COMMISSION
EUROPÉENNE

Bruxelles, le 20.1.2026
COM(2026) 9 final

RAPPORT DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

sur l'évaluation de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) et du cadre européen de certification de cybersécurité

{SWD(2026) 2 final}

1. INTRODUCTION

1.1 À propos de l'ENISA

Créée en 2004, l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) visait initialement à garantir un niveau élevé de sécurité des réseaux et de l'information au sein de l'UE ainsi qu'à forger une culture de la sécurité dans l'intérêt de ses parties prenantes. Au fil des ans, le mandat et les responsabilités de l'Agence ont considérablement évolué, ce qui lui a permis de suivre la métamorphose rapide de l'environnement de la sécurité numérique en Europe. En réponse à la complexité croissante des défis en matière de cybersécurité, le règlement sur la cybersécurité a élargi le mandat de l'ENISA en 2019 et lui a conféré un statut permanent au sein du cadre institutionnel de l'UE. Ce mandat élargi a renforcé le rôle de l'ENISA dans l'appui à la gestion et à la coordination des efforts en matière de cybersécurité dans l'ensemble de l'UE, rôle principalement axé sur plusieurs domaines clés:

- contribuer à l'élaboration et à la mise en œuvre des stratégies et de la législation de l'UE en matière de cybersécurité;
- renforcer la capacité de l'Union à prévenir et à détecter les incidents en matière de cybersécurité ainsi qu'à y faire face, notamment en fournissant une assistance opérationnelle et technique aux États membres et aux institutions de l'UE;
- favoriser le renforcement des capacités et la coopération en matière de cybersécurité au sein de l'UE;
- sensibiliser aux risques en matière de cybersécurité et promouvoir les bonnes pratiques auprès du grand public, des organisations et des entreprises;
- contribuer à la conception et à la mise en œuvre du cadre européen de certification de cybersécurité, qui vise à réduire la fragmentation du marché et à renforcer la cybersécurité des produits, services et processus des technologies de l'information et de la communication (TIC) dans l'ensemble de l'UE; et
- épauler la coopération avec les partenaires internationaux conformément aux politiques extérieures de l'UE.

Les activités de l'ENISA comprennent désormais des recommandations de base en matière de sécurité, des rapports sur le contexte des menaces, des lignes directrices en matière de normalisation et des études sur les bonnes pratiques dans divers domaines. L'Agence organise des ateliers, des exercices et des programmes de formation afin de consolider l'expertise des professionnels de la cybersécurité et des responsables politiques. En outre, l'ENISA joue un rôle essentiel en répondant aux demandes de la Commission et des États membres, en soutenant les démarches de certification et en fournissant des conseils sur mesure quant à l'élaboration et à la mise en œuvre des stratégies en matière de cybersécurité.

Les résultats attendus de la part de l'ENISA comprennent l'amélioration de la sécurité des réseaux et de l'information au sein de l'UE, le renforcement de la confiance dans le marché unique numérique et la promotion de la coopération en matière de cybersécurité entre les principales parties prenantes en Europe. Alors que l'Europe poursuit sa transformation numérique, les stratégies d'adaptation de l'ENISA garantissent la sécurité et la résilience du paysage numérique de la région, permettant de faire face à des défis tels que les menaces en matière de cybersécurité, les tensions géopolitiques et la fragmentation des politiques entre les États membres.

1.2 À propos du cadre européen de certification de cybersécurité (ECCF)

Le cadre européen de certification de cybersécurité (ECCF) a été mis en place dans le cadre du règlement sur la cybersécurité, avec pour objectif principal d'améliorer l'environnement de la cybersécurité dans l'ensemble de l'Union européenne. L'ECCF est conçu pour créer une approche unifiée et horizontale de la certification de cybersécurité dans tous les États membres, réduisant ainsi la fragmentation au sein du marché intérieur des produits, services et processus dans le domaine des TIC. Ce faisant, il renforce la confiance du marché, favorise la croissance du marché de la cybersécurité de l'UE et garantit la résilience ainsi que des capacités solides en matière de cybersécurité. Le cadre répond à six besoins fondamentaux:

- promouvoir la confiance du marché à l'échelle de l'UE;
- améliorer les mesures de cybersécurité et la résilience en la matière;
- établir des normes de résilience élevées dans les offres du marché;
- renforcer la coopération entre les acteurs de la cybersécurité;
- réduire les charges liées à la certification; et
- sensibiliser les citoyens et les entreprises européens à la cybersécurité.

En outre, l'ECCF cherche à accroître la transparence de l'assurance en matière de cybersécurité en promouvant la sécurité dès la conception et par défaut, ce qui implique d'atténuer la vulnérabilité et de respecter des exigences de sécurité spécifiques.

Pour atteindre ces objectifs, l'ECCF s'appuie sur plusieurs piliers essentiels, la mise au point de schémas européens de certification de cybersécurité étant au cœur de ces efforts. Par l'intermédiaire de ces schémas, le cadre met en avant l'assurance globale en matière de cybersécurité et la résilience dans l'ensemble de l'UE. L'ECCF encourage le développement d'un esprit de communauté qui permettrait d'apporter une contribution cruciale aux parties prenantes et de faciliter la coopération avec les États membres et entre eux. Le règlement sur la cybersécurité impose en outre la consultation publique de toutes les parties prenantes concernées au moyen d'un processus de consultation formel, ouvert, transparent et inclusif, ainsi que la formation de groupes consultatifs ad hoc chargés de recueillir des points de vue et une expertise diversifiés dans le cadre du processus d'élaboration du schéma de certification. L'ENISA joue un rôle central dans l'orchestration de ces efforts en consultant systématiquement les parties prenantes afin de veiller à ce que tous les éléments législatifs soient pris en considération avant de soumettre les schémas candidats finaux à la Commission européenne en vue de leur adoption.

