RAPPORT SPÉCIAL 19/2026 **FR**

Incidents de cybersécurité: détection et réaction

Le cadre de coopération de l'UE progresse, mais son efficacité reste partielle en raison de retards de mise en œuvre et d'un partage d'informations limité

CURIA RATIONUM
COUR DES COMPTES EUROPÉENNE

Table des matières

Points

Annexes

Sigles, acronymes et abréviations

Glossaire

Réponses de la Commission

Réponses du Centre de compétences européen en matière de cybersécurité (ECCC)

Réponses de l'Agence de l'Union européenne pour la cybersécurité (ENISA)

Calendrier

L'équipe d'audit

01 Principaux messages

Pourquoi ce thème est-il important?

01 Alors que nous passons à une économie et à un quotidien toujours plus numériques, les risques de cyberattaques vont croissant. La cybersécurité, à savoir «les actions nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces»[1], nécessite d'adopter une approche globale pour prévenir ces menaces, les détecter, y réagir et s'en rétablir.

02 Le paysage de la cybersécurité de l'UE englobe un grand nombre d'acteurs civils publics et privés aux niveaux régional et national, ainsi qu'à celui de l'UE. La cybersécurité est également un rouage essentiel de la sécurité et de la défense nationales.

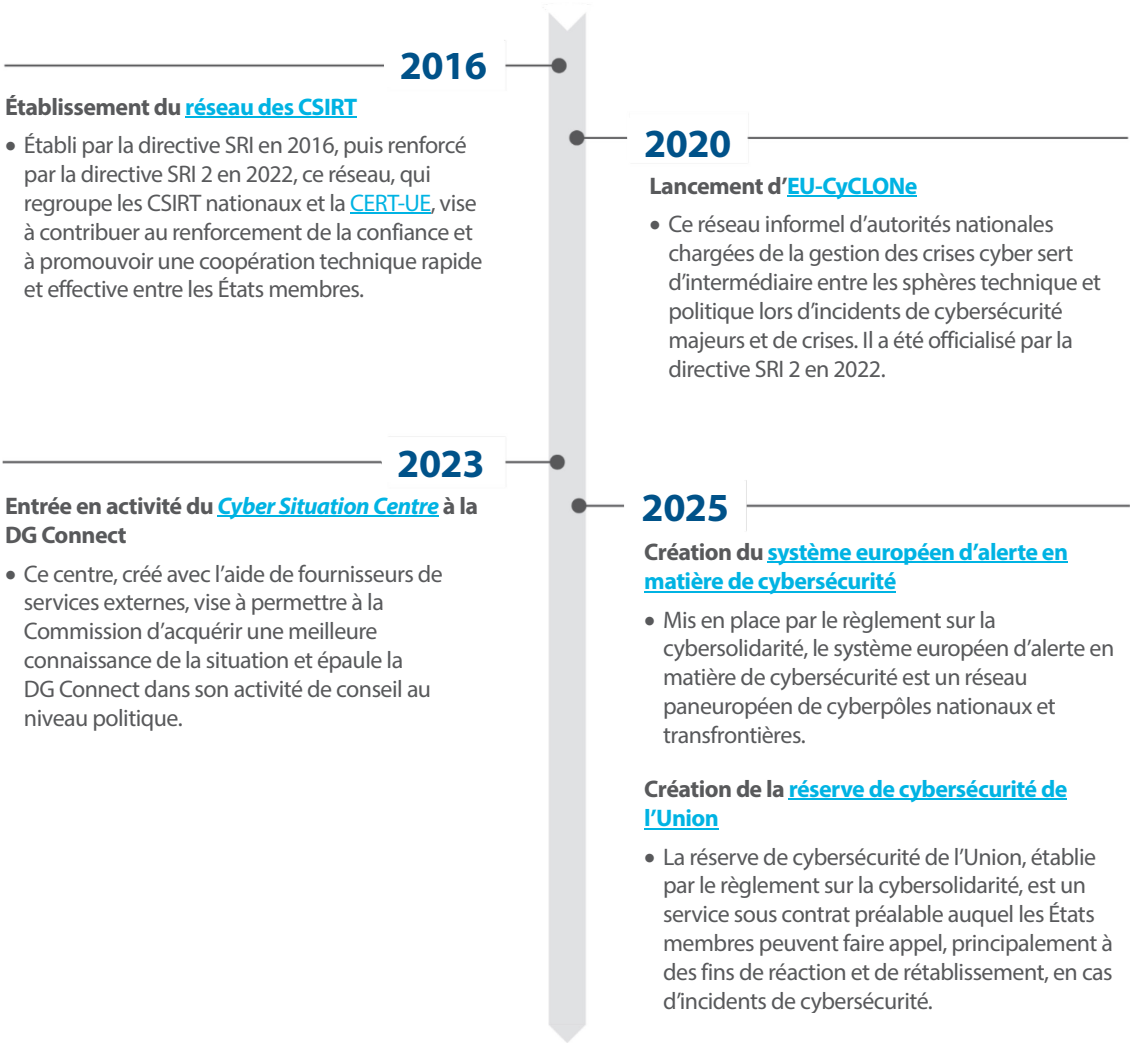
03 La prévention des incidents et des crises dans le domaine de la cybersécurité ainsi que la préparation et la réaction en la matière relèvent au premier chef de la responsabilité des États membres. Les cyberincidents étant susceptibles de perturber le bon fonctionnement du marché intérieur, l'UE a elle aussi un rôle important à jouer en cas d'incident important ou de crise. Ces dernières années, elle a renforcé son cadre réglementaire en matière de cybersécurité[2], qui évolue constamment, et a mis en place divers réseaux et mécanismes, comme le montrent la ***figure 1*** et l'***annexe II***.

---

[1] Règlement (UE) 2019/881 (règlement sur la cybersécurité).

[2] Elle a ainsi présenté des propositions concernant un règlement omnibus numérique, en novembre 2025, et un règlement sur la cybersécurité révisé, en janvier 2026.

Figure 1 | Réseaux et mécanismes de cybersécurité de l'UE, de 2016 à 2025



CSIRT: centres de réponse aux incidents de sécurité informatique
DG Connect: direction générale des réseaux de communication, du contenu et des technologies
EU-CyCLONe: réseau européen pour la préparation et la gestion des crises cyber
Directive SRI: directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union
Directive SRI 2: directive (UE) 2022/2555 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union

Source: Cour des comptes européenne.

04 Dans le cadre financier pluriannuel en cours, celui de la période 2021-2027, le programme pour une Europe numérique (DIGITAL) est la principale source de financement dans le domaine de la cybersécurité. Il est doté d'un budget total de 8,1 milliards d'euros, dont 1,4 milliard d'euros affectés au renforcement de la cybersécurité.

05 Notre audit a visé à évaluer si l'action de l'UE facilitait efficacement la détection des incidents de cybersécurité importants et majeurs et la réaction à ces incidents. Nous avons en particulier examiné si tel était le cas:

- des réseaux et mécanismes au niveau de l'UE, à savoir le réseau des centres de réponse aux incidents de sécurité informatique (réseau des CSIRT), le réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONe), le système européen d'alerte en matière de cybersécurité, le *Cyber Situation Centre* et la réserve de cybersécurité de l'Union;
- des actions financées au titre du programme DIGITAL.

06 Nous pensons que nos constatations contribueront à renforcer la cyberrésilience de l'UE en rendant ses réseaux et mécanismes plus efficaces et efficients, ainsi qu'à améliorer la sélection et le suivi des actions qu'elle finance.

07 Notre audit a couvert la période allant de 2022 à 2025. Il a reposé sur un contrôle sur pièces, une analyse de documents pertinents, des visites d'audit dans trois États membres (l'Irlande, la Grèce et l'Italie), des questionnaires écrits et des entretiens avec des parties prenantes du domaine. L'***annexe I*** contient davantage d'informations générales et de précisions sur l'étendue et l'approche de l'audit.

Quelles sont nos constatations et nos recommandations?

08 Globalement, nous concluons que l'action de l'UE ne facilite que partiellement la détection des incidents de cybersécurité importants et majeurs et la réaction à ces incidents. Un cadre de coopération a été élaboré au fil des ans, mais les travaux nécessaires pour le rendre entièrement opérationnel se poursuivent toujours. Un partage d'informations limité, des faiblesses dans les signalements et des retards considérables dans la mise en œuvre empêchent les réseaux et mécanismes de l'UE d'atteindre leur plein potentiel. Les projets financés au titre du programme DIGITAL poursuivent des objectifs pertinents, mais certains se heurtent à des difficultés opérationnelles ou subissent des retards, tandis que le cadre global de suivi de la performance présente des faiblesses.

09 L'ensemble actuel de réseaux et de mécanismes de l'UE destinés à faciliter la détection des incidents de cybersécurité importants et la réaction à ces incidents s'est développé graduellement. En 2025, le Conseil a adopté le schéma directeur en matière de cybersécurité, qui définit le cadre de l'Union pour la gestion des crises de cybersécurité et qui, d'après nos constatations, présente avec une grande clarté les rôles et les responsabilités dans la gestion desdites crises par l'UE. Cependant, les modalités procédurales de la collaboration entre le réseau des CSIRT (établi en 2016) et EU-CyCLONe (officialisé en 2023) n'ont pas encore été formellement adoptées (points ***24*** à ***30***).

10 Nous avons constaté que le partage d'informations via ces réseaux était limité. Cela s'explique principalement par des retards dans la transposition de la directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (directive SRI 2), des difficultés pour déterminer si un incident a un impact transfrontière, et des restrictions du partage d'informations, posées par la législation sur la sécurité nationale. La valeur ajoutée des réseaux est considérablement réduite si les États membres ne sont pas disposés à partager en temps utile des informations sur la base desquelles agir (points ***31*** à ***44***).

Recommandation n° 1

Renforcer le partage d'informations entre les États membres

Pour améliorer la détection des cyberincidents et la réaction à ces incidents, la Commission, avec l'aide de l'Agence de l'Union européenne pour la cybersécurité (ENISA), devrait:

a) inviter le groupe de coopération sur la sécurité des réseaux et de l'information à réaliser une analyse détaillée des restrictions, liées à la sécurité nationale, qui limitent le partage d'informations et entravent la cyberrésilience de l'UE, et à trouver des solutions juridiques et techniques pour intensifier le partage d'informations tout en restant dans les limites autorisées par la sécurité nationale;

b) sans préjudice des décisions des colégislateurs, agir conjointement avec les États membres pour faire en sorte que le guichet unique pour le signalement des incidents prévu dans la proposition de règlement omnibus numérique soit apte à détecter les incidents transfrontières potentiels;

c) concevoir des solutions qui permettent de signaler les incidents à l'ENISA en temps réel.

Quand? a) et b) d'ici fin 2027; c) d'ici fin 2028.

