
# Introduction

**1.1 L’ENISA**

L’Agence européenne chargée de la sécurité des réseaux et de l’information (ENISA) a été créée, à l’origine, en 2004 et son mandat a été renouvelé régulièrement. Le mandat actuel de l’ENISA est fixé dans le règlement (UE) n° 526/2013[[1]](#footnote-1) (ci-après le «règlement ENISA») et vient à expiration le 19 juin 2020.

Le mandat de l’ENISA est de contribuer à un niveau élevé de sécurité des réseaux et de l’information au sein de l’Union. Le règlement ENISA énumère les objectifs spécifiques de l’Agence, en précisant que celle-ci doit:

* acquérir et maintenir un niveau élevé de compétence;
* assister les institutions, organes et organismes de l’Union dans l’élaboration des politiques de sécurité des réseaux et de l’information;
* assister les institutions, organes et organismes de l’Union et les États membres dans la mise en œuvre des politiques nécessaires pour satisfaire aux exigences légales et réglementaires requises au titre des actes juridiques existants et à venir de l’Union en matière de sécurité des réseaux et de l’information, contribuant ainsi au bon fonctionnement du marché intérieur;
* aider l’Union et les États membres à améliorer et à renforcer leurs moyens et leur préparation pour prévenir les problèmes et incidents de sécurité des réseaux et de l’information, les détecter et y faire face;
* mettre à profit ses compétences spécialisées pour encourager une large coopération entre les acteurs des secteurs public et privé.

En outre, les colégislateurs de l’Union ont fixé à l’ENISA, dans la directive (UE) 2016/1148[[2]](#footnote-2) concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d’information dans l’Union (la «directive SRI»), des missions importantes en ce qui concerne la mise en œuvre de la législation. En particulier, l’Agence assure le secrétariat du réseau des CSIRT (mis en place pour promouvoir une coopération rapide et effective, au niveau opérationnel, entre les États membres) et elle est aussi appelée à assister le groupe de coopération dans l’exécution de ses tâches liées à la coopération stratégique. En outre, la directive SRI exige de l’ENISA qu’elle assiste les États membres et la Commission en fournissant son expertise et ses conseils et en facilitant l’échange de bonnes pratiques.

L’Agence a ses bureaux en Grèce, son siège administratif se trouve à Héraklion (Crète) et son centre opérationnel à Athènes. Elle emploie 84 personnes et est dotée d’un budget de fonctionnement annuel de 11,25 millions d’EUR. Elle est dirigée par un directeur exécutif, et sa gouvernance est assurée par un conseil d’administration, un conseil exécutif et un groupe permanent des parties prenantes. Un réseau informel d'agents de liaison nationaux facilite le dialogue avec les États membres.

# 1.2 Objet du rapport

L’article 32 du règlement ENISA fait obligation à la Commission de procéder, avant le 20 juin 2018, à une évaluation de l’ENISA «*portant, en particulier, sur l’impact, l’efficacité et l’efficience de l’action de l’Agence et de ses pratiques professionnelles*» et de déterminer si le mandat actuel de l’Agence doit être prolongé.

Dans sa communication de 2016 intitulée «Renforcer le système européen de cyber-résilience et promouvoir la compétitivité et l’innovation dans le secteur européen de la cybersécurité»[[3]](#footnote-3), la Commission a annoncé que, compte tenu des bouleversements survenus dans le paysage en matière de cybersécurité depuis 2013, au moment de l’adoption du règlement ENISA actuel, et du niveau de maturité atteint sur les plans politique, commercial et technologique, elle entendait avancer l'évaluation et le réexamen de l’ENISA. Elle faisait observer, en particulier, que ce processus fournirait l’occasion de renforcer, éventuellement, les compétences et les moyens de l’Agence pour aider de manière durable les États membres à atteindre la résilience en matière de cybersécurité.

Cette approche a été confirmée, par la suite, dans les conclusions du Conseil de 2016[[4]](#footnote-4), dans lesquelles il a été reconnu que «les cybermenaces et les vulnérabilités continuent d’évoluer et de s’aggraver, ce qui nécessitera de poursuivre et d’intensifier la coopération, en particulier pour répondre aux cyberincidents transfrontières majeurs». Le Conseil y a réaffirmé que le règlement ENISA constitue l’un des «éléments essentiels d’un cadre de cyber-résilience de l’UE».