Le contexte de cybersécurité qui sous-tend la création de l'ECCF illustre l'évolution rapide de l'ensemble des menaces, marquée par l'augmentation des cas de cyberattaques exploitant les vulnérabilités et l'insuffisance des pratiques de sécurité, qui s'ajoute à une fragmentation émergente de la certification dans l'UE. Ce contexte confirme la nécessité de la mission de l'ECCF, à savoir garantir l'intégrité, la confidentialité et la disponibilité des données tout au long du cycle de vie des produits, services et processus TIC. Une fois ses activités principales menées à bien, l'ECCF devrait produire plusieurs résultats, y compris des documents relatifs aux schémas, des publications, des événements et des améliorations structurelles à l'appui de la mise en œuvre. Ces efforts visent à favoriser une adoption plus généralisée des certifications de cybersécurité, à rationaliser les processus, à accroître la confiance dans le marché intérieur et à renforcer les capacités des secteurs public et privé.

À l'avenir, les contributions de l'ECCF devraient favoriser la cyberrésilience et la compétitivité de l'UE, en garantissant la sûreté et la fluidité des interactions numériques au sein de l'UE, tout en relevant les défis émergents en matière de cybersécurité. Des incidences majeures sont attendues à moyen et à long terme, avec des résultats favorables subordonnés à des facteurs internes et externes dynamiques, y compris les changements géopolitiques, l'évolution de l'environnement en matière de sécurité et les besoins émergents du marché.

1.3 Objet du présent rapport

Le présent rapport vise à évaluer l'incidence et l'efficacité de l'ENISA et de l'ECCF, compte tenu de l'évolution du contexte technologique et réglementaire. Conformément à l'article 67 du règlement (UE) 2019/881, connu sous le nom de «règlement sur la cybersécurité», la présente évaluation porte non seulement sur le mandat et les activités de l'ENISA, mais aussi sur le rôle de l'ECCF dans la promotion d'un cyberespace sûr dans l'ensemble de l'UE, au 28 juin 2024. Les conclusions présentées sont tirées du rapport d'évaluation préparatoire achevé en décembre 2024.

L'analyse couvre la période 2017-2023 et sert plusieurs objectifs clés. Elle vise principalement à examiner les performances, la gouvernance et les méthodes de travail de l'ENISA et de l'ECCF. Il s'agit pour cela de déterminer dans quelle mesure ces instruments ont atteint leurs objectifs et contribué à l'amélioration de la cybersécurité et du fonctionnement du marché intérieur au sein de l'UE. L'évaluation se concentre sur cinq critères principaux, à savoir l'efficacité, l'efficience, la pertinence, la cohérence et la valeur ajoutée de l'UE, fournissant ainsi un cadre qui permet d'appréhender à la fois ce qu'ont accompli ces deux entités et quels sont les domaines à améliorer.

En examinant ces éléments, le rapport donne un aperçu des ajustements potentiels du mandat de l'ENISA et des stratégies visant à renforcer l'incidence de l'ECCF. En fin de compte, ces évaluations visent à faciliter une prise de décision éclairée en vue de faire progresser la résilience de l'UE en matière de cybersécurité. Le rapport s'articule en plusieurs sections distinctes: une présentation de l'ENISA et de l'ECCF, une analyse des résultats de l'évaluation et une synthèse des conclusions et recommandations.

Le règlement (UE) 2024/2847 (règlement sur la cyberrésilience) a introduit des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques (produits matériels et logiciels, y compris leurs composants lorsqu'ils sont mis sur le marché séparément). Il subordonne leur mise sur le marché de l'Union au respect d'un ensemble d'exigences essentielles en matière de cybersécurité, conformément à l'approche du nouveau cadre législatif de l'Union. Le règlement sur la cyberrésilience est entré en vigueur le 10 décembre 2024 et s'appliquera dans son intégralité à partir du 11 décembre 2027. La proposition de la Commission était accompagnée d'une analyse d'impact complète, qui exposait la raison d'être de l'introduction de telles règles. Compte tenu de ce qui précède et du fait que le règlement sur la cyberrésilience se trouve encore dans sa période de transition, il n'a pas été jugé nécessaire d'évaluer plus avant, dans le présent rapport, le troisième élément visé à l'article 67, paragraphe 3, du règlement sur la cybersécurité, à savoir «s'il est nécessaire de fixer des exigences essentielles en matière de cybersécurité comme condition d'accès au marché intérieur pour empêcher que des produits TIC, services TIC, processus TIC et services de sécurité gérés qui ne satisfont pas aux exigences de base en matière de cybersécurité entrent sur le marché intérieur».

Étant donné que les conclusions du présent rapport sous-tendent les objectifs stratégiques de la révision du règlement sur la cybersécurité, le présent rapport accompagne l'acte législatif et il est donc essentiel de le présenter dans le cadre de cet ensemble de mesures.

2. PRINCIPALES CONCLUSIONS DE L'EVALUATION

2.1 ENISA

La présente section expose les principales conclusions de l'évaluation de l'ENISA, en mettant l'accent sur l'efficacité, l'efficience, la pertinence et la cohérence de l'Agence ainsi que sur la valeur ajoutée qu'elle apporte à l'environnement de cybersécurité de l'UE. En outre, un examen plus approfondi de la gouvernance interne et des pratiques au sein de l'Agence est présenté afin de mettre en lumière sa dynamique opérationnelle et les domaines à améliorer.