11 En 2022, la Commission a créé son centre de situation en matière de cybersécurité (le *Cyber Situation Centre*) destiné à améliorer son appréciation de la situation et, ainsi, à faciliter l'exercice de ses responsabilités institutionnelles dans la gestion des crises. Le fonctionnement du centre est, dans une large mesure, assuré au moyen d'un contrat conclu avec des fournisseurs de services externes. Nous avons constaté que les travaux de ces fournisseurs font partiellement double emploi avec les capacités existantes de l'ENISA en matière d'appréciation de la situation et de surveillance des menaces. Selon nous, les opérations du centre n'ont pas été organisées de manière à tirer suffisamment parti des possibilités de rationalisation en exploitant les données déjà disponibles auprès de la Commission et de l'ENISA. En outre, l'absence d'un plan détaillé et complet concernant l'avenir du centre après la fin du contrat met en péril son exploitation après 2026 (points ***45*** à ***51***).

Recommandation n° 2

Rationaliser les capacités d'appréciation de la situation en matière de cybersécurité et optimiser la diffusion des informations

Pour davantage d'efficience, la Commission devrait collaborer avec l'ENISA pour évaluer la faisabilité d'une acquisition et d'une analyse conjointes d'informations à des fins d'appréciation de la situation. Elle devrait également diffuser ces informations et les rapports sur les cybermenaces correspondants dans l'ensemble des services et organismes compétents de l'UE.

Quand? D'ici fin 2027.

12 Le règlement sur la cybersolidarité adopté en 2024 institue la réserve de cybersécurité de l'Union, qui vise à aider les États membres à réagir aux cyberincidents de grande ampleur et à s'en rétablir. La réserve est constituée de fournisseurs de services sélectionnés pour chaque État membre et aptes à réagir aux incidents 24 heures sur 24. S'il est vrai que cette approche contribue à établir la confiance et à répondre aux exigences particulières des différents États membres, le budget disponible est réparti à parts égales entre ces derniers, sans tenir compte des besoins spécifiques de chacun d'eux (points ***52*** à ***57***).

13 Selon nous, le recours à des fournisseurs sous contrat préalable permet un déploiement rapide des services de réaction aux incidents. La réserve de cybersécurité de l'Union vise essentiellement à soutenir la réaction et le rétablissement, mais lorsqu'elle n'est pas exploitée à des fins de réaction aux incidents, elle peut l'être dans un but de préparation. Cette approche flexible peut empêcher des services prépayés de rester inutilisés, mais s'accompagne du risque que, contrairement à ce qui en était attendu, la réserve de cybersécurité de l'Union serve principalement à des fins de préparation et non de réaction (points *58* à *61*).

14 Le système européen d'alerte en matière de cybersécurité est un réseau de cyberpôles nationaux et transfrontières destiné à améliorer la détection et l'analyse des cybermenaces, ainsi que la réaction face à ces menaces. Nous avons constaté qu'au moment de l'audit, en raison de retards considérables dans la passation de marchés pour l'acquisition d'outils et de services, les deux pôles (ATHENA et ENSOC) n'étaient pas encore opérationnels, et que le système européen d'alerte en matière de cybersécurité ne fonctionnait pas encore (points *62* à *70*).

15 Un des objectifs essentiels du système européen d'alerte en matière de cybersécurité consiste à favoriser le partage d'informations utiles entre petits groupes d'États membres. Cela pourrait permettre de résoudre certains des problèmes liés au partage d'informations, mais l'intégration des cyberpôles dans un paysage de cybersécurité déjà complexe comportera, elle aussi, des difficultés considérables. Nous avons constaté que les accords de coopération réglementaires, la taxonomie commune et les normes d'interopérabilité nécessaires au plein fonctionnement du système européen d'alerte en matière de cybersécurité n'étaient pas encore en place (points *71* à *74*).

Recommandation n° 3

Intégrer le système européen d'alerte en matière de cybersécurité dans le paysage de l'UE

La Commission, l'ENISA et les États membres devraient veiller à ce que des modalités de coopération et des normes d'interopérabilité soient établies, afin de faciliter le partage d'informations entre les cyberpôles transfrontières du système européen d'alerte en matière de cybersécurité, le réseau des CSIRT et EU-CyCLONe.

Quand? D'ici fin 2028.

16 La Commission a proposé, en 2018, de créer le Centre de compétences européen en matière de cybersécurité (ECCC) et de le charger de gérer le volet «cybersécurité» du programme DIGITAL à partir de 2021. Le règlement qui a établi l'ECCC appelait à la création d'une communauté des compétences en matière de cybersécurité rassemblant des représentants de l'industrie, d'institutions académiques et de recherche. Des membres sélectionnés au sein de cette communauté formeraient ensuite un groupe consultatif stratégique (points ***75*** et ***76***).

17 Nous avons constaté que l'autonomie financière de l'ECCC, ainsi que la création de la communauté des compétences en matière de cybersécurité et du groupe consultatif stratégique avaient été retardées, si bien que la communauté et le groupe consultatif n'avaient pas pu contribuer à l'élaboration des programmes de travail destinés à DIGITAL. À nos yeux, cela a constitué une occasion manquée (points ***77*** à ***81***).

18 D'après nos constatations, tous les projets que nous avons examinés poursuivaient des objectifs pertinents qui contribuaient à la réalisation des objectifs de DIGITAL en matière de cybersécurité. Dans certains cas, toutefois, la qualité ou les résultats obtenus n'étaient pas satisfaisants, et ce principalement en raison de retards de mise en œuvre (points ***82*** à ***87***).

19 Le règlement établissant le programme DIGITAL dispose que, pour des raisons de sécurité, il est possible de restreindre le bénéfice des financements en faveur de la cybersécurité aux entités établies dans les États membres de l'UE et contrôlées par ces mêmes États ou par des ressortissants de ces États. Le service central de validation, à l'Agence exécutive européenne pour la recherche, se charge de cette évaluation du contrôle et de la propriété pour le compte de l'ECCC (points ***88*** à ***91***).

20 En cas de soutien financier à des tiers, l'évaluation du contrôle et de la propriété incombe aux bénéficiaires du projet, qui appliquent leur propre approche et leur propre méthode. Nous avons constaté que l'ECCC ne validait pas ces méthodes, pas plus qu'il n'effectue de contrôles afin de vérifier que les tiers sélectionnés pour bénéficier du soutien sont effectivement détenus et contrôlés par des États membres ou des citoyens de l'UE. Selon nous, il existe un risque non négligeable que les bénéficiaires ne soient pas à même d'opérer correctement ces contrôles. Ce risque, qui n'a pas été atténué de manière adéquate, pourrait entraîner la mise en danger d'éléments sensibles tels que des infrastructures, des données opérationnelles et des technologies essentielles à la sécurité (points ***92*** à ***96***).

Recommandation n° 4

Garantir une évaluation rigoureuse du contrôle et de la propriété des entités qui reçoivent des fonds de l'UE dans le cadre du programme pour une Europe numérique

Le Centre de compétences européen en matière de cybersécurité devrait:

a) obtenir une assurance raisonnable que les bénéficiaires qui apportent un soutien financier à des tiers disposent des capacités administratives et techniques nécessaires pour effectuer des évaluations appropriées du contrôle et de la propriété en suivant la méthode mise à leur disposition;

b) vérifier, sur la base d'un échantillon, si les entités qui ont reçu des fonds de l'UE sont toutes éligibles.

Quand? a) d'ici fin 2026; b) d'ici fin 2027.

21 Les bénéficiaires qui gèrent des projets financés par l'UE doivent rendre compte à l'ECCC de leur avancement et de leurs résultats, mesurés en fonction de jalons et d'éléments livrables. Ceux-ci sont essentiels pour le suivi des projets et doivent être définis de manière appropriée. Nous avons constaté que les instructions relatives au libellé des jalons et des éléments livrables n'avaient été suivies dans presque aucun des projets de notre échantillon, et que parmi ces jalons et éléments livrables, beaucoup n'étaient pas utiles pour suivre les progrès accomplis (points ***97*** à ***99***).

22 D'après ce que nous avons pu observer, beaucoup des indicateurs de performance utilisés par les bénéficiaires ne sont pas pertinents ou pas mesurables et sont dépourvus de valeur cible ou de valeur de référence. En outre, les informations communiquées concernant ces indicateurs laissent à désirer et ne peuvent donc pas servir de base pour évaluer la performance des projets (points ***100*** à ***102***).

23 Le suivi des réalisations de DIGITAL dans son ensemble nécessite que des informations sur des indicateurs de programme spécifiques, utilisés par la Commission pour établir chaque année ses fiches de performance des programmes, soient fournies pour chaque projet. L'ECCC est chargé de collecter et de vérifier les données relatives à ces indicateurs. Nous avons relevé de nombreuses insuffisances dans les modalités de leur collecte et dans leur qualité générale. Nous n'avons trouvé aucun élément probant attestant que l'ECCC ait vérifié l'exactitude des données communiquées. Sur la base de nos contrôles par sondage, nous estimons que les données fournies ne rendent pas fidèlement compte des résultats obtenus (points ***103*** à ***106***).

Recommandation n° 5

Renforcer le cadre de suivi de la performance du volet «cybersécurité» du programme pour une Europe numérique

Pour permettre un suivi approprié des progrès et de la performance, le Centre de compétences européen en matière de cybersécurité devrait:

a) vérifier, avant la signature de la convention de subvention, que des jalons, des éléments livrables et des indicateurs de performance conformes aux instructions figurant dans le formulaire de demande ont été définis pour chaque projet;

b) concevoir et mettre en place un système solide en vue de la collecte, de la traçabilité, de la vérification et de l'agrégation des données destinées aux indicateurs de performance du volet «cybersécurité» du programme pour une Europe numérique, afin de faire en sorte que les indicateurs rendent fidèlement compte des résultats obtenus.

Quand? D'ici fin 2027.

02

Nos observations en détail

Les réseaux et mécanismes de cybersécurité de l'UE facilitent certes la coopération et la réaction, mais un partage d'informations limité et une application incomplète réduisent leur efficacité

Les réseaux de l'UE créent les conditions de la coopération entre les États membres, mais un partage d'informations limité réduit leur valeur ajoutée

24 L'ensemble actuel de réseaux et de mécanismes de l'UE destinés à faciliter la détection des incidents de cybersécurité importants et la réaction à ces incidents s'est développé graduellement depuis l'entrée en vigueur, en août 2016, de la directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union[3] (directive SRI). Une représentation du paysage actuel de l'UE dans ce domaine figure à l'***annexe II***.

[3] Directive (UE) 2016/1148.

Les réseaux de l'UE permettent aux États membres de coopérer aux niveaux technique et opérationnel

25 Le réseau des centres de réponse aux incidents de sécurité informatique (réseau des CSIRT) a été institué par la directive SRI. Il regroupe la CERT-UE (le service de cybersécurité pour les institutions, organes et organismes de l'Union) et les CSIRT désignés par les États membres, et vise à renforcer la confiance entre les CSIRT nationaux ainsi qu'à promouvoir une coopération opérationnelle rapide et effective entre les États membres.

