European Commission

Étude sur l'évaluation de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA)

RÉSUMÉ

Une étude préparée pour la Commission européenne DG Communications Networks, Content & Technology (DG CONNECT) (Direction générale des réseaux de communication, du contenu et de la technologie) par:

RAMBØLL

carsa

Marché unique numérique

L'étude a été réalisée pour la Commission européenne par

Karin Attström, Vanessa Ludden, Franziska Lessmann
Ramboll

Pär Weström, Johannes Conrads
Carsa
Carretera de Asúa, 6
48930 Getxo
Vizcaya – Spain
http://www.carsa.es

Avec des contributions de: Helena Farrand Carrapico, Aston University; Andrej Savin, Copenhagen Business School; Cristina de la Maza, RedBorder

Identification interne

Numéro de contrat: 30-CE-0815229/00-33 (Contrat cadre No 30-CE-0677656/00-00)

Numéro SMART 2016/0077

NON-RESPONSABILITÉ

Par la Commission européenne, la Direction générale des réseaux de communication, du contenu et de la technologie.

Les informations et les points de vue énoncés dans la présente publication sont ceux des auteurs et ne reflètent pas nécessairement l'opinion officielle de la Commission. La Commission ne garantit pas l'exactitude des données incluses dans cette étude. Ni la Commission ni aucune personne agissant au nom de la Commission ne peuvent être tenues responsables de l'utilisation qui peut être faite de l'information contenue dans ce document.

ISBN 978-92-79-72113-7
doi:10.2759/035839

RESUME ANALYTIQUE

L'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) a été fondée en 2004. L'Agence fournit des recommandations, des conseils et des analyses de données, et soutient une plus grande sensibilisation et coopération des organes européens et des États membres dans le domaine de la cybersécurité. L'ENISA utilise son expertise pour améliorer la coopération entre les États membres et entre les acteurs des secteurs public et privé, ainsi que pour soutenir le renforcement des capacités.

La présente étude porte sur l'évaluation d'ENISA pour la période 2013-2016, moyennant la mesure de la performance, la gouvernance et la structure organisationnelle de l'Agence, et de son positionnement par rapport à d'autres organismes européens et nationaux. Elle évalue les forces, les faiblesses, les opportunités et les menaces (analyse SWOT) d'ENISA dans le contexte du nouveau paysage de cybersécurité et de protection des données numériques. Elle propose également des options pour modifier le mandat de l'Agence afin de mieux répondre aux nouveaux besoins émergents et elle évalue leurs conséquences financières.

Les conclusions de l'étude d'évaluation montrent qu'ENISA a réalisé des progrès importants en matière de renforcement de la sécurité des réseaux et des systèmes d'information (SRI) dans l'UE. Toutefois, une approche fragmentée à la cybersécurité dans l'UE et les problèmes internes de l'Agence, notamment de ressources financières limitées, entravent la capacité d'ENISA à répondre aux besoins sans cesse croissants des parties prenantes dans un contexte de développements technologiques et de menaces changeantes à la cybersécurité.

RESUME

Le présent document est le résumé de l'«Étude sur l'évaluation de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA)».

Objectifs

ENISA est l'Agence européenne chargée de la sécurité des réseaux et de l'information. Elle a été établie en 2004 en vertu du Règlement (CE) Nº 460/2004. Depuis lors, le mandant d'ENISA a été révisé une fois et a été étendu à plusieurs reprises. Les derniers changements ont été mis en œuvre par le Règlement (UE) Nº 526/2013 (ci-après «le Règlement»). L'article 32, paragraphe 1 du Règlement demande à la Commission de «commander une évaluation portant, en particulier, sur l'impact, l'efficacité et l'efficience de l'action de l'Agence et de ses pratiques professionnelles. Cette évaluation examinera également la nécessité éventuelle de modifier le mandat de l'Agence, ainsi que les conséquences financières d'une telle modification».

L'étude porte sur l'évaluation d'ENISA pour la période 2013-2016, moyennant la mesure de la performance, la gouvernance et la structure organisationnelle de l'Agence, et de son positionnement par rapport à d'autres organismes européens et nationaux. En outre, l'étude évalue les forces, les faiblesses, les opportunités et les menaces (analyse SWOT) d'ENISA dans le contexte du nouveau paysage de cybersécurité et de protection des données numériques. Elle propose également des options pour modifier le mandat de l'Agence afin de mieux répondre aux nouveaux besoins et elle évalue leurs conséquences financières.