Efficacité

Le rapport d'évaluation préparatoire souligne que l'ENISA a rempli son mandat en produisant la quasi-totalité des résultats prévus. Il convient toutefois de mentionner qu'en l'absence d'indicateurs suffisants, l'analyse de l'efficacité repose principalement sur les entretiens et les enquêtes réalisés auprès des parties prenantes. En particulier, dans une période difficile, marquée notamment par la pandémie de COVID-19 et par la guerre d'agression menée par la Russie contre l'Ukraine, l'Agence a fait preuve de flexibilité et les parties prenantes ont fait part d'évaluations positives à son égard. Pendant la pandémie de COVID-19, l'ENISA a soutenu la Commission et les États membres en définissant, dans de brefs délais, des exigences de sécurité adaptées à ce contexte. Elle a également joué un rôle dans la coopération avec l'Ukraine, s'employant à faire en sorte que les attaques n'aient pas de retombées sur les infrastructures et secteurs critiques, tels que l'énergie. L'efficacité de l'ENISA découle d'une structure de gouvernance solide et d'un modèle organisationnel matriciel qui facilite la réalisation des tâches et la coopération. L'ENISA a atteint bon nombre de ses objectifs. Les parties prenantes ont généralement reconnu et apprécié les contributions de l'ENISA au renforcement de la résilience de l'UE en matière de cybersécurité. L'Agence a encouragé la coopération et l'échange d'informations entre les États membres et les autres parties prenantes pour favoriser la réalisation des objectifs de l'UE dans le domaine de la cybersécurité. Les efforts qu'elle a déployés pour faciliter la coopération technique, promouvoir des normes communes en matière de cybersécurité et appuyer les initiatives de renforcement des capacités ont été particulièrement appréciés. . Le rapport d'évaluation indique par ailleurs qu'il est possible d'améliorer la hiérarchisation des tâches dans les méthodes de travail de l'ENISA. En réévaluant l'orientation de ses activités, l'Agence peut tirer parti des cadres existants et des retours d'information des parties prenantes pour améliorer l'accomplissement de ses tâches. Cette démarche est particulièrement cruciale pour répondre aux priorités émergentes sans compromettre les engagements existants. L'investissement sans relâche de l'ENISA en faveur de la participation et de la consultation des parties prenantes est un point fort, mais sa capacité opérationnelle n'est pas étayée par des ressources suffisantes. Une réaffectation plus dynamique des tâches et des ressources permettrait, en partie, de mieux répondre aux nouvelles demandes en temps utile et de renforcer la capacité de l'ENISA à relever les défis en matière de cybersécurité, dans une certaine mesure. L'Agence pourrait mieux atteindre son objectif consistant à préserver et à consolider sa réputation dans le secteur de la cybersécurité en veillant à ce que ses tâches soient alignées non seulement sur ses objectifs stratégiques, mais aussi sur sa capacité opérationnelle. Cette hiérarchisation devrait être facilitée par des efforts de collaboration entre l'ENISA, les États membres et les responsables politiques de l'UE afin de garantir l'alignement des activités sur les objectifs stratégiques et la capacité opérationnelle.

Efficience

Au cours de la période d'évaluation allant de 2017 à 2023, l'ENISA a démontré l'efficience de ses opérations dans le cadre de la structure de gouvernance qu'elle a mise en place. Le cadre d'organisation matriciel a aidé l'ENISA à hiérarchiser ses tâches, à optimiser l'alignement de ses ressources et à favoriser la coopération entre ses différentes unités. Cette approche, associée à une combinaison équilibrée de personnel opérationnel et administratif, lui a permis de mieux exécuter les tâches qui lui ont été confiées. Toutefois, l'ENISA a clairement la possibilité d'accroître son efficience en améliorant la hiérarchisation de ses priorités, la clarté de ses axes de travail et l'allocation stratégique de ses ressources. L'efficience de l'Agence est parfois compromise par des facteurs externes et par la nécessité de rationaliser davantage la gouvernance interne. En interne, l'ENISA a mis au point des solutions innovantes, telles qu'un modèle d'organisation matriciel, afin de coordonner plus efficacement les fonctions opérationnelles et administratives.

Malgré cela, l'évaluation a révélé plusieurs domaines clés dans lesquels l'Agence dispose d'une marge de manœuvre pour améliorer son efficience. Les entretiens avec le personnel de l'ENISA, les enquêtes auprès des parties prenantes et la documentation interne ont montré que l'Agence avait du mal à suivre le rythme des demandes de plus en plus nombreuses et à pourvoir des postes spécialisés, difficulté aggravée par une pénurie mondiale de spécialistes des technologies de l'information. Cette situation a engendré des retards, une redéfinition des tâches prioritaires et des périodes de pression et de charge de travail élevées. Néanmoins, certains ajustements pourraient atténuer ces difficultés. Les récentes décisions stratégiques de réaffectation des ressources humaines témoignent d'une capacité à répondre, dans une certaine mesure, aux changements de priorités. Bien que l'Agence ait bénéficié, en 2022, d'une augmentation budgétaire considérable, de l'ordre de 15 millions d'euros, pour mener son action de soutien à la cybersécurité (Cybersecurity Support Action), cette augmentation n'a pas entraîné de hausse proportionnelle des effectifs. En réalité, environ 10,5 équivalents temps plein (ETP) ont été réaffectés en 2022 pour mettre en œuvre l'action de soutien à la cybersécurité, ce qui montre la capacité qu'a l'Agence d'optimiser ses ressources actuelles lorsque cela s'impose, même si, dans ce cas, les ETP nécessaires à la réalisation de l'action de soutien ont en fait été mobilisés en partie par une passation de marchés et en partie par le personnel chargé de la gestion des contrats, comme le souligne le rapport d'évaluation préparatoire. Les 10,5 ETP ont été réaffectés à partir du programme de travail existant de l'Agence, soit 4 ETP de l'activité 4 (Permettre la coopération opérationnelle), 4 ETP de l'activité 5 (Réaction concertée au niveau de l'Union et des États membres) et 2,5 ETP d'autres activités. Par conséquent, l'ENISA a pris des mesures pour abaisser le niveau de priorité et/ou l'investissement de ressources dans certaines activités en 2023 et réorienté ses ressources humaines vers les tâches opérationnelles découlant notamment des missions concrètes prévues par la législation, ce qui a eu des effets secondaires négatifs pour d'autres tâches moins clairement définies dans le mandat de l'ENISA, par exemple en ce qui concerne les compétences et la sensibilisation.

Des améliorations peuvent également être envisagées en ce qui concerne la gestion du budget. L'Agence a enregistré une tendance à la baisse dans l'équilibrage des crédits approuvés et engagés entre 2019 et 2022 en raison de retards dans des mesures telles que l'action de soutien à la cybersécurité. En inversant cette tendance et en consacrant des efforts à la gestion des dépenses administratives, notamment en remédiant aux retards dans la passation de marchés, il serait possible d'améliorer encore l'efficience interne.

