.

L'académie constituerait un **point d'entrée unique** pour les personnes intéressées par une carrière dans le domaine de la cybersécurité. À court terme, cet objectif pourra être atteint grâce au renforcement de la **plateforme de la Commission en faveur des compétences et des emplois numériques**, avec le soutien du projet ECCO. Une section spécifique aux carrières dans le domaine de la cybersécurité permettra de faire le lien avec des outils existants, allant des programmes d'enseignement supérieur aux possibilités de formation, y compris les cours qui débouchent sur des microcertifications et les programmes d'enseignement et de formation professionnels, sans oublier les offres d'emploi. Pour y parvenir, il sera nécessaire de faire référence aux travaux et aux initiatives en cours sur la plateforme ou de s'y intégrer, notamment les travaux et initiatives de l'ENISA qui, en collaboration avec le monde universitaire, a établi une **cartographie des établissements d'enseignement** qui proposent des programmes de cybersécurité. Cette action sera renforcée avec le soutien des centres nationaux de coordination. En outre, deux **registres des formations existantes des secteurs public et privé et des certifications en matière de cybersécurité** seront mis au point et consolidés par l'ENISA avec le soutien des centres nationaux de coordination, de la Commission et du projet ECCO, en collaboration avec les entités qui délivrent des certifications et en s'appuyant également sur d'autres initiatives pertinentes[70]. Ces registres seront en outre intégrés au point d'entrée unique de la plateforme des compétences et des emplois numériques. Les centres nationaux de coordination, dont la mission est notamment de promouvoir et de diffuser des programmes éducatifs en matière de cybersécurité, en profiteront eux aussi[71].

Il est également nécessaire de garantir aux professionnels que les formations qu'ils entreprennent sont de la qualité requise. À cet égard, l'ENISA mettra au point un **projet pilote** afin d'étudier la mise en place d'un système européen d'attestation des compétences en matière de cybersécurité.

---

[69] L'académie de lutte contre la cybercriminalité (Cybercrime Academy) du CEPOL a été créée en 2019 dans le but de mettre en place une plateforme de pointe en vue d'améliorer les connaissances et les capacités informatiques en matière de cybercriminalité en Europe.

[70] Par exemple, l'initiative W4C Academy – Women4Cyber ou le Global Cybercrime Certification project (projet de certification mondiale en matière de cybercriminalité) pour les services répressifs et les autorités judiciaires.

[71] «1. Les centres nationaux de coordination s'acquittent des tâches suivantes: […] g) sans préjudice des compétences des États membres en matière d'éducation et en tenant compte des tâches pertinentes de l'ENISA, nouer un dialogue avec les autorités nationales en ce qui concerne d'éventuelles contributions à la promotion et à la diffusion de programmes éducatifs en matière de cybersécurité», article 7, paragraphe 1, point g), du règlement ECCC. Voir également le considérant 28 s'y rapportant.

En outre, s'il est essentiel de recenser les compétences et les formations et de les associer à un profil de poste, il importe également de veiller à ce que les services de cybersécurité disposent des compétences, de l'expertise et de l'expérience requises, en particulier pour les fournisseurs de services de sécurité gérés dans des domaines comme la réaction aux incidents, les tests de pénétration, les audits de sécurité et les services de conseil. La directive SRI 2 et la proposition de règlement sur la cybersolidarité énoncent des tâches concrètes pour ces fournisseurs de services de sécurité gérés. La Commission propose donc également une **modification ciblée du règlement sur la cybersécurité**[72] afin de permettre la mise en place de systèmes de certification des services de sécurité gérés au niveau de l'UE. Ces systèmes de certification devraient notamment garantir que ce type de services est fourni par du personnel possédant un très haut niveau de connaissances et de compétences techniques dans les domaines concernés.