Approche méthodologique

L'étude d'évaluation vise à mesurer la pertinence, l'efficacité, l'efficience, la cohérence et la complémentarité d'ENISA, ainsi que sa valeur ajoutée à l'échelle de l'UE. Elle contient les réponses à 46 questions d'évaluation basées sur la Feuille de route de la Commission européenne pour l'évaluation d'ENISA[1]. Les conclusions de l'évaluation sont tirées d'une collecte de données à la fois primaires et secondaires et de tâches d'analyse qui alimentent le développement des réponses aux questions d'évaluation. L'évaluation comprend une vaste collecte de données, impliquant notamment la consultation de différents groupes de parties prenantes (tels que le personnel et la direction d'ENISA, le Conseil de gestion d'ENISA, les équipes nationales d'intervention en cas d'urgence informatique et les équipes de réaction aux incidents touchant la sécurité informatique (CERT/CSIRT), les institutions de l'UE, des parties prenantes privées). Les données primaires ont été collectées à l'aide de différents outils: entretiens approfondis, deux enquêtes, une consultation publique ouverte et un atelier. L'évaluation se base sur une matrice d'évaluation qui relie les questions d'évaluation aux sources de données, aux indicateurs et aux stratégies analytiques qui ont été utilisées pour répondre aux questions, ce qui permet d'identifier clairement la façon dont les conclusions ont été adoptées.

L'évaluation a été réalisée entre novembre 2016 et juillet 2017 par Ramboll Management Consulting et CARSA, et a impliqué l'intervention de trois experts externes couvrant les aspects politiques, juridiques et techniques de la cybersécurité.

Constatations et conclusions

Une évaluation de la performance, de la gouvernance, de la structure organisationnelle et du positionnement d'ENISA pour la période 2013-2016 sur la base des critères d'évaluation est présentée dans le tableau ci-après. Les principales constatations qui ont mené à cette évaluation sont décrites ci-dessous.

[1] Commission européenne (2016) : Feuille de route pour l'évaluation – Évaluation de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA)

Tableau 1: Évaluation d'ENISA sur la base des critères d'évaluation

Critère d'évaluation	Évaluation globale
Pertinence	Atteint dans une grande mesure
Efficacité	Partiellement atteint
Efficience	Atteint dans une grande mesure
Cohérence	Partiellement atteint
Valeur ajoutée à l'échelle UE	Partiellement atteint

Pertinence: Dans le contexte des développements technologiques et des menaces changeantes, le renforcement de la sécurité des réseaux et des systèmes d'information (SRI) dans l'UE est essentiel. Les ajouts récents au cadre législatif, tels que la directive SRI[2] soulignent ce besoin. Les États membres et les organes de l'UE s'appuient sur l'expertise relative à l'évolution de la SRI, les capacités doivent être renforcées dans les États membres afin de comprendre et de faire face aux menaces et les parties prenantes doivent coopérer dans les différents domaines thématiques et dans les diverses institutions. Compte tenu de ce contexte, les objectifs énoncés dans le mandat d'ENISA se sont avérés pertinents au cours de la période sur laquelle porte l'évaluation et continuent d'être éminemment pertinents aujourd'hui.

Bien que le mandat définisse les objectifs de l'Agence en termes généraux, laissant au Conseil de gestion d'ENISA la possibilité d'établir des priorités en fonction des derniers développements en vue de répondre aux besoins changeants et faire face à des menaces en constante évolution, les activités d'ENISA ne répondent pas entièrement aux besoins de toutes ses parties prenantes:

- le programme de travail d'ENISA est dominé par les intérêts des États membres et, pourtant, il convient d'envisager une perspective à plus long terme ainsi que des activités d'autres parties prenantes dans le domaine de la cybersécurité (telles que d'autres agences européennes ou le secteur privé) afin de garantir le maintien de la pertinence de l'Agence
- les parties prenantes d'ENISA ont des besoins très différents et, de ce fait, il est difficile de répondre à tous ces besoins. Certains États membres (comme l'Allemagne, la France ou la Suède) ont des capacités et des ressources significatives dans le domaine de la cybersécurité et s'appuient sur ENISA exclusivement pour des services spécifiques. D'autres États membres (de l'Europe de l'Est et du Sud) sont moins expérimentés et dépendent davantage de l'expertise et des capacités d'ENISA. La Commission a ses propres besoins et attentes en ce qui concerne les services qu'ENISA peut fournir aux différentes DG. En outre, les parties prenantes du secteur, y compris un grand nombre de petites et moyennes entreprises (PME), sont des acteurs importants dans le domaine de la SRI et pourraient aussi bénéficier des activités d'ENISA

Efficacité: De manière générale, ENISA accomplit ses tâches et atteint ses objectifs. ENISA a contribué à un renforcement de la SRI en Europe par le biais des quatre tâches présentées dans le tableau ci-dessous, même si chacune de ces tâches peut encore être améliorée.