Pertinence

L'ENISA a particulièrement démontré sa pertinence dans le domaine de la cybersécurité par sa réactivité à l'évolution des besoins des parties prenantes et par la flexibilité dont elle a fait preuve pour s'adapter à l'évolution du contexte. L'Agence a constamment démontré sa capacité à réexaminer et à réaligner ses domaines d'action pour faire face aux évolutions émergentes, ce qui lui a permis de demeurer une composante essentielle du cadre de cybersécurité de l'UE. Bien que les parties prenantes soient généralement satisfaites des efforts déployés par l'ENISA, sa pertinence pourrait être renforcée dans certains aspects. Malgré sa nature réactive, l'Agence pourrait améliorer son soutien et accroître sa visibilité dans les différents secteurs et parmi les différentes parties prenantes, en particulier les PME, qui peinent souvent à satisfaire aux exigences en matière de cybersécurité. L'ENISA pourrait accroître son impact en changeant de stratégie pour fournir des outils et des ressources plus directs, adaptés à des secteurs spécifiques, mais aussi des informations et des outils pour faire face aux menaces émergentes. L'approche adoptée par l'Agence pour mobiliser les parties prenantes s'est avérée efficace, se fondant sur des forums, des comités et des groupes de travail pour associer activement des experts nationaux aux activités et aux publications. Toutefois, la complexité de la structure décentralisée au sein de certains États membres a posé des problèmes qui pourraient être atténués par une meilleure organisation et par une coordination plus claire avec les autorités nationales. Les initiatives actuellement menées par l'ENISA, y compris la formulation de lignes directrices en matière de cybersécurité et l'élaboration de programmes de renforcement des capacités, témoignent de sa volonté de favoriser la coopération et de renforcer la position collective de l'UE en matière de cybersécurité. La promotion d'une collaboration plus étroite entre les industries et l'amélioration de l'accès à l'information pourraient remédier à certaines limites perçues par le secteur industriel. Le considérable potentiel d'amélioration de l'ENISA réside dans la réévaluation des priorités, la rationalisation des processus, l'acquisition de nouvelles ressources pertinentes et l'optimisation efficiente des ressources existantes, ce qui consoliderait son rôle fondamental dans l'écosystème européen de la cybersécurité. Grâce à un alignement stratégique sur la stratégie européenne en matière de cybersécurité, les nouvelles priorités de l'ENISA pourraient créer des moyens d'obtenir des contributions plus efficaces. Pour renforcer sa capacité à fournir un appui stratégique et technique, l'Agence pourrait envisager de fournir davantage de ressources, d'être plus sélective dans ses engagements et d'affiner ses domaines d'action prioritaires. En conclusion, bien que la pertinence de l'ENISA soit incontestable, des améliorations sont encore possibles. En redéfinissant ses activités prioritaires, en prévoyant davantage de ressources et en optimisant ses ressources existantes, l'ENISA peut renforcer à la fois son efficacité et son incidence globale, en s'alignant plus étroitement sur les exigences dynamiques de l'environnement européen de la cybersécurité.

Cohérence

Dans l'examen de la cohérence de l'ENISA, l'évaluation met en évidence à la fois des points forts et des domaines à améliorer. L'Agence fait preuve d'un engagement manifeste en faveur de la coopération en matière de cybersécurité au niveau de l'UE, notamment par ses démarches de facilitation et de dialogue direct avec les parties prenantes. Cette double approche a permis à l'ENISA de contribuer considérablement à la formation du cyberespace, en s'alignant sur les cadres législatifs récents. Toutefois, bien que le rôle de facilitatrice et de coordonnatrice endossé par l'ENISA soit positif, plusieurs domaines doivent être améliorés pour renforcer sa cohérence. L'évaluation a révélé la nécessité d'améliorer les synergies entre les responsabilités et les actions

de l'ENISA et celles d'autres organes de l'UE, tels que le Centre de compétences européen en matière de cybersécurité (ECCC), ainsi que celles des autorités nationales chargées de la cybersécurité. Ces rôles sont souvent complémentaires, mais il serait possible de rationaliser davantage les opérations et d'améliorer l'efficacité organisationnelle. En formalisant les accords de coopération avec d'autres entités, telles que l'Agence européenne pour la sécurité maritime (AESM) et le Centre commun de recherche (JRC), l'ENISA pourrait mieux tirer parti des synergies et garantir une approche unifiée des initiatives en matière de cybersécurité. La communication interne et la gestion des ressources au sein de l'ENISA devraient également être affinées. Les interactions entre l'Agence et les parties prenantes privées ainsi que les partenaires internationaux doivent être plus prévisibles et transparentes afin d'entretenir la confiance et de favoriser les efforts de collaboration. Conformément au règlement sur la cyberrésilience et à la directive révisée sur la sécurité des réseaux et des systèmes d'information (SRI 2), délimiter clairement les tâches de l'ENISA en matière d'appui à la mise en œuvre des politiques pourrait renforcer l'efficacité et garantir la cohérence entre les mesures réglementaires. Cette clarté améliorerait également la capacité de l'Agence à répondre aux exigences réglementaires sectorielles. En résumé, si l'ENISA a démontré qu'elle s'appuyait sur une base solide pour promouvoir la cohérence en matière de cybersécurité dans l'UE, elle dispose d'une marge de manœuvre pour redéfinir les priorités dans ses efforts. Cette démarche l'aidera à remplir efficacement son mandat et à s'adapter à l'évolution de l'environnement en matière de cybersécurité. En remédiant aux inefficacités actuelles et en améliorant la coordination entre les agences, l'ENISA pourra continuer à jouer efficacement son rôle crucial au sein du cadre de cybersécurité de l'UE.