Les mécanismes d'assurance de la qualité et de reconnaissance des microcertifications[73] facilitent la transparence, la comparabilité et la portabilité des acquis d'apprentissage. Dans la droite ligne de la recommandation du Conseil sur une approche européenne des microcertifications[74], les États membres sont encouragés à inclure dans leurs cadres nationaux de certification les microcertifications de cybersécurité. Cela devrait leur permettre de relier les microcertifications de cybersécurité au cadre européen des certifications[75]. L'infrastructure de justificatifs numériques européens relatifs à l'apprentissage peut délivrer des certifications et microcertifications de cybersécurité signées numériquement. Celles-ci contiennent des données précieuses, notamment sur les résultats d'apprentissage en matière de cybersécurité, et pourront être stockées dans le futur **portefeuille numérique EUeID**[76].

Actions à mener au titre de l'académie

Les États membres et le secteur

- Garantir le soutien au développement et à la reconnaissance des **microcertifications** d'apprentissage en matière de cybersécurité, conformément à la recommandation du Conseil sur une approche européenne des microcertifications.
- Inclure les certifications de cybersécurité, y compris les microcertifications, dans les **cadres nationaux de certification.**
- Offrir des **possibilités de formation sur le tas** par l'intermédiaire de programmes d'apprentissage à destination des personnes qui participent à des initiatives de développement des compétences en matière de cybersécurité.

La Commission

- À court terme, créer **un point d'entrée unique** pour les programmes en matière de

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

[73] Par exemple, l'enregistrement ou les certificats des acquis d'apprentissage obtenus à l'issue de formations courtes.

[74] Recommandation du Conseil sur une approche européenne des microcertifications pour l'apprentissage tout au long de la vie et l'employabilité.

[75] Recommandation du Conseil du 22 mai 2017 concernant le cadre européen des certifications pour l'apprentissage tout au long de la vie et annulant la recommandation du Parlement européen et du Conseil du 23 avril 2008 établissant le cadre européen des certifications pour l'éducation et la formation tout au long de la vie.

[76] Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique.

cybersécurité, les formations existantes et les certifications de cybersécurité par l'intermédiaire de la **plateforme des compétences et des emplois numériques** avant la fin de 2023.

- Proposer une modification du **règlement sur la cybersécurité** afin de permettre la certification des fournisseurs de services de sécurité gérés le 18 avril 2023.

Les organes et organismes de l'Union européenne

- Mettre en place l'**ECSF** en tant qu'approche commune des profils de rôle en matière de cybersécurité et des compétences associées d'ici la fin de 2023.
- L'ENISA doit amorcer le développement d'un projet pilote portant sur la création d'un **système européen d'attestation** des compétences en matière de cybersécurité au deuxième trimestre de 2023.
- L'ENISA doit revoir son **catalogue de cours** et ouvrir son **programme de «formation des formateurs»** aux opérateurs critiques publics et privés avant la fin de 2023.
- Terminer l'**alignement des programmes du CESD sur l'ECSF** d'ici la mi-2023.

5. Participation des parties prenantes: l'engagement de remédier à la pénurie de compétences dans le secteur de la cybersécurité

Dans le cadre de l'académie, une approche coordonnée de la participation des parties prenantes sera élaborée afin de remédier à la pénurie de compétences dans le secteur de la cybersécurité. L'objectif sera de maximiser la visibilité et l'impact des différents engagements des parties prenantes en vue de réduire la pénurie de compétences dans le secteur de la cybersécurité.

La Commission invite les parties prenantes à prendre des engagements concrets, notamment pour ce qui est de promouvoir le perfectionnement et la reconversion professionnels des travailleurs au moyen d'actions spécifiques, en s'appuyant dans la mesure du possible sur la pénurie de compétences constatée dans le secteur de la cybersécurité. Les **engagements des parties prenantes en matière de cybersécurité** devraient être communiqués sur la **plateforme des compétences et des emplois numériques**, de la même façon que d'autres engagements dans le domaine du numérique déjà visibles sur la plateforme. La Commission encourage également les parties prenantes à prendre un engagement en matière de cybersécurité sur la plateforme afin de participer au **partenariat à grande échelle en matière d'écosystème numérique lancé dans le cadre du pacte pour les compétences**[77]. Les parties prenantes sont encouragées à présenter, sur la plateforme des compétences et des emplois numériques, les engagements en matière de cybersécurité qu'elles ont pris dans le cadre du partenariat à grande échelle en matière d'écosystème numérique. De même, les parties prenantes sont invitées à présenter un rapport sur les engagements qu'elles ont formulés dans le cadre de la plateforme des compétences et des emplois numériques, au titre du partenariat à grande échelle en matière d'écosystème numérique découlant du pacte pour les compétences.