Renforcement de la sensibilisation communautaire		**Renforcement des capacités**	
Réalisations	Domaines d'amélioration	Réalisations	Domaines d'amélioration
✓ Contribution importante au renforcement de la coopération entre les États membres et les parties prenantes à la SRI, en particulier entre les CERT/CSIRT	- La coopération pourrait être renforcée entre ENISA et la Commission et d'autres agences de l'UE, et avec le secteur privé	✓ Contribution au renforcement des capacités dans les États membres, plus particulièrement dans les États membres dont les capacités et les ressources sont limitées dans le domaine de la	- Le renforcement des capacités avec le secteur privé pourrait s'intensifier

[2] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union

		cybersécurité ✓ Les activités importantes comprennent notamment les exercices Cyber Europe et les formations pour les CERT/CSIRT	
Source d'expertise		**Soutien à l'élaboration et à la mise en œuvre des politiques**	
Réalisations	Domaines d'amélioration	Réalisations	Domaines d'amélioration
✓ Contribution importante au soutien des CERT/CSIRT	- ENISA n'est pas parvenue à être reconnue comme un centre d'expertise ou un point de référence pour d'autres parties prenantes telles que les institutions de l'UE ou le secteur privé - Forte dépendance vis-à-vis de l'obtention d'expertise externe et limitation des ressources disponibles en interne	✓ ENISA a aidé les États membres et la Commission à formuler et à mettre en œuvre des politiques	- ENISA n'est pas systématiquement invitée par la Commission à participer à toutes les activités liées à la SRI

La contribution d'ENISA à la SRI en Europe est limitée par plusieurs facteurs clés parmi lesquels nous pouvons citer:

- Le mandat global qui couvre une multitude de tâches, ce qui laisse peu de marge à sa propre initiative et aux travaux qui ne lui soient pas spécifiquement demandés
- Les difficultés de l'Agence pour attirer et retenir des experts en cybersécurité comme membres de son personnel, pour différentes raisons, notamment de faibles procédures de ressources humaines au cours de la période considérée
- La visibilité limitée d'ENISA – l'Agence n'est pas suffisamment connue dans l'UE et n'a pas été capable d'établir une marque, contrairement à d'autres agences de l'UE

Efficience: Le budget et les niveaux de ressources humaines d'ENISA sont parmi les plus bas comparativement aux autres agences européennes. Afin d'exécuter les différentes tâches énoncées dans son mandat, ENISA doit être très efficiente dans la mise en œuvre de son budget et doit envisager scrupuleusement la destination des ressources et des heures de travail. L'Agence produit un grand nombre de publications chaque année et met en place de nombreuses autres activités. Malgré son budget réduit, l'Agence a été en mesure de contribuer à la réalisation des objectifs et impacts ciblés, ce qui reflète une utilisation efficiente de son budget.

En termes d'efficience, ENISA est confrontée à deux défis principaux:

- Un certain nombre d'exigences administratives établies par la Commission sont identiques pour toutes les agences de l'UE, mais ont des répercussions plus lourdes pour les agences de plus petite taille
- Un site d'implantation réparti entre Athènes et Héraklion, ce qui implique des efforts additionnels de coordination et des coûts supplémentaires

Cohérence: Les activités d'ENISA sont généralement cohérentes avec les politiques et les activités de ses parties prenantes, mais une approche plus coordonnée à la cybersécurité au niveau européen est nécessaire. Le potentiel de coopération entre ENISA et la Commission européenne, ainsi qu'avec d'autres organes de l'UE, n'est pas pleinement exploité. Par exemple, la division des responsabilités entre ENISA et CERT-UE devrait être clarifiée.

Les activités d'ENISA sont cohérentes, en grande partie, avec le travail réalisé au niveau national dans le domaine de la cybersécurité. La cohérence est particulièrement forte entre les CERT/CSIRT et ENISA. Certains chevauchements ont été détectés entre les activités d'ENISA et celles des États membres jouissant d'une forte expertise dans le domaine de la cybersécurité. Toutefois, les États membres dont les capacités et les ressources dans le domaine de la cybersécurité sont plus limitées bénéficient encore des activités de l'Agence.