26 EU-CyCLONe a été établi en 2020 sous la forme d'un réseau de coopération informel destiné aux autorités nationales chargées de la gestion des crises cyber. Il sert d'intermédiaire entre le niveau technique, où opère le réseau des CSIRT, et le niveau politique, celui du Conseil de l'Union européenne et de son dispositif intégré pour une réaction au niveau politique dans les situations de crise. La directive SRI 2, entrée en vigueur en 2023, a officialisé le rôle d'EU-CyCLONe et lui a conféré un mandat clair.

27 Nous avons examiné si les rôles et les responsabilités de ces réseaux du niveau de l'UE sont bien définis et s'ils créent les conditions d'une coopération entre les États membres.

28 L'ENISA assure le secrétariat du réseau des CSIRT ainsi que d'EU-CyCLONe. Elle leur fournit les ressources, l'expertise, l'infrastructure et les outils informatiques nécessaires à la coopération et aux communications sécurisées en vue du partage d'informations. Dans son enquête sur la satisfaction des parties prenantes[4] réalisée début 2025, elle a obtenu de bonnes notes pour la réalisation de sa mission de secrétariat de ces réseaux. Ce retour positif a également été confirmé lors de nos visites d'audit, au cours desquelles les autorités nationales chargées de la cybersécurité ont fait part de leur satisfaction.

[4] Rapport annuel d'activités consolidé de l'ENISA relatif à 2024, p. 33 et 36.

29 En 2025, le Conseil a adopté le schéma directeur en matière de cybersécurité, qui définit les rôles et les responsabilités des principaux acteurs (y compris le réseau des CSIRT et EU-CyCLONe) ainsi que les mécanismes concernés aux différentes étapes d'un cyberincident majeur ou d'une crise cyber. Nous avons constaté que ce schéma directeur présentait avec une grande clarté les rôles et les responsabilités dans la gestion des crises de cybersécurité par l'UE et qu'il tenait compte de l'évolution du paysage depuis l'adoption du premier document de ce type, en 2017. Il définit trois niveaux de coopération: le niveau technique, le niveau opérationnel et le niveau politique. Il décrit en détail les nouveaux réseaux et structures mis en place après 2017 (comme EU-CyCLONe, les équipes d'intervention rapide de l'UE en cas de menaces hybrides et le système européen d'alerte en matière de cybersécurité) et aborde la manière dont la gestion des crises de cybersécurité devrait être intégrée dans le cadre de l'UE pour la réaction aux crises en général.

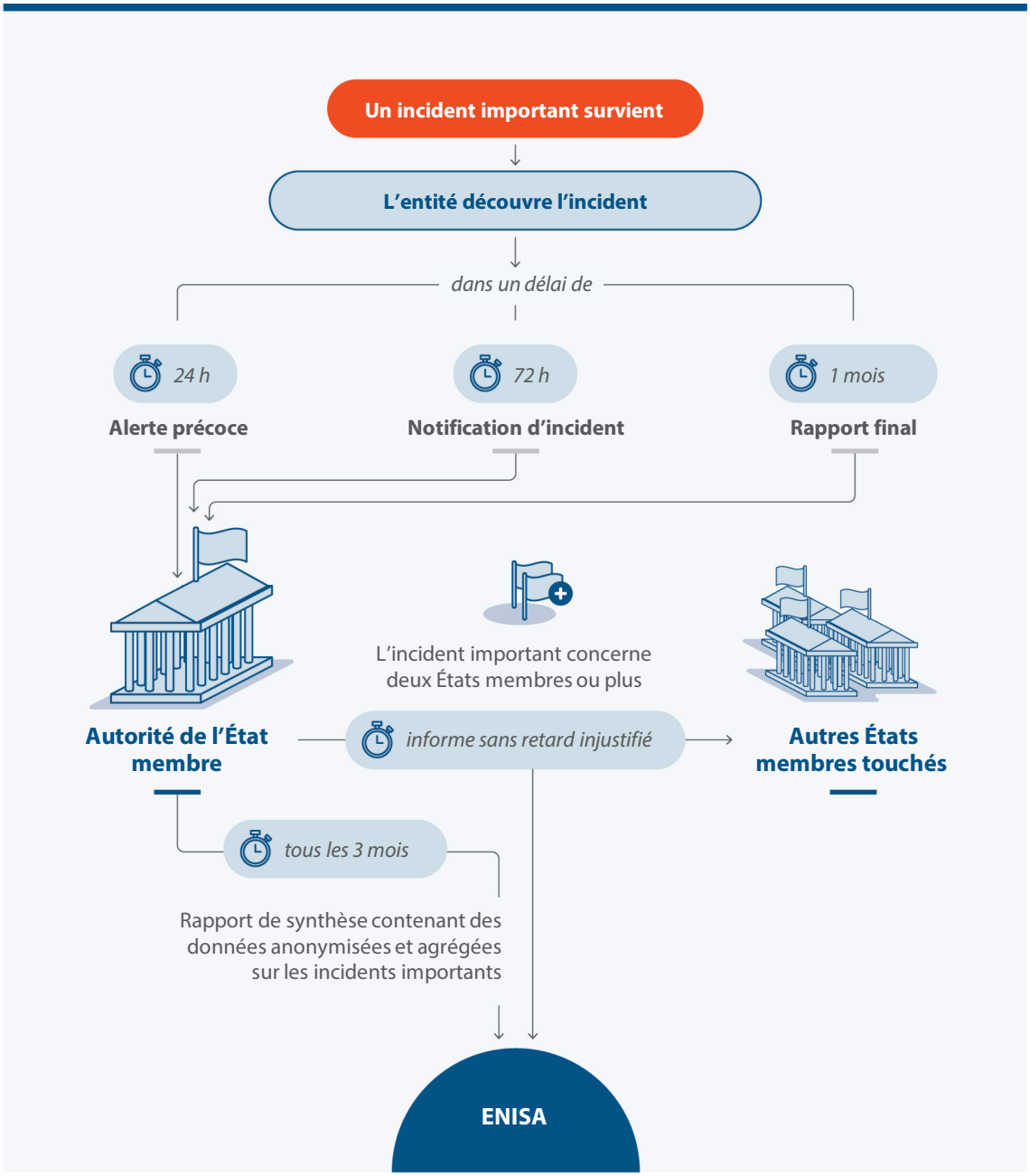
30 Cependant, bien qu'officiellement établis en 2016 et en 2023, respectivement, le réseau des CSIRT et EU-CyCLONe n'ont pas encore formalisé les modalités procédurales de leur collaboration. Ils ne sont pas non plus convenus des critères que le réseau des CSIRT doit appliquer pour informer EU-CyCLONe qu'un incident de cybersécurité observé constitue un incident de cybersécurité majeur, potentiel ou en cours. Il leur reste aussi à se mettre d'accord sur une taxonomie commune des niveaux de gravité des incidents et des concepts clés (tels que ceux de «menace», d'«acteur de menaces», d'«incident» ou d'«impact»), nécessaire en vue d'un échange automatisé d'informations. Actuellement, les conditions dans lesquelles un incident est à considérer comme «important» ou «majeur» ne sont pas définies de manière univoque. Les autorités chargées de la cybersécurité dans les trois États membres où nous nous sommes rendus ont toutes souligné cette absence de taxonomie commune.

Le partage d'informations et les signalements sont limités, ce qui réduit considérablement la valeur ajoutée des réseaux de l'UE

31 Les frontières géographiques n'empêchent pas la survenue et la propagation des cyberincidents et des cyberattaques. Le partage, par les États membres, d'informations relatives, par exemple, aux tactiques et techniques employées par les acteurs de menaces, et aux signes numériques révélateurs d'une intrusion dans un réseau ou un système d'information («indicateurs de compromission»), peut contribuer de façon non négligeable au renforcement de la cybersécurité.

32 Nous avons constaté que le partage d'informations était limité et que la valeur ajoutée des réseaux de l'UE était, de ce fait, fortement réduite. Les insuffisances que nous avons observées sont principalement liées à des retards dans la transposition de la directive SRI 2, à des difficultés pour déterminer si un incident a un impact transfrontière, à des restrictions du partage d'informations dues aux législations sur la sécurité nationale, et à un manque de confiance. La directive SRI 2 impose plusieurs obligations d'information aux entités auxquelles elle est applicable, ainsi qu'aux autorités des États membres (voir ***figure 2***).

Figure 2 | Délais de communication d'informations sur les incidents en vertu de la directive SRI 2



Source: Cour des comptes européenne, sur la base d'informations fournies par l'ENISA.

33 Les États membres devaient transposer la directive SRI 2 en droit national avant la fin d'octobre 2024, mais seuls deux d'entre eux ont respecté le délai. Ces retards de transposition ont des répercussions considérables sur le partage d'informations parce que, tant que la directive n'a pas été transposée, les entités auxquelles elle s'applique ne sont pas légalement tenues de déclarer les incidents. D'après les estimations de la Commission[5], 15 500 entités étaient assujetties à la directive SRI, alors que plus de 110 000 le sont à la directive SRI 2. Par exemple, l'administration publique – le secteur le plus ciblé par des attaques dans l'UE, d'après le rapport 2025 sur le paysage des menaces de l'ENISA – n'avait aucune obligation de signaler les incidents en vertu de la directive SRI.

34 Le fait que les données sur les incidents sont communiquées à l'ENISA tous les trois mois (c'est-à-dire, dans certains cas, longtemps après l'incident) limite leur valeur ajoutée. Ces données sont principalement utilisées à des fins statistiques et pour établir des rapports historiques sur les tendances, pas pour améliorer la détection et la réaction. L'ENISA met un outil en ligne à la disposition des États membres pour la transmission de leurs rapports. Le modèle de rapport contient un ensemble minimal de données à fournir, comme le type d'incident et le secteur touché. En outre, l'ENISA suggère aux États membres de communiquer d'autres informations pour permettre une analyse plus approfondie des données, par exemple en reliant les incidents à des vulnérabilités précises. Cependant, les États membres ne décident pas tous de fournir ces informations, et la qualité ainsi que la valeur ajoutée des données collectées en pâtissent.

35 Dans son rapport 2024 sur l'état de la cybersécurité dans l'Union, l'ENISA a indiqué que les incidents ne sont probablement pas tous signalés, le nombre de ceux qui le sont paraissant modeste. De 2018 à 2021, les États membres lui ont déclaré entre 100 et 500 incidents par an. Ce nombre a augmenté graduellement et a atteint 1 276 en 2024[6].

---

[5] Commission européenne, rapport d'analyse d'impact de 2020.

[6] Données de CIRAS relatives à 2024.