[77] Lancement de nouveaux partenariats européens pour concrétiser les ambitions de l'UE pour la décennie numérique | Bâtir l'avenir numérique de l'Europe (europa.eu), partenariats créés dans le cadre du pacte pour les compétences afin de remédier à la pénurie relative aux technologies de l'information et de la communication (TIC).

La Commission invite en outre les États membres à **poursuivre leurs efforts en vue de mettre en œuvre la déclaration sur les femmes dans le numérique**[78] afin d'encourager les femmes à jouer un rôle actif et de premier plan dans le secteur des technologies numériques et à parvenir à une parité entre les hommes et les femmes dans les postes de cybersécurité. La Commission encourage également les États membres à opérer des synergies avec leurs programmes dans le cadre du **Fonds social européen plus** (FSE+) afin de continuer à soutenir l'objectif d'égalité entre les hommes et les femmes au niveau de la participation au marché du travail[79], par exemple grâce à la mise en place de **programmes de mentorat pour les filles et les femmes.** Ces synergies peuvent favoriser la construction de modèles permettant d'attirer des filles dans des professions du secteur de la cybersécurité, tout en luttant contre les stéréotypes liés au genre. Cela permet également de promouvoir le perfectionnement et la reconversion professionnels des femmes et de favoriser le développement d'une communauté capable de soutenir les femmes dans leur entrée ou leur promotion sur le marché du travail de la cybersécurité.

Les États membres devraient adopter, dans le cadre de leurs **stratégies nationales de cybersécurité, des mesures spécifiques visant à atténuer la pénurie de compétences dans le secteur de la cybersécurité**[80], à recenser et à mieux canaliser les efforts déployés en vue de remédier à la pénurie de compétences et, à terme, à garantir la bonne mise en œuvre de leurs obligations au titre de la directive SRI 2.

Certains États membres exploitent les **synergies entre les initiatives civiles, militaire et répressive**. Il est par exemple possible d'améliorer les compétences en matière de cybersécurité et de cyberdéfense de la population et, en particulier, des jeunes adultes en augmentant le nombre de professionnels du secteur grâce à l'utilisation du service militaire national obligatoire ou au recours à des cyberréservistes, qui sont des citoyens ayant une formation militaire et qui occupent des postes liés à la cybersécurité dans les forces armées[81]. Il en va de même dans le domaine de la **lutte contre la cybercriminalité**, étant donné qu'il existe de nombreuses similitudes entre les efforts généraux en matière de cybersécurité et les activités répressives visant à répondre aux incidents de cybersécurité. La Commission encourage les États membres à débattre de ces initiatives et les invite à examiner comment une main-d'œuvre qualifiée peut servir au mieux les communautés de la cybersécurité civile et de la défense.

La Commission réfléchira à des propositions sur la manière de remédier à la pénurie actuelle et prévue, constatée lors de son examen des besoins des institutions, organes et organismes de l'UE. Elle encouragera en particulier le personnel à tirer parti de la prochaine **bourse UE-États-Unis dans le domaine de la cybersécurité** créée dans le cadre du dialogue entre l'UE et les États-Unis.

Actions à mener au titre de l'académie

Le secteur

[78] Les pays de l'UE s'engagent à stimuler la participation des femmes au domaine numérique | Façonner l'avenir numérique de l'Europe (europa.eu).

[79] Règlement (UE) 2021/1057 du Parlement européen et du Conseil du 24 juin 2021 instituant le Fonds social européen plus (FSE+) et abrogeant le règlement (UE) nº 1296/2013; article 4, paragraphe 1, point c).

[80] Article 7, paragraphe 2, point f), de la directive SRI 2.