Valeur ajoutée à l'échelle européenne: La valeur ajoutée d'ENISA réside principalement dans sa capacité à renforcer la coopération, essentiellement entre les États membres, mais aussi avec les communautés intervenant dans la SRI. Il n'existe aucun autre acteur à l'échelle européenne qui soutienne la coopération de ce même panel de parties prenantes dans le domaine de la SRI. La valeur ajoutée d'ENISA varie d'un État membre à l'autre, en fonction de leurs capacités et ressources en matière de cybersécurité. Les activités d'ENISA consistant à fournir une expertise et à renforcer les capacités représentent une importante valeur ajoutée pour les États membres qui consacrent peu de ressources nationales à la cybersécurité. Cette valeur ajoutée n'est pas si marquée pour les États membres qui jouissent de plus grandes capacités en matière de cybersécurité.

En conséquence, la cessation des activités d'ENISA aurait un impact variable selon les États membres. Alors que les États membres jouissant de solides capacités en matière de cybersécurité seront à même de remplacer les services fournis par ENISA, tout du moins dans une certaine mesure, il n'en ira pas de même pour les États membres disposant de moins de ressources. Ces derniers dépendent davantage des services d'ENISA au niveau du renforcement des capacités, de l'accès à l'expertise et du soutien à la mise en œuvre des politiques et des législations. La cybersécurité franchit les frontières et il est donc nécessaire de renforcer les capacités afin d'éviter des maillons plus faibles qui pourraient affecter la cybersécurité de l'ensemble de l'UE. Il faut également apporter une réponse paneuropéenne. Il ne sera pas possible d'assurer le même degré de renforcement de la sensibilisation communautaire et de coopération dans les différents États membres sans une agence européenne décentralisée chargée de la cybersécurité. La situation serait plus fragmentée dans les cas où la coopération bilatérale ou régionale interviendrait pour combler le vide laissé par l'ENISA. Par conséquent, la coordination au niveau européen est indispensable.

Une éventuelle disparition d'ENISA représenterait une occasion manquée pour tous les États membres. La plupart des parties prenantes ont estimé qu'ENISA pourrait jouer à l'avenir un rôle plus important dans le paysage européen de la cybersécurité, en assurant une compétence de réponse commune. Ce potentiel pour l'Agence de tirer profit d'opportunités futures serait perdu si elle devait disparaître.

Analyse SWOT: En s'appuyant sur une analyse du contexte – à savoir l'évolution, depuis la dernière révision du mandat d'ENISA en 2013, de l'environnement de la cybersécurité et de la protection des données numériques – l'étude d'évaluation fournit un diagnostic des principales forces et faiblesses d'ENISA, et de ses opportunités et menaces dans le nouvel environnement de la cybersécurité et de la protection des données numériques. Les éléments de cette analyse sont présentés dans l'illustration ci-dessous.

Tableau 2: L'analyse SWOT d'ENISA

Forces	Faiblesses
- Neutre, facilitateur, sans influences politiques ni intérêts commerciaux - Soutien reconnu aux États membres pour le renforcement des capacités et le développement des compétences nécessaires pour renforcer la résilience aux menaces cybernétiques - Collaboration reconnue et renforcement de la sensibilisation communautaire touchant un vaste éventail d'acteurs, notamment les États membres, l'industrie, les organes de l'UE, etc. - Expertise horizontale, «aperçu du paysage» des politiques des Etats membres en matière de cybersécurité	- Faible visibilité pour différentes raisons: manque d'expertise, faible communication/marketing et reconnaissance limitée dans le paysage politique européen de la cybersécurité - Absence d'une vision stratégique à long terme - Difficultés de recrutement - Efficience réduite en raison de l'implantation dans deux endroits différents - Distance par rapport aux décideurs de l'UE à Bruxelles - Manque des ressources financières et humaines nécessaires pour changer la donne
Opportunités	**Menaces**
- Besoin croissant de synergies entre les opérateurs des technologies de l'information et des communications (TIC) afin de garantir des actions politiques concertées et collaboratives en matière de SRI - La directive SRI a le potentiel de renforcer le rôle d'ENISA au niveau de la politique européenne en matière de cybersécurité - Il existe un besoin reconnu et une demande de la part des parties prenantes de renforcer la sensibilisation à la cybersécurité - La communauté accroît son soutien pour une standardisation et une certification des TIC	- La fragmentation des politiques au niveau européen et les priorités divergentes au niveau des politiques dans les États membres limitent le champ d'action d'ENISA - Le contexte de menaces complexes et en rapide évolution, impliquant de multiples disciplines, crée de nouvelles vulnérabilités, par exemple, l'Internet des objets (IdO) - La pénurie de talents (techniques) globaux dans le domaine de la cybersécurité accentue les difficultés de recrutement d'ENISA