36 Dans son rapport 2025 rapport sur le paysage des menaces, qui couvre la période allant de juin 2024 à juin 2025, l'ENISA a fait état d'environ 4 800 incidents de cybersécurité[7], dénombrés sur la base de renseignements de source ouverte tels que des articles de presse. Il ne s'agissait pas uniquement d'incidents à déclaration obligatoire en vertu de la directive SRI 2, car l'agence collecte également des données sur d'autres types d'incidents. Inversement, un grand nombre d'incidents importants sont absents des renseignements de source ouverte. Les données communiquées par les États membres étant anonymisées, l'ENISA ne peut pas corréler les incidents qu'elle recense avec ceux que signalent les États membres. Il n'est donc pas possible de déterminer avec précision combien d'incidents ne sont pas déclarés, mais selon nous, la différence de nombre entre les incidents notifiés par les États membres et ceux mentionnés dans le rapport sur le paysage des menaces prouve que les incidents importants ne sont pas tous signalés.

37 Le nombre de notifications d'incidents transfrontières importants adressées aux autres États membres touchés et à l'ENISA laisse supposer, lui aussi, que les incidents ne sont pas tous signalés. La directive SRI contenait une disposition concernant ces notifications, mais celle-ci est apparemment restée sans effet, puisque la Commission a conclu[8], en 2020, que les notifications, bien qu'obligatoires, étaient rarement envoyées. Selon elle, cela s'expliquait par l'absence de modalités claires guidant le partage d'informations, et par celle d'objectifs communs encourageant ce partage.

38 L'obligation d'informer les autres États membres est cruciale pour empêcher la propagation des incidents – l'absence de notification compromet la cybersécurité de l'UE. En 2025, seuls 14 incidents transfrontières importants ont été signalés, par sept États membres. En 2024, les États membres ont présenté deux rapports sur des incidents susceptibles d'avoir un impact transfrontière, contre trois rapports en 2022 et aucun en 2023. Cela montre que le nombre d'incidents transfrontières importants déclarés reste très faible et ne rend pas compte de la réelle ampleur de ces attaques. À titre de comparaison, l'ENISA a fait état, dans son rapport 2024 sur le paysage des menaces, de 322 incidents ciblant spécifiquement deux États membres ou plus. L'incident qui a touché Collins Aerospace (voir ***encadré 1***) est un exemple d'attaque que les États membres n'ont pas signalée malgré son impact transfrontière important.

---

[7] Rapport 2025 de l'ENISA sur le paysage des menaces.

[8] Commission européenne, rapport d'analyse d'impact de 2020.

Encadré 1

Perturbation des opérations aéroportuaires à la suite d'un cyberincident

En septembre 2025, Collins Aerospace, un fournisseur de technologie de premier plan dans le secteur de l'aviation, a été victime d'une grave attaque par rançongiciel qui a ciblé son application de contrôle des passagers. De grands aéroports européens ont dû revenir à des opérations manuelles, ce qui a entraîné de très nombreux retards et annulations de vols. Les aéroports qui ont subi les perturbations les plus lourdes sont ceux de Londres Heathrow, de Bruxelles, de Berlin Brandebourg et de Dublin.

D'après la directive SRI 2, un incident est considéré comme «important» si, entre autres, il cause une perturbation opérationnelle grave ou des pertes financières pour l'entité concernée. Cependant, aucun État membre n'a traité cette attaque comme un incident transfrontière important ou majeur, si bien qu'aucun des pays touchés ne l'a officiellement notifiée à l'ENISA ou aux autres États membres. Le réseau des CSIRT n'a pas informé EU-CyCLONe, qui n'a donc pas participé à la gestion coordonnée de l'incident.

Source: Analyse de la Cour des comptes européenne, sur la base d'entretiens avec des représentants de l'ENISA.

39 Une autre raison explique que seul un nombre limité d'incidents transfrontières soient notifiés: il incombe à l'autorité de chaque État membre de déterminer si un incident signalé a un impact transfrontière et, le cas échéant, quels sont les autres États membres touchés. Or les informations dont dispose l'autorité qui effectue le signalement ou celle de l'État membre ne lui permettent pas nécessairement de prendre conscience du caractère transfrontière de l'attaque. Actuellement, il n'existe pas de plateforme au niveau de l'UE qui recevrait des rapports d'incidents en temps réel émanant de tous les États membres et qui pourrait corréler les informations relatives aux différents secteurs ou les indicateurs de compromission afin de détecter les incidents transfrontières. Dès lors, certains incidents transfrontières risquent fort de ne pas être reconnus comme tels et signalés.

40 Depuis 2016, aucun cyberincident n'a été considéré comme «majeur» par un État membre. La définition d'incident majeur recouvre, en principe, tout incident qui a un impact important sur au moins deux États membres. Cependant, même des incidents de cybersécurité qui ont provoqué des pannes d'ampleur mondiale et occasionné des dommages considérables, comme ceux mentionnés à la ***figure 3***, n'ont pas été jugés «majeurs», et la procédure d'intervention par paliers d'EU-CyCLONe n'a jamais été pleinement activée à la suite d'un incident de cybersécurité d'une telle étendue.

Figure 3 | Exemples d'incidents de cybersécurité de grande ampleur

WannaCry

2017

Attaque mondiale par rançongiciel

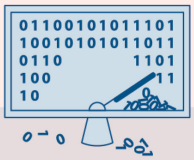
A touché plus de 200 000 ordinateurs dans plus de 150 pays et ainsi, réduit à l'impuissance des exploitants d'infrastructures critiques; cryptait les données sur les appareils touchés et demandait une rançon pour supprimer le cryptage

NotPetya

2017

Maliciel destructeur camouflé en rançongiciel

Conçu pour effacer définitivement les données, avec l'Ukraine pour première cible; s'est rapidement propagé dans le monde entier, paralysant des multinationales et causant des dommages sur toute la planète



Panne informatique liée à CrowdStrike

Juillet 2024

Panne informatique majeure d'ampleur mondiale

Résultat d'une mise à jour défectueuse d'un logiciel d'une entreprise de cybersécurité, CrowdStrike; a fait planter des millions d'ordinateurs

Source: Cour des comptes européenne, d'après des informations de Cloudflare, de l'ENISA, d'Europol, de Wired, d'IBM et de CrowdStrike.

41 Outre l'obligation de signalement imposée aux entités et aux États membres, le réseau des CSIRT a été créé pour faciliter le partage d'informations. Ce réseau, où la communication d'informations repose sur le volontariat, a pour pierre angulaire la confiance entre les États membres. Sa valeur ajoutée est considérablement réduite si ceux-ci ne sont pas disposés à partager en temps utile des informations sur la base desquelles agir.

42 Le partage d'informations au niveau de l'UE est soumis aux restrictions qu'impose la législation de chaque État membre en matière de sécurité nationale. Si un État membre considère comme classifiées les informations liées à une cyberattaque à l'encontre d'une entité critique, ou s'il estime que le signalement d'un incident en particulier porterait atteinte à sa sécurité nationale, il n'est pas tenu de fournir ces informations. Au cours de nos visites dans les États membres, les représentants du réseau des CSIRT et d'EU-CyCLONe ont déclaré que le partage d'informations n'était possible que dans les limites autorisées par la législation sur la sécurité nationale. Aucune analyse des cadres juridiques nationaux des États membres et de leurs incidences sur le partage d'informations n'a été réalisée au niveau de l'UE.

43 En 2016, le réseau des CSIRT se composait de 28 centres nationaux, avec deux représentants par État membre. Le problème du manque de partage des informations a perduré, et la Commission a reconnu, dans son évaluation de la directive SRI, que «les États membres ne partagent pas de manière systématique les informations entre eux», ce qui nuit tout particulièrement à l'efficacité des mesures de cybersécurité et au degré de connaissance collective de la situation au niveau de l'UE. Depuis l'adoption de la directive SRI 2, un grand nombre d'États membres ont désigné des CSIRT sectoriels en plus de leur CSIRT national, si bien que le réseau s'est considérablement étendu. Au moment de l'audit, il regroupait 42 CSIRT et plus de 700 participants individuels. Maintenir des relations étroites entre tous les membres n'est donc pas chose facile, et il est d'autant plus ardu d'établir la confiance.

44 Le réseau des CSIRT a conscience du problème de partage d'informations et étudie diverses mesures destinées à accroître la confiance dans un réseau en expansion. Plutôt qu'un réseau à l'échelle de l'UE, la création de petits groupes d'États membres formant des pôles transfrontières, telle qu'elle est présentée en détail aux points ***62*** à ***74***, pourrait contribuer à résoudre cette difficulté.

Les services sous-traités pour le *Cyber Situation Centre* font double emploi avec certaines capacités existantes, et on ne sait pas au juste comment le centre fonctionnera à l'avenir

45 La directive SRI 2 dispose que, lorsqu'un incident de cybersécurité majeur, potentiel ou en cours, a ou est susceptible d'avoir un impact important, la Commission devient membre d'EU-CyCLONe[9]. Face à ce nouveau rôle et à l'évolution du paysage des menaces, celle-ci a établi, en 2022, une *task force* chargée de la coordination cyber au sein de la DG Connect. La *task force* comprend un centre de situation en matière de cybersécurité (le *Cyber Situation Centre*) qui doit aider la Commission à mieux apprécier la situation et à assumer ses responsabilités institutionnelles dans la gestion des crises. Il doit également épauler la DG Connect dans son activité de conseil au niveau politique.

46 Pour faire fonctionner le *Cyber Situation Centre*, la Commission a, dans une large mesure, recours à des fournisseurs de services externes avec lesquels elle a passé, en décembre 2022, un marché d'une valeur de près de 18 millions d'euros sur quatre ans. Nous avons examiné la mise en place du centre de situation, ses réalisations et les plans de la Commission concernant son exploitation à l'avenir.

[9] Article 16, paragraphe 2, de la directive SRI 2.

47 Dans le cadre des services fournis, les contractants ont créé un tableau de bord fondé sur des flux commerciaux de renseignements sur les cybermenaces, afin de présenter et de partager les informations relatives à celles-ci. Ils établissent également divers rapports de renseignement sur les menaces, dont des rapports quotidiens ou hebdomadaires, et des rapports thématiques consacrés à des pays ou à des secteurs spécifiques de l'économie. Physiquement, le *Cyber Situation Centre*, qui consiste en un local équipé de postes de travail connectés, à distance, au tableau de bord hébergé par les contractants, a été installé dans un bâtiment de la Commission. Au moment de l'audit, ses effectifs se composaient de quelques membres du personnel de la Commission, assistés d'un grand nombre d'analystes employés par les contractants et d'experts de l'ENISA.

48 Nous avons constaté que les travaux effectués par les fournisseurs de services externes pour le *Cyber Situation Centre* faisaient partiellement double emploi avec les capacités existantes de l'ENISA. L'agence est dotée de capacités permanentes en matière d'appréciation de la situation et de surveillance des menaces. Elle publie régulièrement des rapports sur les cybermenaces, y compris des rapports succincts sur des incidents précis et des rapports hebdomadaires donnant une vue d'ensemble des menaces. Les rapports, qui se fondent sur des renseignements de source ouverte, sont similaires à ceux que réalisent les contractants. En temps de crise, l'ENISA rédige en outre des notes d'information de haut niveau à l'intention des décideurs politiques, comparables à celles qu'établit le *Cyber Situation Centre*, ou participe à l'élaboration de telles notes.