Les résultats de l’évaluation de l’ENISA ont été pris en compte dans l’analyse d’impact accompagnant la proposition de règlement relatif à l’ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) n° 526/2013, et relatif à la certification de sécurité des technologies de l’information et des communications en matière de cybersécurité («règlement sur la cybersécurité»).

En application de l’article 32 du règlement ENISA, la Commission doit transmettre le rapport d’évaluation, accompagné de ses conclusions, au Parlement européen, au Conseil et au conseil d’administration. Le présent rapport succinct est accompagné d’un document de travail des services de la Commission relatif à l’évaluation de l’Agence européenne chargée de la sécurité des réseaux et de l’information (SWD(2017) 502).

# Principales constatations de l’évaluation

Conformément aux lignes directrices pour une meilleure réglementation de la Commission[[5]](#footnote-5), l’évaluation a porté sur l’efficacité, l’efficience, la cohérence, la pertinence et la valeur ajoutée européenne de l’Agence en ce qui concerne son fonctionnement, sa gouvernance, sa structure organisationnelle interne et ses méthodes de travail.

Cette analyse a également tenu compte du contexte différent dans lequel travaille désormais l’Agence, notamment en ce qui concerne: le nouveau cadre réglementaire et politique de l’Union (la directive SRI, le réexamen de la stratégie de cybersécurité de l’UE, par exemple); l’évolution des besoins de la communauté des parties intéressées et la complémentarité et les synergies possibles avec les travaux exécutés par d’autres institutions, organes et organismes nationaux et de l’UE, notamment l’équipe d'intervention en cas d'urgence informatique pour les institutions, organes et organismes de l'Union européenne (CERT-UE) et le Centre européen de lutte contre la cybercriminalité (EC3) au sein d’Europol.

Pour évaluer le fonctionnement de l’Agence,

* la Commission a commandé une étude indépendante qui a été réalisée entre novembre 2016 et juillet 2017 et qui, avec l’analyse interne effectuée par la Commission, constitue la principale base de l’évaluation.
* Cette étude comprenait des travaux de recherche documentaire et de collecte et d’analyse de données, menés notamment en recourant à des enquêtes auprès des parties prenantes et des entretiens approfondis avec les principaux acteurs du secteur de la cybersécurité, à un atelier réunissant les parties intéressées, à une analyse comparative et à un exercice de positionnement de l’Agence ainsi qu’à une analyse des forces, des faiblesses, des opportunités et des menaces (analyse «SWOT»).
* La Commission a également organisé une consultation publique en ligne de 12 semaines portant à la fois sur l’évaluation ex post et sur l’avenir de l’ENISA, ainsi que des consultations ciblées avec les principaux acteurs concernés.

Les principales conclusions de l’évaluation, en fonction des critères retenus, peuvent être résumées comme suit:

1. **Pertinence:** Compte tenu de l’évolution des technologies et des menaces et du besoin pressant d’accroître la sécurité des réseaux et de l’information dans l’UE, les objectifs de l’ENISA se sont avérés pertinents. Étant donné que les États membres et les organes de l’UE comptent sur une expertise en matière d’évolution de la sécurité des réseaux et de l’information, il faut se doter de moyens, dans les États membres, pour appréhender les menaces et y répondre, et les parties intéressées doivent coopérer dans tous les champs thématiques et toutes les institutions. La sécurité des réseaux et de l’information reste une priorité politique absolue de l’UE à laquelle l’ENISA est censée répondre. Toutefois, le fait que l’ENISA ait été créée en tant qu’agence de l’UE avec un mandat à durée déterminée: i) ne permet aucune planification à long terme et empêche d’apporter un soutien durable aux États membres et aux institutions de l’UE dans un contexte de menaces pour la cybersécurité en mutation rapide; ii) peut créer un vide juridique car les dispositions de la directive SRI confiant des missions à l’ENISA sont de nature permanente.
2. **Efficacité:** L’ENISA a globalement atteint ses objectifs et accompli ses missions. Elle a contribué à accroître la sécurité des réseaux et de l’information en Europe par ses principales activités (dotation de moyens, fourniture d’expertise, création de communautés et soutien aux politiques). Pour chacune d’entre elles, des possibilités d’amélioration ont été recensées. Il est ressorti de l’évaluation que l’ENISA a effectivement permis de créer de solides relations de confiance avec certaines parties intéressées, notamment les États membres et la communauté des CSIRT. Les interventions concernant la dotation de moyens ont été jugées efficaces, en particulier pour les États membres ayant le moins de ressources. L’action en faveur d’une coopération étendue a été l’une des plus remarquables et les parties intéressées s’accordent à dire que l’ENISA a joué un rôle fédérateur utile. Néanmoins, l’ENISA a eu du mal à exercer son influence dans le vaste domaine de la sécurité des réseaux et de l’information. Cela tient aussi au fait qu’elle disposait de ressources humaines et financières assez limitées pour s’acquitter d’un mandat très large. Il a également été conclu de l’évaluation que l’ENISA avait en partie atteint l’objectif de fournir une expertise, cela étant lié aux problèmes pour recruter des experts (voir aussi ci-après la partie «Efficience»).
3. **Efficience:** Malgré son budget limité – l’un des moins élevés de tous les organes de l’UE –, l’Agence a été capable de poursuivre les objectifs fixés, en se montrant globalement efficiente dans l’utilisation de ses ressources. Il est ressorti de l’évaluation que les processus étaient généralement efficients et que le partage clair des responsabilités au sein de l’organisation a permis une exécution satisfaisante des tâches. L’un des principaux problèmes de l’Agence en matière d’efficience tient aux difficultés qu’elle a rencontrées pour recruter et retenir des experts hautement qualifiés. D’après les conclusions, cela peut s’expliquer par une combinaison de facteurs: la difficulté du secteur public, en général, à concurrencer le secteur privé lorsqu’il s’agit d’embaucher des experts hautement spécialisés; le type de contrats (à durée déterminée) que l’Agence pouvait surtout proposer; et le degré d’attractivité relativement faible de l’ENISA dû à sa localisation et, notamment, aux problèmes rencontrés par les conjoints pour trouver du travail. Le dédoublement de l’implantation entre Athènes et Héraklion a exigé des efforts de coordination et engendré des coûts administratifs supplémentaires, mais le déménagement à Athènes, en 2013, du centre opérationnel a permis d’accroître l’efficacité opérationnelle de l’Agence.
4. **Cohérence:** La cohérence entre les activités de l’ENISA et les politiques et activités des parties intéressées a été généralement assurée, aux niveaux national et de l’UE, mais une approche plus coordonnée de la cybersécurité est nécessaire au niveau de l’UE. Les possibilités de coopération entre l’ENISA et d’autres organes de l’UE n’ont pas été pleinement exploitées. L’évolution de l’environnement juridique et politique de l’UE rend le mandat actuel de l’Agence moins cohérent.
5. **Valeur ajoutée européenne:** La valeur ajoutée de l’ENISA résidait d’abord dans la capacité de l’Agence à intensifier la coopération entre les États membres principalement, mais aussi avec les communautés de la sécurité des réseaux et de l’information correspondantes. Il n’y a aucune autre entité au niveau de l’UE qui favorise la coopération d’autant de parties intéressées par la sécurité des réseaux et de l’information. La valeur ajoutée procurée par l’Agence a varié en fonction des besoins et des ressources des parties intéressées (grands États membres par opposition aux petits États membres, États membres par opposition aux entreprises, par exemple) et de la nécessité, pour l’Agence, de hiérarchiser ses activités selon le programme de travail. Il est ressorti de l’évaluation qu’une éventuelle disparition de l’ENISA constituerait une occasion manquée pour tous les États membres. Il serait impossible d’assurer la création de communautés et une coopération aussi poussée de tous les États membres en matière de cybersécurité sans une agence de l’UE décentralisée. La situation serait plus diverse et des formes de coopération bilatérale ou régionale feraient leur apparition pour combler le vide laissé par l’ENISA.

# Conclusions/Recommandations

Il ressort de l’évaluation que le règlement a confié à l’ENISA un mandat très large, qui laisse une certaine souplesse mais est, à certains égards, insuffisamment détaillé, limitant ainsi la capacité de l’Agence à exercer une grande influence, et que les objectifs qui lui étaient fixés se sont révélés pertinents au cours de la période 2013-2016. L’Agence est parvenue à atteindre un bon niveau d’efficacité et a démontré la valeur ajoutée de l’action au niveau de l’UE, en particulier par l’intermédiaire d’activités essentielles telles que les exercices de cybersécurité paneuropéens, le soutien à la communauté des CSIRT ou les analyses du paysage des menaces. Elle a contribué à renforcer la sécurité des réseaux et de l’information en Europe en soutenant la coopération entre les États membres et les parties prenantes dans le domaine de la sécurité des réseaux et de l’information, ainsi que par ses activités de création de communautés et de dotation de moyens.