Valeur ajoutée européenne

L'ENISA a considérablement contribué au renforcement de l'écosystème de la cybersécurité de l'UE, mais il existe des possibilités d'amélioration qui pourraient amplifier l'incidence de son action. Faisant office de pôle centralisé, l'ENISA a facilité la coopération essentielle dans l'ensemble de l'UE, complété les efforts nationaux, en particulier dans les États membres disposant d'infrastructures de cybersécurité moins développées, et aligné les pratiques et les stratégies en matière de cybersécurité. En tant qu'agence décentralisée de l'UE, l'ENISA a pu, grâce à son mandat spécialisé, consolider son expertise en matière de cybersécurité et dialoguer efficacement avec les États membres, en jouant un rôle central dans le façonnement de l'environnement européen de la cybersécurité. Dans ce contexte, étant donné son rôle consistant à fournir des informations sur les menaces émergentes et à recommander des outils et des stratégies pour y répondre, il est impératif que l'ENISA se concentre sur les États membres. L'Agence pourrait renforcer la coopération internationale, conformément aux priorités de l'Union, y compris avec les partenaires des pays tiers, les organisations internationales et les agences de cybersécurité, afin de mieux faire face au caractère mondial des cybermenaces. En outre, l'ENISA joue un rôle crucial dans la promotion de la certification de cybersécurité et l'appui aux activités de normalisation, qui contribuent à réduire la fragmentation du marché et favorisent des pratiques solides en matière de cybersécurité dans l'ensemble de l'UE. Bien qu'il n'existe pas d'autres organismes similaires ayant l'expertise et la souplesse organisationnelle de l'ENISA, la priorité actuellement accordée par l'Agence aux autorités nationales a suscité des critiques de la part des parties prenantes du secteur privé. D'après les retours d'information des principaux acteurs du secteur, des efforts supplémentaires pourraient être consentis pour adapter les informations aux défis spécifiques du secteur privé. Bien qu'il soit essentiel de se concentrer en premier lieu sur les autorités nationales, un renforcement stratégique de la participation des parties prenantes et de la collaboration

sectorielle pourrait répondre à ces préoccupations. En outre, il serait judicieux de procéder à une réévaluation stratégique du mandat de l'ENISA afin de l'adapter sans heurts à l'évolution des défis en matière de cybersécurité. Cela permettrait à l'Agence de continuer à apporter ses précieuses contributions à l'UE, tout en répondant efficacement aux besoins croissants de ses diverses parties prenantes.

Principales réalisations et principaux défis

L'ENISA est largement reconnue au sein de la communauté de la cybersécurité de l'UE pour sa solide réputation, ses publications de qualité et son rôle important dans la promotion de la coopération entre les États membres et les autres entités compétentes dans le domaine de la cybersécurité. Les travaux de l'Agence qui contribuent à l'harmonisation des exigences en matière de cybersécurité sont essentiels pour établir un niveau de protection cohérent dans tous les États membres et favorisent directement le renforcement des capacités, en particulier pour les petits États membres. Non seulement cette harmonisation garantit un environnement numérique sûr dans l'ensemble de l'UE, mais elle améliore également le niveau de préparation en matière de cybersécurité parmi toutes les parties prenantes.

Toutefois, l'évaluation a mis en évidence plusieurs difficultés rencontrées par l'ENISA. L'Agence n'a pas la flexibilité suffisante pour répondre à l'évolution des menaces en matière de cybersécurité, ce qui peut entraîner des retards dans ses activités. En vue de limiter les problèmes liés aux contraintes en matière de ressources, les parties prenantes consultées[2] ont souligné, entre autres, la nécessité d'améliorer les processus de recrutement et les stratégies de gestion de la charge de travail. Élargir le mandat de l'ENISA afin de renforcer son rôle opérationnel pourrait répondre à ces préoccupations, en permettant à l'Agence d'exploiter les progrès technologiques et d'améliorer les cadres de cybersécurité. Cette restructuration lui permettrait de faire face aux menaces dynamiques de manière proactive, en augmentant son incidence grâce à des initiatives de formation conjointes et à sa contribution aux processus d'élaboration des stratégies.

Enfin, les systèmes de consultation et de gestion des parties prenantes de l'ENISA sont jugés efficaces pour faciliter la gestion des besoins et des attentes de ces parties prenantes, mais une relation plus étroite et plus transparente avec les États membres est nécessaire pour améliorer la coopération et le partage d'informations. Parmi les priorités futures, on peut citer la mise à jour des cadres internes afin de mieux gérer les responsabilités croissantes et les divers défis de l'Agence, en veillant à ce qu'elle puisse exécuter pleinement les tâches qui lui sont confiées compte tenu de ses effectifs.

2.2 ECCF

La présente section expose les principales conclusions de l'évaluation concernant l'ECCF, en mettant l'accent sur son efficacité, son efficience, sa pertinence et sa cohérence ainsi que la valeur ajoutée qu'il apporte au paysage de la cybersécurité de l'UE. En outre, elle résume les principaux points forts et points faibles du cadre, recensés à l'issue d'une analyse de ses forces, faiblesses, opportunités et menaces (SWOT).