49 De plus, les données que le centre de situation utilise pour établir ces rapports trouvent leur source dans des flux commerciaux de renseignements sur les cybermenaces, et sont similaires à celles dont se servent d'autres services de la Commission tels que la direction générale des services numériques et la CERT-UE. Nous estimons que les opérations du *Cyber Situation Centre* n'ont pas été organisées de manière à tirer suffisamment parti des possibilités de rationalisation en exploitant les données dont la Commission et l'ENISA disposent déjà.

50 Le marché arrivera à expiration en décembre 2026, après quoi les contractants n'apporteront plus les services destinés au *Cyber Situation Centre*, qui consistent notamment à fournir les données disponibles dans le tableau de bord, à établir des rapports sur les menaces et à munir le centre de la majeure partie de sa main-d'œuvre. Le tableau de bord sera placé entre les mains de la Commission, mais perdra sa valeur ajoutée s'il n'est pas constamment tenu à jour au moyen de renseignements sur les cybermenaces.

51 Au moment de l'audit, la Commission n'avait pas arrêté de plans concernant la contribution des fournisseurs de services externes à l'exploitation du *Cyber Situation Centre* après l'expiration du marché. À nos yeux, l'absence d'un plan détaillé et complet pour la période qui suivra la fin du contrat met en péril l'exploitation du centre après 2026.

La réserve de cybersécurité de l'Union permet de déployer rapidement des services de réaction aux incidents

52 En 2022, immédiatement après l'agression militaire de la Russie contre l'Ukraine, la Commission, consciente de la fréquence accrue des cyberattaques majeures, a fourni à l'ENISA 15 millions d'euros de financement exceptionnel aux fins du projet pilote relatif à l'action de soutien à la cybersécurité, laquelle a été lancée l'année suivante. Cette même année, la Commission a apporté un supplément de fonds (environ 20 millions d'euros) pour prolonger le programme jusqu'à la fin 2026.

53 La Commission a également présenté la proposition de règlement sur la cybersolidarité – règlement qui a été adopté en décembre 2024 – afin de parer aux incidents de cybersécurité majeurs. Le règlement sur la cybersolidarité établit une réserve de cybersécurité de l'Union composée de services de réaction aux incidents apportés par des fournisseurs de confiance. La réserve est graduellement entrée en service en 2025, avec un budget de 36 millions d'euros pour la période 2025-2027.

54 Nous avons examiné l'organisation de l'action de soutien à la cybersécurité, qui est à la base de la réserve de cybersécurité de l'Union. Nous avons également vérifié si la conception de cette dernière tenait compte des enseignements tirés depuis 2022.

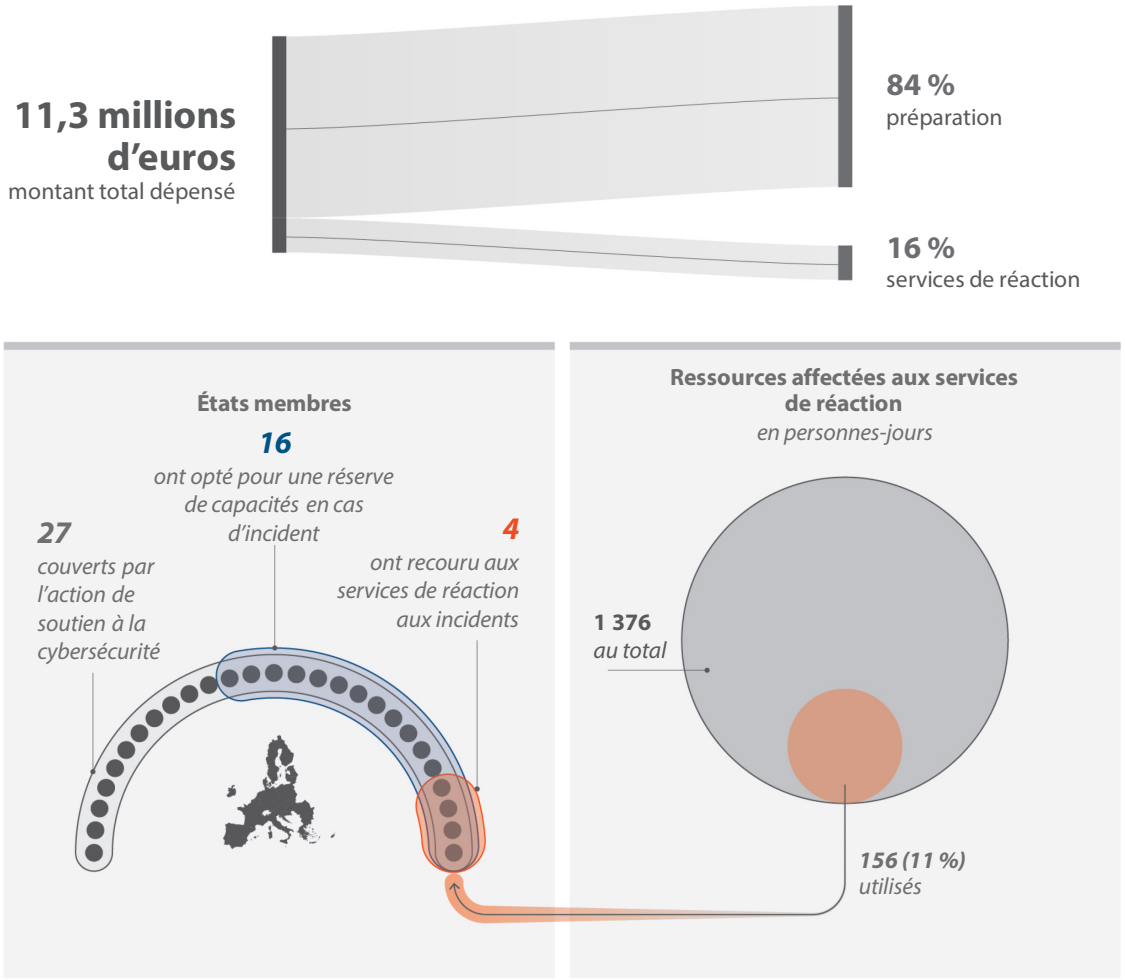
55 L'ENISA a conçu l'action de soutien à la cybersécurité comme un mécanisme destiné à délivrer des services afin de soutenir la préparation et la réaction des États membres aux incidents de cybersécurité majeurs et aux crises cyber. Elle passe des contrats préalables pour tous les services concernés: ainsi, les prestataires peuvent se mettre au travail dès que les États membres en ont besoin. Cette disponibilité tient également à l'organisation de l'ENISA, qui garantit qu'un agent est de garde 24 heures sur 24 pour traiter les demandes des États membres.

56 L'ENISA a décidé de répartir le budget disponible à parts égales entre les États membres. Concrètement, elle a lancé une procédure d'appel d'offres ouverte divisée en 27 lots (un par État membre) afin de sélectionner jusqu'à trois fournisseurs de services de sécurité privés, chargés d'assurer les prestations jusqu'à la fin 2026. Dans le cadre d'un lot paneuropéen, elle a en outre sélectionné des fournisseurs pour apporter ces services aux pays tiers éligibles ainsi qu'aux institutions, organes et organismes de l'Union, et pour faciliter la réaction aux incidents transfrontières.

57 Cette approche a permis à l'agence de tenir compte des exigences nationales spécifiques, dont celles liées à la langue, aux habilitations de sécurité nationales ou à l'implantation effective dans les États membres. Elle présente cependant un inconvénient de taille: puisque les fournisseurs n'ont pas été sélectionnés pour assurer des services dans l'ensemble de l'UE, si un État membre ne recourt pas aux prestations couvertes par les contrats préalables, le budget engagé pour lui fournir les services ne peut pas être utilisé pour venir en aide à autre État membre.

58 Dans le cadre de l'action de soutien à la cybersécurité, trois options ont été proposées aux États membres: des services de préparation, des services de réaction, ou un panachage de ces deux types de services. Les États membres ont choisi d'utiliser l'essentiel des fonds disponibles pour améliorer leur degré de préparation (84 % des dépenses en 2023). Ceux qui ont opté pour une réserve de capacités en cas d'incident (c'est-à-dire un accord préalable, passé avec un fournisseur, qui leur garantit un accès à la demande aux services du fournisseur en vue d'une réaction rapide aux cyberincidents) en ont usé avec modération, comme le montre la ***figure 4***. Dans les trois États membres où nous nous sommes rendus, les autorités se sont déclarées reconnaissantes envers l'ENISA pour sa gestion de l'action de soutien à la cybersécurité.

Figure 4 | L'action de soutien à la cybersécurité de l'ENISA jusqu'en 2023



Source: Cour des comptes européenne, sur la base des données de l'ENISA.

59 Pour la période 2024-2026, seuls neuf États membres ont demandé à disposer d'une réserve de capacités en cas d'incident. Nos entretiens avec des représentants de l'ENISA et des autorités de trois États membres ont permis de confirmer l'existence d'une forte préférence en faveur des actions de préparation.

60 Bien que la réserve de cybersécurité de l'Union vise principalement à soutenir la réaction et le rétablissement en cas d'incident de cybersécurité de grande ampleur, les services affectés au préalable qui relèvent de cette réserve peuvent être convertis en services de préparation s'ils n'ont pas été utilisés à des fins de réaction aux incidents. Cette approche flexible peut empêcher des services prépayés de rester inutilisés.

61 Selon nous, le modèle retenu pour la réserve de cybersécurité de l'Union tire les leçons de l'expérience issue de l'action de soutien à la cybersécurité. Cependant, les données sur le recours à cette action font apparaître le risque que, contrairement à l'objectif qui lui a été assigné dans le règlement sur la cybersolidarité, la réserve de cybersécurité de l'Union serve principalement à des fins de préparation et non de réaction.