L’Agence a réussi à obtenir ces résultats en dépit de nombreuses difficultés, décrites dans les paragraphes précédents du présent rapport et dans le document de travail des services de la Commission ci-joint. L’une des principales difficultés tenait aux ressources limitées dont disposait l’Agence, qui n’étaient pas proportionnées à l’ampleur de son mandat, notamment eu égard aux nombreuses missions qui lui ont été confiées par la directive SRI et à l’évolution rapide du paysage des menaces. L’ENISA reste aussi la seule agence de l’Union européenne dont le mandat ait une durée limitée, en dépit, notamment, des missions qui lui ont été assignées par la directive SRI, comme indiqué plus haut.

Le paysage des menaces dans le domaine de la cybersécurité évolue rapidement. De nouvelles menaces apparaissent alors que la dépendance de l’Europe à l’égard des infrastructures et des services numériques s’accroît, non seulement en raison des dispositifs connectés mais aussi d’une connectivité désormais omniprésente. L’internet des objets ouvre de nouvelles perspectives dans le domaine de l’efficacité énergétique, de la protection de l’environnement, de la mobilité connectée, du suivi en temps réel de paramètres de santé et des transactions financières intelligentes et sans discontinuité dans l’économie et la société numériques. Malheureusement, cette dynamique du marché s’accompagne de nouvelles vulnérabilités et de nouveaux exploits permettant à des dispositifs dont la sécurité serait compromise de perturber le marché unique numérique.

Il ressort de l’évaluation que le mandat actuel ne permet pas de doter l’ENISA des outils nécessaires pour faire face aux défis actuels et futurs en matière de cybersécurité.

En outre, compte tenu du nombre d’acteurs européens dans le domaine de la cybersécurité et du manque de coordination entre eux, le risque de voir s’accentuer le morcellement au niveau de l’UE s’accroît. L’UE doit se doter d’un centre de liaison pour faire face à de nouvelles menaces qui sont transversales par nature et concernent de multiples secteurs d'activité, et pour répondre aux besoins de la communauté de la cybersécurité, en particulier des États membres, des institutions de l’UE et des entreprises. Selon les conclusions de l’évaluation, il est nécessaire de créer une agence de l’UE organisée sur une base transversale/intersectorielle et de la doter d’un mandat fort.

L’évaluation montre que, malgré un certain nombre de difficultés, si l’ENISA est dotée d’un mandat suffisant et d’un soutien adéquat en ce qui concerne les ressources financières et humaines, elle possède le potentiel nécessaire pour contribuer à renforcer la cybersécurité dans l’UE.

Le besoin d’établir une coopération et une coordination entre les différentes parties intéressées apparaît aussi clairement. La nécessité de disposer, au niveau de l’UE, d’une entité de coordination chargée de faciliter les flux d’information, de combler les lacunes et d’éviter tout chevauchement des rôles et des responsabilités devient de plus en plus pressante. L’ENISA, en tant qu’agence décentralisée de l’UE et intermédiaire neutre, est en mesure de coordonner l’approche de l’UE en matière de cybermenaces.

Compte tenu de ce qui précède, la Commission a présenté une proposition visant à réformer l’ENISA et à la doter d’un mandat permanent qui se fonde sur les points forts de l’Agence et les nouveaux domaines d’action prioritaires, par exemple dans le domaine de la certification de cybersécurité. Ce nouveau mandat devrait tenir compte de l’évolution de la situation et donner à l’Agence les moyens d’apporter à l’UE, dans l’avenir, une assistance adaptée aux besoins.

1. <http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32013R0526&from=EN> [↑](#footnote-ref-1)
2. <http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L1148&from=EN> [↑](#footnote-ref-2)
3. Communication de la Commission européenne «Renforcer le système européen de cyber-résilience et promouvoir la compétitivité et l’innovation dans le secteur européen de la cybersécurité», COM(2016) 410 final. [↑](#footnote-ref-3)
4. Conclusions du Conseil intitulées «Renforcer le système européen de cyber-résilience et promouvoir la compétitivité et l’innovation dans le secteur européen de la cybersécurité», 15 novembre 2016. [↑](#footnote-ref-4)
5. COM (2015)215final; SWD (2015)111 final;

<http://ec.europa.eu/smart-regulation/guidelines/docs/swd_br_guidelines_en.pdf> [↑](#footnote-ref-5)