En conclusion, pour améliorer à l'avenir la pertinence, l'efficacité, l'efficience, la cohérence et la valeur ajoutée d'ENISA et pour l'aider en fin de compte à contribuer à une plus grande sécurité des réseaux et des systèmes d'information (SRI) dans l'UE, les **principaux problèmes** qui ont été identifiés et qui requièrent l'adoption de mesure sont les suivants:

- *Un cadre institutionnel et juridique déficient pour la cybersécurité au sein de l'UE* - La cybersécurité est essentiellement considérée comme une question qui relève des compétences nationales, alors que, en réalité, c'est un domaine qui dépasse les frontières.
- *Fragmentation de la politique européenne en matière de cybersécurité* – La fragmentation de la politique de cybersécurité est due à l'existence d'un certain nombre d'acteurs de niveau européen dans le domaine de la cybersécurité et au manque de coordination entre ces différents acteurs. Un facteur important à cet égard est la division des responsabilités entre ENISA et CERT-EU.
- *Limitations pour ENISA en raison de sa taille* – ENISA éprouve des difficultés à créer un véritable impact dans le vaste domaine de la SRI étant donné que l'Agence dispose uniquement de ressources humaines et financières limitées pour accomplir une mission ambitieuse.
- *Visibilité limitée* – ENISA n'est pas parvenue à développer une marque puissante et n'est pas considérée comme une référence pour la cybersécurité au niveau européen.
- *Pas perçue comme Agence proactive, visionnaire* – Compte tenu de son vaste mandat, ENISA a tendance à être réactive et à répondre aux besoins du plus grand nombre de parties prenantes possible, mais cela signifie qu'elle perd son orientation. ENISA n'est pas en mesure d'utiliser ses propres connaissances pour établir des priorités de travail étant donné que ce sont les États membres qui dictent son programme de travail.
- *Un mandat qui n'est pas aligné sur les besoins en matière de cybersécurité* – Les menaces liées à la cybersécurité sont devenues un problème permanent dans l'UE et ENISA s'est vue attribuer des responsabilités à long terme (p. ex., en vertu de la directive SRI) qui exigent un mandat permanent.
- *ENISA ne répond pas, dans une mesure suffisante, aux besoins de toutes ses parties prenantes* – Dans le cadre de la structure de gouvernance actuelle, les besoins du secteur privé ne sont pas suffisamment pris en considération et, par conséquent, ils ne sont pas reflétés dans les programmes de travail de l'Agence.
- *ENISA devrait élargir ses activités pour mieux répondre aux besoins des parties prenantes* – Il y a une demande de la part des parties prenantes (bien qu'il ne s'agisse pas d'une demande unanime) pour l'établissement dans l'UE d'un système cohérent de certification et standardisation des TIC. Les États membres disposant de moins de ressources et d'expertise

requièrent un soutien additionnel pour recevoir des informations sur les menaces à la cybersécurité et pour évaluer ces menaces afin de faire face aux attaques.

Malgré ces problèmes, ENISA jouit d'un important potentiel qui lui permettrait de participer à l'amélioration de la sécurité des réseaux et des systèmes d'information dans l'UE, pour autant que son mandat soit adéquat et qu'elle bénéficie du soutien nécessaire en termes de ressources humaines et financières. Il existe un besoin manifeste de coopération et de coordination entre les différentes parties prenantes, et ENISA, en sa qualité d'agence européenne décentralisée, est en mesure d'assurer une approche coordonnée aux menaces à la cybersécurité dans l'UE.

Options pour l'avenir de l'Agence

Sur la base des problèmes clés présentés ci-dessus et identifiés à partir des constatations et conclusions de l'étude, quatre options ont été élaborées en vue de réviser le mandat actuel d'ENISA. Ces options sont présentées dans le **Error! Reference source not found.** ci-dessous qui souligne, pour chacune des options concernées, les facteurs spécifiques de changement qui pourraient être mis en œuvre.