[81] Rapport – «Cyber Conscription: Experience and Best Practice from Selected Countries» (Cyberconscription: expérience et bonnes pratiques des pays sélectionnés), Martin Hurt et Tiia Sõmer, International Centre for Defence and Security, février 2021.

- Proposer des **engagements concrets en matière de cybersécurité** sur la plateforme des compétences et des emplois numériques à partir du 18 avril 2023.

Les États membres

- Inclure dans les **stratégies nationales en matière de cybersécurité** des mesures spécifiques visant à remédier à la pénurie de compétences dans le secteur de la cybersécurité.

Les États membres et le secteur

- Mettre en œuvre la déclaration sur les femmes dans le numérique afin de parvenir à une **parité entre les hommes et les femmes dans les postes de cybersécurité** d'ici à 2030.

6. Financement: créer des synergies pour que les dépenses consacrées au développement des compétences en matière de cybersécurité aient le plus grand impact possible

Dans le cadre de l'académie, il est possible de maximiser l'impact des investissements réalisés dans le domaine des compétences en matière de cybersécurité en prévoyant un point d'entrée commun, en facilitant une meilleure canalisation des fonds en fonction des besoins du marché et en exploitant au maximum les financements, en favorisant les synergies entre les différents instruments et en veillant à éviter toute répétition inutile d'activités[82].

6.1. Faire en sorte que les fonds correspondent aux besoins

Dans le cadre de l'académie, l'ECCC, avec le soutien de la Commission, du projet ECCO et des centres nationaux de coordination, recueillera des **informations sur la manière dont les fonds sont utilisés pour financer les compétences en matière de cybersécurité**, et évaluera dans quelle mesure les fonds de l'UE contribuent à réduire la pénurie de compétences dans le secteur de la cybersécurité. En tenant compte des informations recueillies, l'ECCC s'efforcera de mieux canaliser les fonds de l'UE en fonction des besoins recensés. Il financera des actions qui permettront de combler les lacunes les plus pressantes au niveau de la main-d'œuvre en matière de cybersécurité, y compris celles qui sont liées à la mise en œuvre des besoins de la politique en matière de cybersécurité.

6.2. Donner de la visibilité aux fonds disponibles et aux initiatives de partenariat pour les compétences en matière de cybersécurité

À court terme, la **plateforme des compétences et des emplois numériques** constituera le point d'entrée unique où les parties prenantes pourront avoir accès à toutes les informations disponibles sur les possibilités de financement pour les compétences en matière de cybersécurité.

L'UE investit dans le capital humain et dans ses compétences et se sert de partenariats, notamment avec l'industrie, pour susciter des actions en faveur du perfectionnement et de la reconversion professionnels au moyen de plusieurs instruments recensés dans le cadre de la

[82] Possibilités de financement (europa.eu). Les services de soutien du pacte pour les compétences fournissent un point d'entrée unique en vue d'obtenir des informations sur le financement des compétences, y compris pour l'écosystème numérique. Les services de soutien du pacte fournissent des informations générales sur les instruments de financement qui ne ciblent pas spécifiquement les compétences en matière de cybersécurité. Leur travail devrait toutefois être pris en considération par l'académie afin d'éviter toute répétition inutile d'activités

stratégie européenne en matière de compétences[83], en particulier le **pacte pour les compétences**[84] et le **plan d'éducation en matière d'éducation numérique**[85]. Le **programme pour une Europe numérique** permet de financer des possibilités dans le domaine des compétences en matière de cybersécurité, notamment au moyen de projets multinationaux, en nette complémentarité avec le soutien apporté par le programme Horizon Europe à la recherche et à des solutions technologiques innovantes dans le domaine de la cybersécurité. Le **Fonds européen de la défense**[86] permet de financer la recherche et le développement technologique en vue de mener des cyberopérations efficaces, notamment des formations et des exercices[87]. **Le programme Erasmus+** continuera de soutenir de telles initiatives, au moyen, entre autres, de programmes intensifs hybrides et de projets de coordination.