Efficacité

L'ECCF a été conçu comme un pilier pour améliorer l'assurance en matière de cybersécurité dans l'ensemble du marché intérieur de l'UE, en vue d'harmoniser la certification des produits, services et processus TIC. Il a été mis en place pour résoudre des problèmes persistants tels que la fragmentation du marché et la nécessité d'accroître la transparence ainsi que la confiance du public dans les solutions numériques. Grâce à son modèle de gouvernance structuré, qui associe des entités telles que l'ENISA, le groupe européen de certification de cybersécurité (GECC) et le réseau des autorités nationales de certification de cybersécurité, l'ECCF a jeté les bases d'une coordination renforcée entre les parties prenantes, y compris les États membres et les entités privées. Toutefois, la réalisation concrète de ces objectifs s'est heurtée à de nombreuses difficultés, qui ont limité l'efficacité du cadre. Une lacune importante de l'ECCF actuel réside dans son incapacité à remédier efficacement à la fragmentation des systèmes de certification dans l'ensemble de l'UE, principalement en raison de limitations d'ordre procédural. Cette fragmentation a persisté malgré la vocation du cadre à harmoniser les processus de certification, ce qui a entraîné des incohérences et de l'inefficacité dans l'assurance en matière de cybersécurité. En témoigne le retard considérable pris dans la mise en œuvre du premier système de certification, un certificat fondé sur des critères communs à l'UE (certificat EUCC), 57 mois ayant séparé la conception de cette initiative et son adoption. Ce retard met en évidence l'inefficacité des processus du cadre, principalement due à la complexité et aux multiples aspects des procédures d'approbation. En outre, l'ambiguïté des responsabilités et de l'obligation de rendre compte entre les parties prenantes a, elle aussi, entravé la capacité du cadre à atteindre ses objectifs. Des facteurs externes ont également compliqué la réalisation des objectifs de l'ECCF. L'évolution du paysage géopolitique, caractérisée par l'augmentation des cybermenaces et des tensions politiques autour de la souveraineté des données et du contrôle numérique, a nécessité des mesures d'adaptation que l'ECCF a peiné à mettre en œuvre rapidement. Ces pressions extérieures ont entraîné des retards dans l'adoption des schémas, à l'instar du schéma européen de certification des services cloud (EUCS), pour lequel les discussions ont été ralenties par des débats non techniques, par exemple sur les exigences en matière de localisation des données. Malgré ces obstacles, le cadre a obtenu des résultats positifs, notamment en ce qui concerne la sensibilisation de tous les États membres à l'importance et aux complexités de la certification de cybersécurité. La pandémie de COVID-19, si elle a provoqué des retards opérationnels, a également mis en évidence la nécessité de disposer d'infrastructures numériques résilientes, plaçant la cybersécurité au cœur des débats stratégiques. La COVID-19 a eu une influence à la fois négative et positive sur l'ECCF. Du côté «négatif», le passage soudain à l'organisation des réunions en ligne a retardé les processus d'élaboration des schémas. Du côté «positif», la pandémie de COVID-19 a sensibilisé à l'importance de mettre en place des chaînes d'approvisionnement résilientes et moins dépendantes des pays tiers. En outre, l'analyse a fait ressortir certains enseignements essentiels, révélant une allocation inégale des ressources entre les parties prenantes, y compris les États membres, qui entrave l'élaboration et la mise en œuvre uniformes des schémas de certification. Il est essentiel de remédier à ces disparités pour garantir l'efficience et l'efficacité futures du cadre, notamment en conservant le personnel spécialisé au sein de l'ENISA et en favorisant un dialogue permanent entre toutes les parties concernées.

Efficience

L'efficience de l'ECCF a fait l'objet d'un examen particulier en raison la durée des délais nécessaires à l'adoption des schémas de certification de cybersécurité et de la myriade de complexités en jeu. Malgré son objectif stratégique consistant à rationaliser le processus de

certification dans l'ensemble de l'UE, l'efficience de l'ECCF a notamment été entravée par la longueur excessive des discussions et des phases de préparation, qui a engendré des retards importants: le premier schéma n'a été adopté qu'au début de l'année 2024, soit près de cinq ans après la mise en œuvre du cadre. Ces longs délais peuvent être attribués à des difficultés multidimensionnelles qui revêtent à la fois des dimensions politiques et des dimensions techniques.

Les difficultés politiques, y compris la politisation des débats sur les exigences en matière de certification, ont entravé les progrès en créant un environnement peu propice à la transparence et à la communication. Par exemple, la création du schéma européen de certification des services cloud (EUCS) a été fortement influencée par les débats sur les exigences en matière de souveraineté des données, subissant les pressions politiques de pays tiers et de l'industrie en dehors de l'UE; le discours technique a ainsi cédé la place à un discours politique au sein du GECC.

Les complexités techniques ont également été des sources d'inefficacité, et notamment la difficulté de traduire les projets de schémas en actes juridiques, compte tenu de la nature diversifiée et exigeante des produits/services soumis à certification, tels que la 5G et l'informatique en nuage. Les demandes de grande envergure et l'absence de normes établies dans certains domaines ont ajouté des niveaux de difficulté aux démarches de préparation et d'adoption, obligeant de nombreuses parties prenantes à s'aligner sur les stratégies et pratiques existantes à de nombreuses étapes. Malgré ces exemples d'inefficacité, plusieurs éléments positifs sont ressortis du cadre. La création de groupes et de forums spécialisés, y compris le groupe européen de certification de cybersécurité (GECC), le groupe de travail ad hoc (GTAH) consacré à certains schémas particuliers et le groupe des parties prenantes pour la certification de cybersécurité (GPPCC), a facilité la participation nécessaire des parties prenantes. Néanmoins, d'importants éléments restent encore à améliorer pour garantir le fonctionnement optimal de ces structures: par exemple, les membres du GPPCC ont estimé que la participation de leur groupe à l'ECCF était insuffisante. Il est essentiel d'affiner la gouvernance interne pour assurer la participation active et la contribution stratégique des parties prenantes.

Pertinence

L'ECCF apparaît comme une réponse essentielle à la complexité et à la sophistication croissantes des cybermenaces dans l'ensemble de l'UE, aspirant à mettre en place des schémas de certification de cybersécurité harmonisés qui garantissent la confiance et favorisent un marché numérique sûr. Malgré ce postulat prometteur, la pertinence du cadre est toujours considérée comme étant davantage potentielle que pratique, les schémas de certification n'étant entrés que récemment dans leur phase opérationnelle. Les retards dans l'obtention de résultats tangibles révèlent des disparités en matière d'exécution et jettent l'incertitude sur la position actuelle de l'ECCF dans le paysage de la cybersécurité. L'importance du cadre réside dans son rôle stratégique, qui consiste à rehausser les normes de cybersécurité et à permettre la reconnaissance mutuelle des certifications dans tous les États membres, réduisant ainsi les coûts individuels pour les entreprises et améliorant le fonctionnement du marché intérieur. Le cadre devrait permettre une intégration solide avec d'autres actes juridiques de l'UE, dans le but de rationaliser les procédures et de faciliter les échanges transfrontières.

Plusieurs facteurs renforcent la pertinence de l'ECCF, malgré les difficultés auxquelles il est confronté dans l'accomplissement de ses tâches. La recrudescence des cybermenaces accroît considérablement la nécessité d'une stratégie unifiée en matière de cybersécurité qui puisse

s'adapter rapidement à des scénarios changeants, tels que la pertinence accrue de la certification dans des domaines requérant un degré d'assurance élevé, par exemple ceux des services en nuage et des infrastructures 5G. Les mandats en matière de marchés publics dans ces secteurs reflètent la demande de plus en plus pressante en faveur d'un cadre de certification unifié et fiable, demande à laquelle l'ECCF peut répondre. En outre, le lien qu'entretient l'ECCF avec les nouveaux actes législatifs, notamment le règlement sur la cyberrésilience et la directive SRI 2 (sécurité des réseaux et de l'information), met en évidence sa valeur attendue au regard des besoins en infrastructures critiques et de la conformité juridique dans l'ensemble de l'UE. Le rôle proactif de l'ENISA et la mise en place d'autorités nationales de certification de cybersécurité marquent des étapes cruciales vers le renforcement des interactions collaboratives et l'adoption de la certification. Toutefois, les écarts dans la répartition des ressources et de l'expertise entre les «grands» et les «petits» États membres perpétuent les déséquilibres en matière de participation et d'efficacité, ce qui entrave l'élaboration de schémas collectifs.