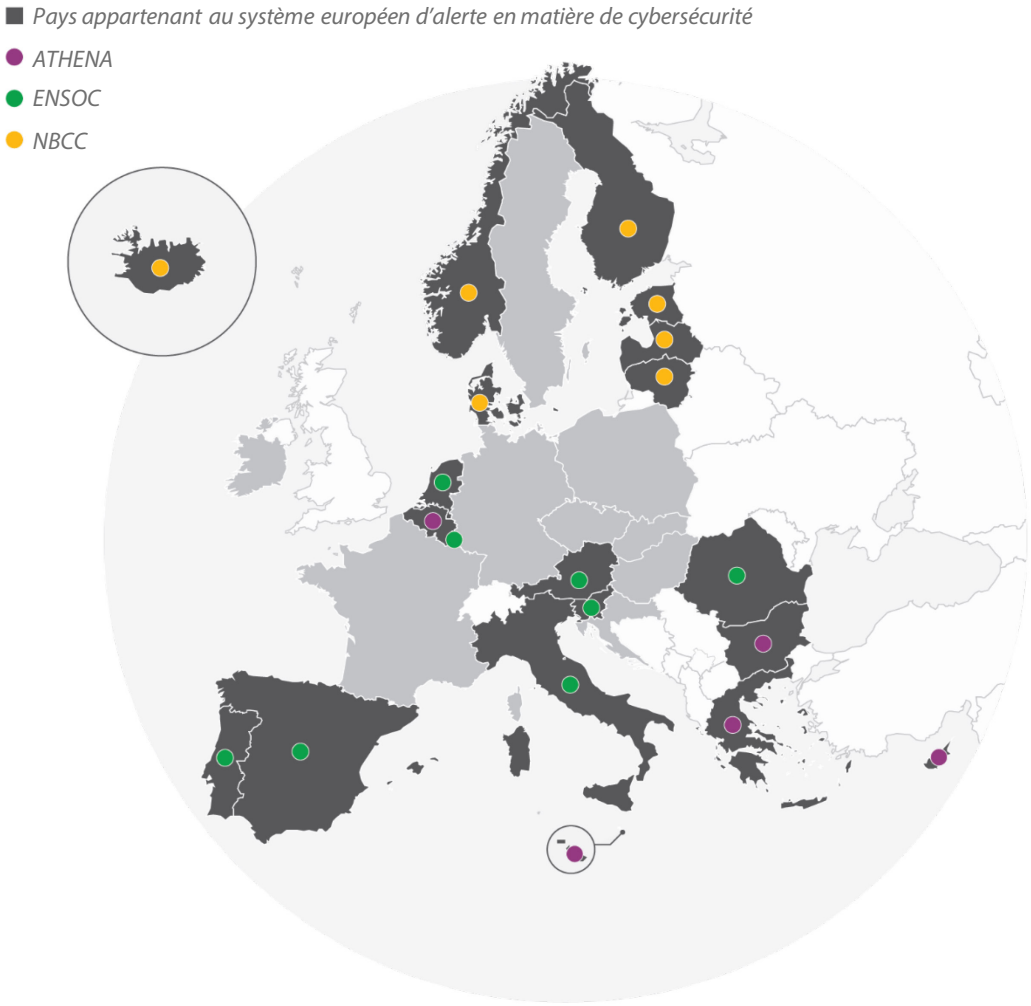
Le système européen d'alerte en matière de cybersécurité vise à renforcer les capacités de détection des menaces, mais il n'est pas opérationnel

62 Un des objectifs essentiels du système européen d'alerte en matière de cybersécurité consiste à favoriser le partage d'informations utiles afin d'améliorer la détection et l'analyse des cybermenaces, ainsi que la réaction face à ces menaces. La participation au système d'alerte est facultative, mais les États membres qui décident d'adhérer à un cyberpôle transfrontière doivent prendre l'engagement de partager les informations pertinentes avec les autres membres du pôle. En collaborant en petits groupes dans un environnement sûr et de confiance, les États membres pourraient éviter certains des problèmes liés au partage d'informations évoqués aux points ***31*** à ***44***.

63 Au moment de l'audit, 13 États membres avaient décidé d'adhérer au système européen d'alerte en matière de cybersécurité. Deux pôles transfrontières avaient ainsi été constitués: ATHENA et ENSOC. En 2026, un troisième cyberpôle transfrontière, NBCC, a bénéficié d'un financement en vue de sa mise en place, si bien que le nombre total de membres du réseau est passé à 20 (18 États de l'UE, ainsi que l'Islande et la Norvège[10]), comme le montre la ***figure 5***.

[10] En tant que pays tiers associés en vertu de l'article 10, paragraphe 1, point a), du règlement (UE) 2021/694.

Figure 5 | Pays appartenant au système européen d'alerte en matière de cybersécurité



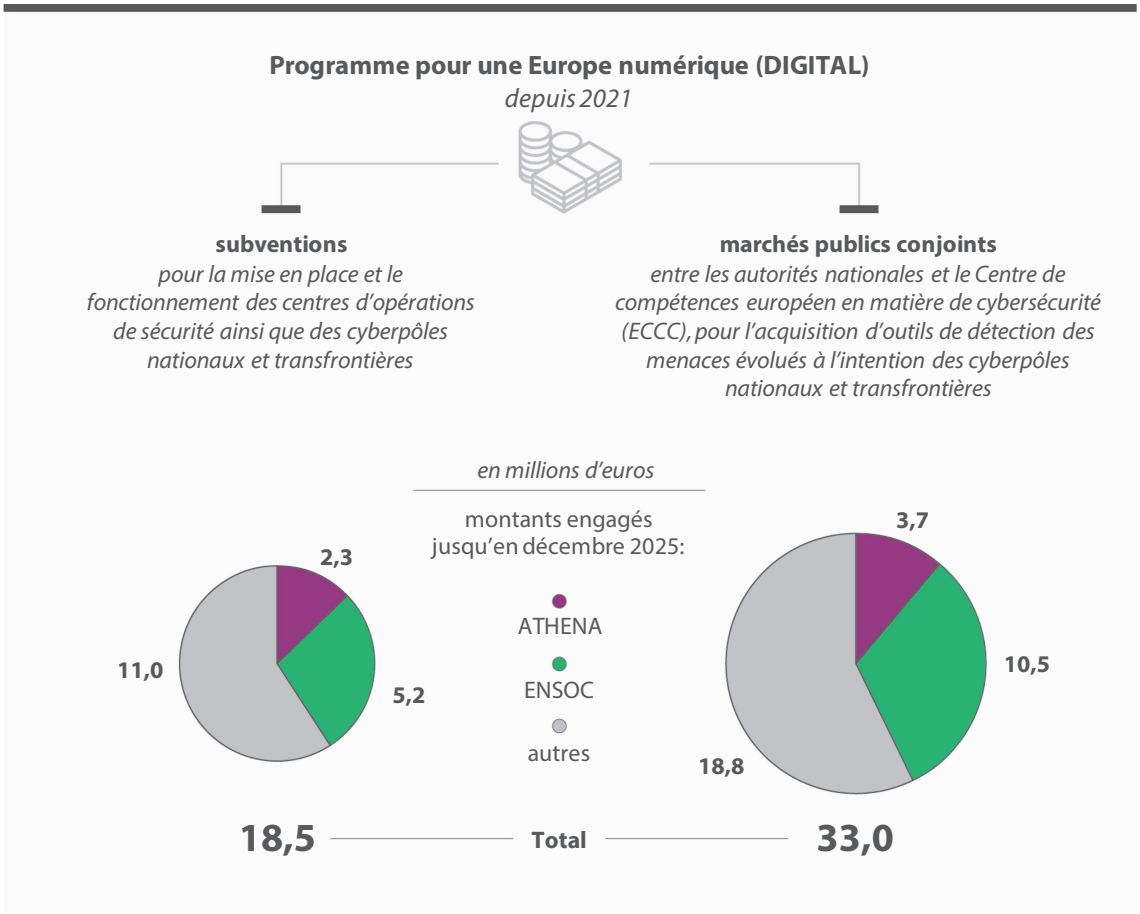
Source: Cour des comptes européenne.

64 Nous avons examiné la manière dont les deux premiers cyberpôles transfrontières ont été établis, et évalué leurs progrès dans la réalisation des objectifs du système européen d'alerte en matière de cybersécurité. Nous avons également analysé la place de l'établissement des cyberpôles transfrontières dans le paysage de la cybersécurité en général, et leurs interactions avec les réseaux et structures existants.

En raison de retards considérables dans la passation de marchés, aucun résultat concret n'a été obtenu jusqu'à présent

65 Des fonds destinés à soutenir l'établissement de cyberpôles nationaux et transfrontières sont disponibles dans le cadre du programme DIGITAL depuis 2021. L'octroi de ces financements passe par une procédure complexe, avec deux flux parallèles: des subventions classiques pour soutenir la mise en place et le fonctionnement des pôles, et des marchés publics conjoints pour l'acquisition d'outils de pointe pour la détection des menaces (voir ***figure 6***). Après un appel à propositions en novembre 2022, ATHENA et ENSOC ont commencé à fonctionner en janvier 2024.

Figure 6 | Le financement destiné aux cyberpôles dans le programme pour une Europe numérique



Source: Cour des comptes européenne, sur la base des données du Centre de compétences européen en matière de cybersécurité.

66 Les procédures de marché restreintes en deux phases[11] ont été organisées par les membres d'ATHENA et d'ENSOC, avec, pour la première phase, la DG Connect et, pour la deuxième, l'ECCC, qui venait d'être institué. L'organisation en deux phases vise à limiter la diffusion d'informations sensibles: les spécifications techniques détaillées ne sont communiquées qu'aux candidats sélectionnés à l'issue de la première phase.

67 La première phase a été engagée en mai 2024 pour ENSOC et en juillet 2024 pour ATHENA. Les entreprises intéressées disposaient d'un mois pour soumissionner. Les candidats retenus n'ont toutefois été informés qu'en avril 2025, près d'un an après le lancement de la procédure.

68 En outre, ni la procédure de marché d'ENSOC, ni celle d'ATHENA n'ont pu entrer dans la deuxième phase à ce moment-là, car les membres des pôles et l'ECCC n'avaient pas encore finalisé les spécifications techniques nécessaires à la présentation d'une offre et ne pouvaient donc pas les communiquer aux entreprises présélectionnées.

69 Dans le cas d'ENSOC, la deuxième phase de la procédure n'a commencé qu'en août 2025 et ne concernait que certains lots; pour ATHENA, elle était prévue pour début 2026. Au moment de l'audit, soit 18 mois après le lancement des procédures de marché, aucun contrat n'avait été signé pour quelque lot que ce soit. Nous pensons que la préparation insuffisante, ainsi que la complexité des procédures de marché, ont fait obstacle à leur achèvement en temps utile.

70 Nous avons constaté que, dans ces conditions, les cyberpôles transfrontières n'étaient pas en bonne voie pour atteindre leurs objectifs. Faute d'outils pour détecter les menaces et partager les informations, ils ne sont pas encore opérationnels, et le système européen d'alerte en matière de cybersécurité ne fonctionne pas encore, ce qui retarde le développement effectif de capacités avancées permettant de détecter et de prévenir les cybermenaces et les autres cyberincidents. Des avenants ont été signés pour prolonger la durée de la convention de subvention, compte tenu des retards qu'accusent actuellement les procédures de marché (15 mois pour ATHENA et 18 mois pour ENSOC).

[11] Appels d'offres d'ENSOC et d'ATHENA.

Les cyberpôles transfrontières créent des canaux de communication supplémentaires qui accroissent encore la complexité

71 Une des principales missions des cyberpôles transfrontières consiste à partager les informations pertinentes pour améliorer la détection des menaces et la réaction à ces dangers, ce qui englobe des informations sur les cybermenaces, sur les vulnérabilités, sur les indicateurs de compromission et sur les acteurs de menaces. Les tâches des cyberpôles transfrontières font partiellement double emploi avec celles des CSIRT nationaux et du réseau des CSIRT, en particulier pour ce qui est du partage d'informations sur les cybermenaces et les vulnérabilités. Il n'existe pas de démarcation claire entre le rôle des cyberpôles transfrontières et celui des CSIRT. D'après le schéma directeur en matière de cybersécurité de 2025 (point ***29***), les cyberpôles transfrontières visent à œuvrer au niveau à la fois technique (comme les CSIRT nationaux et le réseau des CSIRT) et opérationnel (comme EU-CyCLONe).