Les États membres sont encouragés à utiliser les fonds de l'UE qu'ils gèrent directement afin de soutenir les compétences et les emplois dans le domaine de la cybersécurité. Les fonds de la politique de cohésion, comme le **Fonds européen de développement régional (FEDER)** et le **Fonds social européen plus (FSE+)** présentent un immense potentiel de synergies à cet égard[88]. Le champ d'application des actions menées au titre de la **facilité pour la reprise et la résilience** (FRR)[89] et du programme **InvestEU**[90] présente d'autres complémentarités essentielles au niveau de la réalisation des objectifs de l'académie.

Actions à mener au titre de l'académie

Le Centre de compétences européen en matière de cybersécurité et l'ENISA

- **Recenser** les financements européens actuels pour les compétences en matière de cybersécurité et les mettre en adéquation avec les besoins du marché, évaluer l'**efficacité** et déterminer les **priorités** de financement d'ici la fin de 2024.

La Commission

- Créer un **point d'entrée unique** pour les possibilités de financement relatives aux compétences en matière de cybersécurité sur la plateforme des compétences et des emplois numériques avant la fin de 2023.

[83] Stratégie européenne en matière de compétences – Emploi, affaires sociales et inclusion – Commission européenne (europa.eu).

[84] Instruments de financement de l'UE pour le perfectionnement et la reconversion professionnels – Emploi, affaires sociales et inclusion – Commission européenne (europa.eu).

[85] Plan d'action en matière d'éducation numérique 2021-2027.

[86] Règlement (UE) 2021/697 du Parlement européen et du Conseil du 29 avril 2021 établissant le Fonds européen de la défense et abrogeant le règlement (UE) 2018/1092.

[87] Les États membres s'engagent dans des formations et des exercices communs, par exemple en mettant en place des projets de formations et d'exercices dans le domaine du cyber dans le cadre de la coopération structurée permanente (CSP) et en y participant, notamment l'académie et la plateforme d'innovation de l'UE dans le domaine du cyber (EU CAIH) et les fédérations de plateformes de simulation cyber.

[88] Article 3, paragraphe 1, du règlement (UE) 2021/1058 et article 4, paragraphe 1, point g), du règlement (UE) 2021/1057.

[89] Par exemple, le plan estonien pour la reprise et la résilience prévoit des investissements (10 millions d'EUR) dans les compétences numériques; il envisage notamment de réviser des formations proposées aux experts en TIC et de financer le perfectionnement et le recyclage des spécialistes des TIC dans le domaine de la cybersécurité et contribuera à l'élaboration d'un programme pilote visant à redéfinir le cadre de certification des spécialistes des TIC.

[90] Les parties prenantes (par exemple, les prestataires de formation et les entreprises qui cherchent à organiser ou à améliorer leurs activités de formation en matière de cybersécurité) peuvent s'adresser à la plateforme de conseil InvestEU, qui propose un soutien et une assistance techniques, y compris le renforcement des capacités, aux promoteurs de projets et aux entités, et peuvent aussi consulter le portail InvestEU.

7. Mesure des progrès accomplis: mécanisme de responsabilité intégré

Dans le cadre de l'académie, une **méthode** sera mise au point pour **mesurer les progrès accomplis en vue de remédier à la pénurie de compétences dans le secteur de la cybersécurité**.

7.1. Définir des indicateurs de cybersécurité pour suivre l'évolution du marché du travail en matière de cybersécurité

L'**indice relatif à l'économie et à la société numériques** (DESI) récapitule les indicateurs sur les performances numériques de l'Europe et suit les progrès réalisés par les États membres de l'UE. Dans le cadre de l'académie des compétences en matière de cybersécurité, l'ENISA travaillera en collaboration avec la Commission et le groupe de coopération SRI[91] pour mettre au point des **indicateurs**, notamment en matière d'égalité entre les hommes et les femmes, afin de suivre les progrès accomplis dans les États membres de l'UE pour accroître le nombre de professionnels de la cybersécurité, en consultant également les acteurs du marché concernés et les centres nationaux de coordination. L'ENISA s'appuiera sur la méthodologie du DESI[92] et veillera à ce que les indicateurs soient conformes aux objectifs numériques de l'Europe en ce qui concerne les professionnels des TIC et la parité entre les hommes et les femmes dans le domaine des TIC. La Commission s'emploiera ensuite à intégrer ces indicateurs dans le DESI, afin de permettre un suivi annuel de l'évolution des compétences en matière de cybersécurité et de l'état du marché de l'emploi dans ce domaine.