Cohérence

La cohérence de l'ECCF est également compromise par l'absence de mécanismes clairs de responsabilisation, ce qui a entraîné des difficultés concernant l'alignement de ses objectifs sur d'autres mesures législatives. Ce décalage risque de créer des chevauchements et des inefficacités dans l'environnement de la cybersécurité. Il est essentiel d'assurer la cohérence totale de l'ECCF avec d'autres instruments législatifs de l'UE, y compris la directive SRI 2 et le règlement sur la cyberrésilience, pour garantir une approche unifiée en matière de cybersécurité. En théorie, l'ECCF est aligné sur ces mesures législatives, conçues pour encadrer différents aspects de la cybersécurité dans le contexte de l'UE, mais son intégration pratique reste complexe et nécessite un contrôle diligent. La mise en œuvre prochaine du schéma européen de certification de cybersécurité fondé sur des critères communs (EUCC) constitue un test de cohérence important, car la réussite de son déploiement démontrera la capacité de l'ECCF à harmoniser et à exploiter efficacement de nouveaux efforts législatifs. Les parties prenantes ont souligné la nécessité d'une coordination minutieuse entre l'ECCF et les actes réglementaires émergents afin d'éviter les chevauchements, qui risqueraient de nuire à leur efficacité et de diluer leurs effets escomptés dans tous les secteurs. Plus précisément, des préoccupations sont soulevées concernant l'interface entre l'ECCF et le règlement sur la cyberrésilience, étant donné que ces deux initiatives visent à renforcer les normes de cybersécurité, mais qu'elles risquent d'être redondantes si elles ne sont pas appliquées en synergie totale dans les cas où l'un des instruments soutient et complète l'autre. Sur le plan sectoriel, la cohérence doit être élargie de manière à tenir compte de la technologie qui ne cesse de progresser, en veillant à ce que les initiatives en matière de cybersécurité soient suffisamment nuancées pour répondre aux besoins en infrastructures critiques.

Valeur ajoutée européenne

Malgré son potentiel, l'ECCF a eu du mal à concrétiser sa valeur ajoutée en favorisant un environnement unifié et efficace en matière de cybersécurité dans l'ensemble de l'UE. Le cadre avait pour but d'améliorer considérablement le paysage de la cybersécurité de l'UE en introduisant une procédure de développement et une structure de gouvernance inédites pour les processus de certification. En substance, l'ECCF a représenté une avancée décisive dans la capacité de l'UE à créer une approche harmonisée de la certification des produits, services et processus TIC. La valeur ajoutée européenne inhérente à ce cadre réside dans sa capacité à combler les disparités entre les

approches nationales, en favorisant l'établissement d'un marché intérieur doté de normes de cybersécurité cohérentes, fiables et reconnues dans tous les États membres. Toutefois, les très longs délais et l'application fragmentée des schémas ont entravé la capacité de l'ECCF à tirer pleinement parti de sa valeur escomptée. Plus précisément, les retards dans les schémas susceptibles de donner lieu à des actions, à l'instar de l'adoption tardive d'initiatives telles que le schéma fondé sur des critères communs (EUCC), ont réduit les incidences immédiates de ces instruments, dont le potentiel théorique reste dès lors largement inexploité. Les disparités dans la mise en œuvre systémique, aggravées par des degrés variables de préparation et de disponibilité des ressources entre les États membres, diluent encore davantage l'influence globale du cadre. Néanmoins, l'ECCF a dynamisé la coopération dans l'ensemble de l'UE. En créant des groupes tels que le GECC, il a institutionnalisé les efforts de coordination, permettant une mobilisation plus large au sein des différents niveaux de gouvernance. Cette infrastructure collaborative encourage le partage d'informations et les stratégies conjointes, promouvant une approche unifiée en matière de cybersécurité face aux menaces en constante évolution. Pour que l'ECCF puisse offrir toute sa valeur ajoutée à l'échelle européenne, il est impératif d'assurer une participation accrue et concise des parties prenantes. La promotion d'un environnement inclusif, dans lequel les partenaires industriels, les autorités nationales et les organes de l'UE contribuent activement au processus de certification et l'orientent, garantira l'acceptation et l'efficacité générales des normes de cybersécurité.

Principales réalisations et principaux défis

L'ECCF constitue un outil essentiel pour améliorer la collaboration au niveau de l'UE entre l'ENISA, les États membres et les entreprises, ce qui renforce la pertinence de l'Agence dans un environnement de cybersécurité dynamique. Son adaptabilité facilite l'élaboration des schémas par l'intermédiaire de groupes de travail ad hoc et son alignement sur les cadres législatifs de l'UE tels que la directive SRI 2. Ce potentiel, bien qu'important, reste largement inexploité en raison de l'application limitée des schémas actuels.

L'ECCF est crucial pour faire face aux menaces émergentes en matière de cybersécurité et favoriser le respect des règles, notamment dans l'exploitation des nouvelles technologies telles que l'intelligence artificielle. Les parties prenantes reconnaissent son rôle dans le renforcement de la coopération entre les États membres et dans l'amélioration de la préparation en matière de cybersécurité. Sa valeur dans la promotion des échanges sur le marché intérieur, grâce au remplacement des schémas nationaux de certification par des schémas à l'échelle de l'UE, est également mise en avant.