72 Le règlement sur la cybersolidarité oblige les cyberpôles transfrontières à conclure entre eux des accords de coopération afin de faciliter le partage d'informations. En vertu de ce même règlement, l'ENISA aurait dû publier des lignes directrices en matière d'interopérabilité entre les cyberpôles transfrontières en février 2026 au plus tard. Parallèlement, en décembre 2025, l'ECCC a accordé une subvention à un consortium (qui comprend certains membres d'ENSOC et d'ATHENA) pour définir un cadre technique d'interopérabilité entre ces pôles. Cependant, les cyberpôles transfrontières commenceront à fonctionner avant que les lignes directrices et le cadre soient achevés. Comme nous l'avons signalé dans notre avis de 2023 relatif à la proposition de règlement sur la cybersolidarité[12], sans accord rapide, des systèmes incompatibles risquent d'être développés, ce qui se traduirait par des coûts accrus.

[12] Avis 02/2023 sur une proposition de règlement du Parlement européen et du Conseil établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, point 26.

73 Les cyberpôles transfrontières sont également tenus de transmettre à EU-CyCLONe et au réseau des CSIRT, sans retard injustifié, les informations pertinentes relatives aux incidents de cybersécurité majeurs. Au niveau des États membres, la création de cyberpôles nationaux et la participation aux cyberpôles transfrontières engendrent des strates de communication supplémentaires. La coordination avec les pays tiers[13], qui n'appartiennent ni au réseau des CSIRT, ni à EU-CyCLONe, est elle aussi un facteur de complexité.

74 Des accords de coopération clairs sont nécessaires pour convenir d'une taxonomie commune ainsi que des modalités du partage d'informations, et pour garantir l'interopérabilité. L'expérience du réseau des CSIRT montre que cela constitue un défi de taille. Nous avons constaté qu'au moment de l'audit, aucune modalité procédurale en matière de coopération et de partage d'informations n'avait été arrêtée. À notre avis, la création de cyberpôles nationaux et transfrontières pourrait favoriser un partage d'informations plus efficace. Cependant, l'intégration des cyberpôles transfrontières dans un paysage de cybersécurité déjà complexe comportera des difficultés et nécessite des canaux de communication et des accords de coopération supplémentaires.

[13] L'Islande et la Norvège.

Les projets financés par l'UE dans le cadre du programme pour une Europe numérique visent à renforcer la cybersécurité, mais leur mise en œuvre et l'établissement de rapports les concernant posent des problèmes

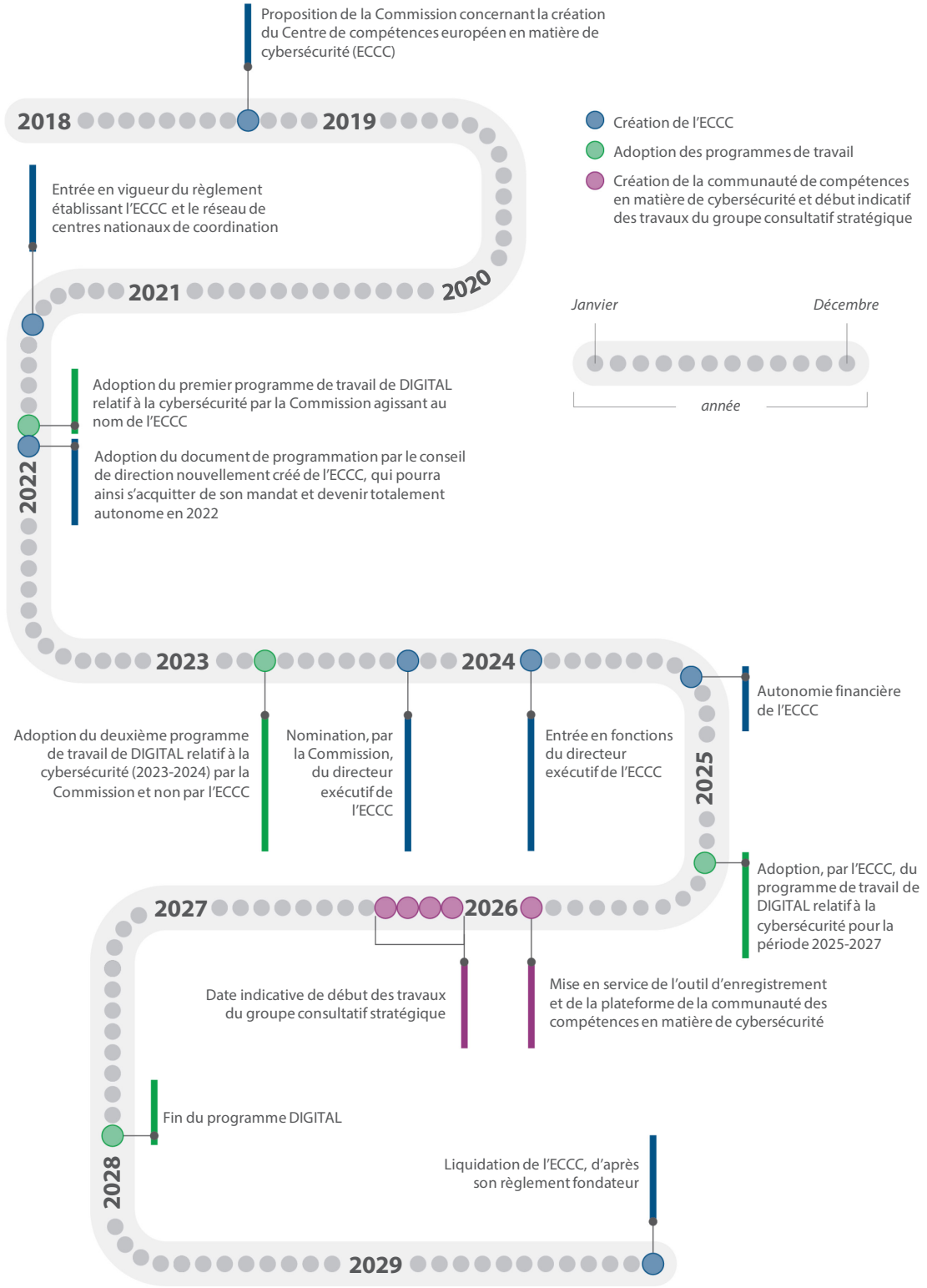
En raison de retards lors de sa création, la communauté des compétences en matière de cybersécurité n'a pas pu faire en sorte que le programme DIGITAL réponde à ses besoins

75 Aux fins de la gestion du volet «cybersécurité» du programme DIGITAL, la Commission a proposé, en 2018, de créer le Centre de compétences européen en matière de cybersécurité (ECCC). Le règlement fondateur de l'ECCC prévoyait que celui-ci dispose du soutien d'un réseau de 29 centres nationaux de coordination (NCC), soit un par État membre, un pour l'Islande et un pour la Norvège. Il appelait également à la création d'une communauté des compétences en matière de cybersécurité (la «communauté») rassemblant des représentants de l'industrie, d'institutions académiques et de recherche, et d'autres associations concernées de la société civile.

76 Des membres de la communauté (20 au maximum) devaient ensuite être nommés au groupe consultatif stratégique, un des trois organes dont se compose la structure de l'ECCC. Ce groupe a entre autres pour mission d'organiser des consultations publiques afin d'alimenter la stratégie du Centre de compétences et les programmes de travail destinés à DIGITAL.

77 Nous avons examiné si l'adoption de DIGITAL et de ses programmes de travail avait reposé sur une analyse rigoureuse des besoins, et comment l'ECCC, le réseau des NCC, la communauté des compétences en matière de cybersécurité et le groupe consultatif stratégique étaient en mesure de contribuer à l'élaboration des programmes de travail. Dans la pratique, la création de l'ECCC, du réseau des NCC, de la communauté et du groupe consultatif stratégique s'est étalée sur plusieurs années (voir ***figure 7***).

Figure 7 | Historique de la création du Centre de compétences européen en matière de cybersécurité, du réseau de centres nationaux de coordination, de la communauté et du groupe consultatif stratégique



Source: Cour des comptes européenne.

78 L'ECCC n'étant devenu pleinement opérationnel qu'en septembre 2024, la Commission a adopté en son nom les programmes de travail des périodes 2021-2022 et 2023-2024, qui n'ont donc pas pu bénéficier des contributions de la communauté.

79 Entre-temps, les États membres ont commencé à mettre en place leurs centres nationaux de coordination, qui jouent le rôle de points de contact au niveau national pour la communauté. La création et l'exploitation de ces centres ont été cofinancées au titre de DIGITAL: au moment de l'audit, l'UE avait ainsi accordé plus de 90 millions d'euros de fonds, dont quelque 44 millions d'euros à redistribuer dans le cadre du soutien financier à des tiers. Un montant supplémentaire de 38 millions d'euros destinés à soutenir les NCC a été inscrit au budget jusqu'en 2027.

80 Nous avons constaté qu'en décembre 2025, soit quatre ans après la création de l'ECCC et du réseau des NCC, la communauté n'avait pas encore été établie et le groupe consultatif stratégique, pas encore été nommé. L'ECCC a adopté le 14 mars 2025 le dernier programme de travail de DIGITAL relatif à la cybersécurité, qui couvre la période 2025-2027. Certes, le Centre de compétences a mené des consultations approfondies auprès des États membres et du réseau des NCC avant d'élaborer et d'adopter son programme de travail, mais il n'a pas pu bénéficier des contributions et des conseils de la communauté ou du groupe consultatif stratégique. Cela est contraire aux dispositions de son règlement fondateur et constitue, à nos yeux, une occasion manquée.

81 DIGITAL est appelé à prendre fin en 2027, et l'ECCC devrait cesser d'exister en 2029 si son mandat n'est pas prorogé. Ainsi, le soutien du réseau des NCC, de la communauté et du groupe consultatif stratégique, une fois mis en place, ne sera peut-être utile que pendant une courte période.

Les projets financés par l'UE poursuivent des objectifs pertinents, mais beaucoup se heurtent à des problèmes opérationnels

82 Nous avons sélectionné un échantillon de 11 projets liés à la détection des cyberincidents et à la réaction à ces incidents, financés au titre de DIGITAL au cours de la période 2022-2025 (voir ***figure 5*** de l'***annexe I*** et ***annexe III***). Nous avons évalué:

- si les objectifs des projets cadraient avec ceux de DIGITAL en général et avec les résultats attendus décrits dans les appels à propositions;
- si les projets avaient produit, à ce jour, les réalisations et résultats prévus;
- si les réalisations des projets avaient été fournies dans les délais.

Les résultats de cette évaluation sont présentés à l'***annexe IV***.