Tableau 3: Options pour l'avenir d'ENISA

Option	Facteur de changement
Option 0: Base de référence, maintien du statu quo Cette option comprend une extension du mandat actuel en termes de champ d'application et d'objectifs, sachant que les dispositions de la directive SRI, du règlement eIDAS[3] et de la directive sur le cadre des télécommunications[4] devraient être prises en compte.	**Révision du mandat d'ENISA de façon à ce que ses nouvelles tâches soient plus spécifiques conformément aux législations récentes/futures:** • Participation au Groupe de coopération conformément à l'exigence stipulée dans la directive SRI • Secrétariat du réseau CSIRT • Code de communication électronique, considérant 92 (Directive cadre sur les télécommunications) • eIDAS
Option 1: Expiration du mandat d'ENISA (cessation des activités d'ENISA) Cette option impliquerait la fermeture d'ENISA, sans qu'une autre institution de niveau européen ne soit créée. On utiliserait plutôt les institutions/organisations existantes pour mettre en œuvre les engagements au titre, par exemple, de la directive SRI et des liens bilatéraux et régionaux au niveau des États membres.	N/A
Option 2: Renforcement d'ENISA (Maintien d'ENISA avec des modifications de son mandat) Cette option propose des modifications significatives du mandat d'ENISA en vue de résoudre les problèmes clés identifiés dans l'étude. Il s'agirait donc de s'appuyer sur son rôle actuel et de s'assurer que le nouveau mandat soit mieux adapté à l'environnement changeant de la cybersécurité.	**Renforcement du rôle opérationnel d'ENISA:** • Transmettre périodiquement des renseignements sur les menaces et des alertes ad hoc • Soutenir le schéma directeur pour répondre aux incidents de cybersécurité à grande échelle et aux crises de niveau européen • Fournir une réponse de cybersécurité d'urgence
	Renforcement du rôle d'ENISA au niveau du développement et de la mise en œuvre des politiques: • Rendre obligatoire la consultation d'ENISA par la Commission pour toutes les questions relatives à la cybersécurité • Prévoir la participation formelle d'ENISA au mécanisme pour l'interconnexion en Europe • Programmer des réunions régulières entre ENISA

[3] Règlement (UE) Nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE

[4] Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive «cadre»)

Option	Facteur de changement
	et d'autres agences/organisations internationales
	Rendre le mandat d'ENISA permanent
	Renforcement de la structure de gouvernance d'ENISA: • Accroître le rôle du Groupe permanent des parties prenantes (GPP) • Accorder à ENISA une plus grande flexibilité pour définir ses priorités de travail
	Prévoir un rôle pour ENISA dans la standardisation et la certification au niveau européen • Soutenir le Cadre européen de certification de la sécurité des TIC • Soutenir la standardisation de la sécurité des TIC
	Renforcement de la position d'ENISA en termes d'innovation et de recherche: • Prendre part à la mise en œuvre des programmations • OU Prendre part à la programmation en qualité d'organe de consultation • OU Bénéficier du financement européen pour la recherche et le développement
	Augmentation de la visibilité d'ENISA: • Établir un bureau de liaison à Bruxelles • Créer une équipe spéciale de communication au sein d'ENISA
Option 3: Agence européenne jouissant de pleines capacités opérationnelles (Établir un Centre européen de cybersécurité) Cette option prévoit la conversion d'ENISA en un nouvel organe de niveau européen qui couvrirait l'intégralité du cycle de la cybersécurité et serait chargé de la prévention, de la détection et de la réponse aux incidents cybernétiques.	**Création d'un organe européen global de cybersécurité:** • Un tel organe engloberait ENISA et CERT-EU
	Création d'une CSIRT européenne virtuelle: • Coordonner les opérations de réseau de CSIRT • Assurer une sensibilisation en temps réel aux situations et alimenter des flux dynamiques d'informations sur les menaces • Maintenir et fournir au secteur public et privé une capacité de réponse aux incidents cybernétiques
	Tous les facteurs énumérés dans l'Option 2 pourraient être réalisés dans le cadre de l'Option 3.

Commission européenne

Évaluation de l’Agence de l'Union européenne chargée de la sécurité des réseaux et de l’information (ENISA)

Luxembourg, Bureau des Publications de l'Union européenne

2017 – 11 pages

ISBN 978-92-79-72113-7
doi:10.2759/035839

KK-02-17-971-FR-N

doi:10.2759/035839 ISBN 978-92-79-72113-7