Toutefois, l'ECCF souffre d'importantes faiblesses. La longueur des procédures d'adoption des schémas nuit à leur efficacité, difficulté exacerbée par la complexité technique et par les pressions politiques qu'exerce le lobby de l'industrie. Ces retards sapent la confiance et empêchent l'adoption rapide des schémas européens de certification de cybersécurité. L'ECCF pourrait consolider les cadres de cybersécurité de l'UE, mais certaines menaces, telles que les contraintes en matière de ressources et les tensions géopolitiques, posent problème. Des changements dans les priorités stratégiques et d'éventuels chevauchements législatifs pourraient compromettre l'efficacité du cadre, ce qui risquerait d'entraîner des incohérences sur le marché. Il est impératif de résoudre ces problèmes pour que l'ECCF, concept prometteur, devienne un mécanisme pleinement opérationnel, renforçant ainsi la normalisation et la certification de l'UE en matière de cybersécurité.

3. CONCLUSIONS ET RECOMMANDATIONS

3.1 ENISA

L'évaluation de l'ENISA met en évidence le rôle crucial de cette agence dans la mise en place d'un paysage cohérent en matière de cybersécurité dans l'ensemble de l'UE. L'Agence a fait preuve d'efficacité et produit des résultats précieux. Les demandes adressées à l'ENISA étant de plus en plus nombreuses, il convient de réévaluer et de rationaliser ses activités afin de mieux aligner ses ressources et ses priorités, en mettant constamment l'accent sur l'appui aux États membres dans la lutte contre les menaces en matière de cybersécurité ainsi que dans la consolidation des infrastructures nationales de cybersécurité. Améliorer son processus d'établissement de rapports, en le rendant plus convivial et plus accessible au moyen d'aides visuelles et de résumés, pourrait renforcer l'efficacité et la pertinence de l'ENISA dans le contexte actuel des menaces. Il est essentiel d'améliorer les canaux de communication pour faire en sorte que les activités et les services de l'Agence soient clairement visibles pour les parties prenantes, y compris les acteurs de l'industrie. Une stratégie de communication bien définie pourrait contribuer à renforcer les liens et la coopération au sein des réseaux de cybersécurité existants, tels que les centres d'échange et d'analyse d'informations (ISAC).

L'ENISA peut gagner en efficacité grâce à une hiérarchisation stratégique plus poussée des tâches, ce qui lui permettra d'adopter une approche plus rationalisée de la gestion des pressions liées à la charge de travail. En vue d'améliorer sa pertinence vis-à-vis des parties prenantes, il conviendrait de continuer à consolider le rôle central de l'Agence dans l'appui aux États membres, en renforçant sa capacité à fournir en temps utile des informations sur les menaces émergentes ainsi que des outils stratégiques pour y faire face. En outre, comme l'ont indiqué un certain nombre de parties prenantes, l'ENISA pourrait mettre en place des méthodes plus structurées et plus transparentes pour dialoguer avec des entités privées, y compris pour l'accompagnement des petites et moyennes entreprises (PME). Il convient de chercher à clarifier le rôle de l'Agence dans la mise en œuvre de la politique avec les autres institutions de l'UE, en veillant à ce que la collaboration avec les États membres soit au cœur de ces efforts afin de renforcer la cohésion de la stratégie unifiée de l'UE en matière de cybersécurité. Cette démarche inclurait également la consolidation de la coopération avec d'autres agences de l'UE et la recherche de synergies avec d'autres organismes de cybersécurité pour déployer des initiatives conjointes visant à améliorer la cohérence opérationnelle dans toute l'Europe.

Dans l'ensemble, il est important de préserver le statut d'agence spécialisée qu'a l'ENISA dans le cadre de l'UE, car il permet de continuer à se concentrer sur les priorités en matière de cybersécurité. Ces recommandations visent à renforcer la capacité de l'Agence à assumer efficacement ses responsabilités et à réaffirmer son rôle de chef de file dans le domaine de la cybersécurité.

3.2 ECCF

Plusieurs recommandations stratégiques ressortent de l'évaluation de l'ECCF. Tout d'abord, malgré le rôle central que joue l'ENISA pour promouvoir la coopération et la cohésion

opérationnelle entre les États membres et les autres parties prenantes, des contraintes manifestes pèsent sur l'efficience et l'efficacité de l'ECCF, principalement en raison de la complexité des processus d'adoption des schémas. Ces problèmes mettent en évidence la nécessité de procéder à une révision substantielle des structures de gouvernance afin de renforcer la clarté opérationnelle et la responsabilité à tous les niveaux.

Pour remédier à ces constatations, plusieurs actions sont recommandées afin d'optimiser la contribution de l'ENISA à l'ECCF. Il conviendrait de déployer des efforts concertés pour garantir une répartition cohérente et adéquate des ressources financières et humaines entre l'ENISA et les autres parties prenantes au sein de l'ECCF. Stabiliser les dispositifs en matière d'emploi sera essentiel pour réduire la rotation du personnel et améliorer la mémoire institutionnelle, facilitant ainsi la mise en œuvre efficace du système et sa continuité. L'élaboration, au sein de l'ECCF, de processus décisionnels rationalisés clarifiant les rôles et les responsabilités favorisera la transparence et l'efficacité, notamment en renforçant les démarches de collaboration entre les États membres, la Commission et l'ENISA. Une telle évolution promouvra l'obligation de rendre compte et réduira les inefficacités. La détermination à fixer des délais réalistes pour l'élaboration et la mise en œuvre des schémas de certification et à les respecter est indispensable. Il faudra pour cela promouvoir une analyse technique détaillée et consolider les efforts préparatoires afin d'anticiper et d'atténuer efficacement les influences politiques.

En outre, il conviendra d'investir activement dans la formation et la rétention du personnel qualifié au sein de l'ENISA pour garantir la continuité et l'expertise en vue de relever les défis complexes en matière de cybersécurité. La stabilité à long terme de la main-d'œuvre sera cruciale pour maintenir l'efficacité opérationnelle de l'ECCF. En outre, il conviendra de sensibiliser davantage le secteur d'activité et les consommateurs en déployant des campagnes ciblées et en assurant leur participation stratégique, pour mettre en avant la valeur des produits et services certifiés. Il sera essentiel d'adopter une approche proactive pour obtenir le soutien des parties prenantes afin de stimuler la demande et de favoriser la confiance dans les initiatives de l'ECCF.