7.2. Collecter des données et produire des rapports

L'ENISA collectera les données sur les indicateurs avec le soutien du projet ECCO et des centres nationaux de coordination. Sur la base des données recueillies, l'ENISA produira un **rapport annuel** qui contribuera à l'élaboration du rapport sur l'état d'avancement de la décennie numérique[93]; ce rapport et le DESI permettront ensuite d'enrichir l'analyse et les recommandations par pays du **Semestre européen**[94]. En outre, les indicateurs sur les compétences en matière de cybersécurité contribueront au **rapport bisannuel** de l'ENISA sur l'état de la cybersécurité dans l'UE prévu dans la directive SRI 2, qui traite des capacités, de la sensibilisation et de l'hygiène en matière de cybersécurité dans l'ensemble de l'UE.

7.3. Élaborer des indicateurs clés de performance (ICP) pour la cybersécurité

Dans le but de remédier à la pénurie de talents dans le secteur de la cybersécurité de l'UE, l'ENISA travaillera en étroite collaboration avec la Commission et les centres nationaux de coordination afin de proposer des ICP à la Commission, en s'appuyant sur la méthodologie décrite dans le programme d'action pour la décennie numérique 2030, ainsi que sur l'expérience de l'industrie. L'ENISA tiendra dûment compte des ICP utilisés par les États membres pour évaluer leurs stratégies nationales en matière de cybersécurité[95].

---

[91] Pour ce faire, elle s'appuiera sur la méthodologie que l'ENISA mettra au point aux fins du rapport bisannuel de l'agence sur l'état de la cybersécurité dans l'Union conformément à l'article 18, paragraphe 3, de la directive SRI 2.

[92] Voir la note méthodologique de l'indice relatif à l'économie et à la société numériques (DESI) 2022, disponible à la page suivante: L'indice relatif à l'économie et à la société numériques | Façonner l'avenir numérique de l'Europe (europa.eu).

[93] Décision (UE) 2022/2481 du Parlement européen et du Conseil du 14 décembre 2022 établissant le programme d'action pour la décennie numérique à l'horizon 2030.

[94] Ibidem, considérant 25

[95] Article 7, paragraphe 4, de la directive SRI 2.

<u>Actions à mener au titre de l'académie</u>

L'ENISA

- Préparer des **indicateurs et des ICP** sur les compétences en matière de cybersécurité d'ici la fin de 2023.
- **Recueillir des données** sur les indicateurs et en rendre compte, une première collecte étant prévue d'ici à 2025.

La Commission

- Œuvrer à l'intégration des **indicateurs sur la cybersécurité dans le DESI** ainsi que dans le **rapport sur l'état d'avancement de la décennie numérique**.

8. Conclusion

La présente communication jette les bases d'une refonte de l'approche de l'UE visant à renforcer les compétences des professionnels en matière de cybersécurité au sein de l'UE. L'objectif est de réduire la pénurie de compétences dans le secteur de la cybersécurité et de doter l'UE de la main-d'œuvre nécessaire pour qu'elle puisse réagir à l'évolution constante du paysage des menaces, mettre en œuvre les politiques qui lui permettront de se protéger contre les cyberattaques, mais aussi stimuler les débouchés commerciaux et la compétitivité. Les communautés **civile, militaire, diplomatique et répressive** peuvent tirer profit d'une main-d'œuvre qualifiée dans le domaine de la cybersécurité, qui favorisera les synergies entre elles.

La Commission invite les États membres et toutes les parties prenantes à concrétiser cette idée d'académie des compétences en matière de cybersécurité.