Certains projets ont produit de premiers résultats, mais beaucoup se heurtent à des difficultés opérationnelles et subissent des retards

83 Nous avons constaté que tous les projets poursuivaient des objectifs qui contribuent à la réalisation des objectifs de DIGITAL[14] relatifs à la cybersécurité, et qu'ils tenaient compte de la plupart des objectifs des appels à propositions[15].

84 Sur les 11 projets de notre échantillon, deux étaient au début de leur mise en œuvre, si bien que nous n'avons pu dégager aucune conclusion au sujet de leur performance. Parmi les projets restants, nous en considérons quatre comme satisfaisants du point de vue de l'obtention de leurs réalisations et de leurs résultats prévus. Nous avons estimé que deux projets présentaient des faiblesses, et nous avons jugé les trois derniers insatisfaisants (voir ***annexe IV***).

85 DIGITAL vise explicitement à rehausser le niveau de cybersécurité des petites et moyennes entreprises (PME). Plusieurs projets visent à apporter des solutions concrètes à des entreprises de cette catégorie (voir ***encadré 2***).

---

[14] Voir article 6 du règlement (UE) 2021/694 établissant le programme pour une Europe numérique.

[15] Appels à propositions *Capacity building of security operation centres*, *Deploying the network of national coordination centres with member states*, *Preparedness support and mutual assistance* et *Novel applications of AI and other enabling technologies for security operation centres*.

Encadré 2

Exemples de projets produisant des résultats tangibles pour les PME

Le projet GR-SME-SOC (projet n° 6 à l'***annexe III***) vise à fournir des outils et des services de cybersécurité aux PME en Grèce, moyennant la création d'un centre d'opérations de sécurité (SOC) adapté à leurs besoins. Ce projet, entamé en janvier 2024, est en cours de mise en œuvre par un consortium de cinq organisations grecques. Il consiste à proposer gratuitement des services de cybersécurité à 120 PME pendant un an, après quoi les services seront commercialisés. Le projet permet d'offrir des services avancés tels que la surveillance en temps réel, la détection des menaces fondée sur l'intelligence artificielle et la réaction rapide aux incidents à des petites et moyennes entreprises.

Dans le cadre du projet NCC-IE (projet n° 3 à l'***annexe III***), le coordinateur de projet a versé quelque 1,8 million d'euros de subventions à plus de 50 PME irlandaises pour leur permettre de renforcer leur cybersécurité. Des sociétés employant entre 2 et 200 salariés environ, dont des entreprises familiales, de jeunes pousses et des exportateurs mondiaux de divers secteurs, ont bénéficié du programme de subventions. Ces dernières étaient réservées à des entreprises qui avaient fait l'objet d'un examen de cybersécurité géré par l'agence gouvernementale Enterprise Ireland. Elles couvraient 80 % des coûts de mise en œuvre des recommandations issues de l'examen (jusqu'à concurrence de 60 000 euros).

Source: Cour des comptes européenne.

86 Des problèmes de respect des délais ou des difficultés opérationnelles touchent un grand nombre de projets de notre échantillon (voir ***annexe IV***). Nous avons constaté que quatre projets accusaient des retards considérables. Tel est entre autres le cas d'ENSOC et d'ATHENA, comme cela est exposé en détail aux points ***65*** à ***70***. Nous en donnons d'autres exemples dans l'***encadré 3***.

Encadré 3

Exemples de projets présentant des difficultés opérationnelles et des retards

En Irlande, la *Local Government Management Authority* (LGMA) est la seule bénéficiaire de la subvention relevant du projet ILG-SOC (projet n° 8 à l'***annexe III***). Celui-ci vise à mettre en place un centre d'opérations de sécurité central permettant à 31 autorités locales d'utiliser des outils avancés pour détecter les menaces et y réagir. Il a commencé en octobre 2023 pour une durée de trois ans. À l'issue de l'examen à mi-parcours, tous les éléments livrables ont été rejetés. Le projet comprend plusieurs procédures de marché qui ont échoué ou ont pris du retard. Sa durée sera prolongée (sans augmentation de budget), si bien que le projet pourra peut-être aboutir.

En Grèce, le projet EL-SOC (projet n° 5 à l'***annexe III***) vise à la création d'un centre d'opérations de sécurité global, qui rassemblerait les informations des SOC sectoriels. Cela permettrait d'avoir un aperçu complet, en temps réel, de la situation en matière de cybersécurité. Le projet doit durer de janvier 2024 à décembre 2026. L'acquisition de matériel et de services, qui était prévue, a été retardée en raison de problèmes pour finaliser et publier les spécifications techniques destinées à l'appel d'offres. Le coordinateur du projet a également expliqué le retard par des difficultés pour obtenir un cofinancement national et par la disponibilité limitée du personnel responsable des marchés publics.

Source: Cour des comptes européenne.

87 Deux autres projets de notre échantillon ont pris un retard modéré. Trois ont produit leurs réalisations dans les délais prévus. Les deux derniers sont au début de leur mise en œuvre, si bien que nous ne pouvons pas formuler de conclusion à leur sujet.

Les restrictions liées à la sécurité ont entraîné des difficultés opérationnelles, et la réalisation des contrôles par des bénéficiaires est porteuse de risques non négligeables

88 Le règlement établissant DIGITAL dispose que, pour des raisons de sécurité, il est possible de restreindre le bénéfice des financements en faveur de la cybersécurité aux entités établies dans l'UE et contrôlées par des États membres ou des citoyens de l'UE. Cette restriction vise à atténuer le risque d'intrusion ou d'influence de pays tiers et à empêcher le partage d'informations sensibles relatives à la sécurité avec des autorités de ces pays.

89 L'obligation de détention et de contrôle par des États membres ou des citoyens de l'UE s'applique non seulement aux bénéficiaires de subventions, mais encore à leurs sous-traitants et aux éventuels bénéficiaires d'un soutien financier à des tiers. Si le bénéficiaire ne relève pas de cette dernière catégorie (voir points ***92*** à ***96***), le service central de validation de l'agence exécutive européenne pour la recherche évalue la conformité à l'obligation susmentionnée. La décision finale concernant l'éligibilité à la participation à un appel restreint n'en revient pas moins à l'autorité qui octroie la subvention, par exemple la DG Connect ou l'ECCC.

90 Au cours de nos travaux d'audit, les bénéficiaires ont évoqué à maintes reprises les difficultés pratiques que comportent les évaluations du contrôle et de la propriété (ECP). Le processus consistant à vérifier si des entités juridiques sont détenues et contrôlées par des États membres ou des citoyens de l'UE peut être long et complexe. Il nécessite d'analyser l'ensemble de la structure de propriété et de la chaîne de contrôle de chaque organisation, en examinant chaque maillon de la chaîne de propriété jusqu'aux propriétaires effectifs. Le service central de validation exige que chaque entité fournisse un grand nombre de preuves documentaires concernant sa structure de propriété et les droits spécifiques y afférents, sa gouvernance d'entreprise et tout lien commercial, financier ou d'un autre type conférant un contrôle sur l'entité.

91 Dans trois projets de notre échantillon, au moins un bénéficiaire ou un consortium a été exclu par la suite parce qu'il était considéré comme appartenant à une entité d'un pays tiers, ou comme étant contrôlé depuis un tel pays. L'exclusion de membres de consortiums montre que les participants à DIGITAL ne comprennent pas tous parfaitement la notion de détention et de contrôle par des États membres ou des citoyens de l'UE. Des données communiquées par le service central de validation indiquent qu'au cours de la période 2022-2025, les demandeurs de subventions de DIGITAL en lien avec la cybersécurité et leurs sous-traitants ont, pour 7 % d'entre eux, fait l'objet d'une évaluation négative. Le fait que des participants inéligibles présentent des demandes dans le cadre d'un appel à propositions occasionne des retards (voir ***encadré 4***).

Encadré 4

Exemple d'exclusion de bénéficiaires à la suite des contrôles de sécurité

Dans le projet NG-SOC (projet n° 7 à l'***annexe III***), l'ECP de deux membres du consortium s'est avérée défavorable. Le résultat a été annoncé un mois environ avant la date limite pour la signature de la convention de subvention. Faute de temps pour trouver un nouveau partenaire, le coordinateur du projet a dû accepter de se charger des travaux initialement confiés aux deux membres exclus. Un de ces derniers opérait dans un secteur spécifique où devait être mené le projet pilote relatif à la solution développée. Dans ces conditions, un volet important du projet, consistant à essayer les solutions dans la pratique, n'a pas pu avoir lieu comme prévu. La situation a ensuite été résolue au moyen d'un avenant à la convention de subvention qui a permis d'inclure de nouveaux membres.

Source: Cour des comptes européenne.

92 Deux des projets que nous avons examinés (NCC-IE et CYberSynchrony) comprennent un soutien financier à des tiers. Ce mécanisme de financement permet aux bénéficiaires de subventions d'octroyer une partie des fonds à d'autres entités, dans le cadre d'appels ouverts. Il peut faciliter l'accès aux financements de l'UE. Dans ce cas, les bénéficiaires sont seuls responsables de la réalisation des ECP. Le service central de validation n'y participe pas.

93 En 2021, la Commission a publié des orientations générales à l'intention des candidats aux appels restreints. Ces orientations ont été actualisées en 2026. Bien que le soutien financier à des tiers soit autorisé depuis 2021 dans les appels à propositions relevant de DIGITAL, ni la Commission ni l'ECCC n'ont fourni aux bénéficiaires une méthodologie détaillée pour la réalisation des ECP lors de l'évaluation des tiers auxquels ils apportent un soutien financier. En juillet 2025, l'ECCC a diffusé des orientations non contraignantes et a ainsi fourni au réseau des NCC une approche structurée en matière d'ECP. Le document d'orientation énonce des principes généraux et décrit des mesures envisageables. Cependant, il ne précise pas comment doivent être effectués les contrôles, de sorte qu'il appartient toujours aux bénéficiaires d'élaborer leur propre démarche.

94 Nous avons constaté que l'ECCC ne validait pas la méthode adoptée par les bénéficiaires et qu'il n'effectuait pas non plus de contrôles par échantillonnage pour vérifier que la méthode retenue était suffisamment fiable et que les entités sélectionnées comme bénéficiaires du soutien financier à des tiers étaient effectivement détenues et contrôlées par des États membres ou des citoyens de l'UE.

95 Dans notre rapport annuel relatif à 2024, nous avons constaté que les bénéficiaires chargés par la Commission de gérer le soutien financier à des tiers (dans le domaine de la recherche) n'étaient pas tenus de démontrer que leurs contrôles permettent de garantir efficacement la régularité des dépenses de l'UE. De même, l'ECCC ne procède à aucune évaluation de la capacité administrative et technique des bénéficiaires à gérer les ECP de manière appropriée. Comme cela est exposé en détail au point ***90***, ces évaluations, qui peuvent être complexes, sont effectuées, au niveau de l'UE, par un service spécialisé possédant des compétences techniques en la matière.

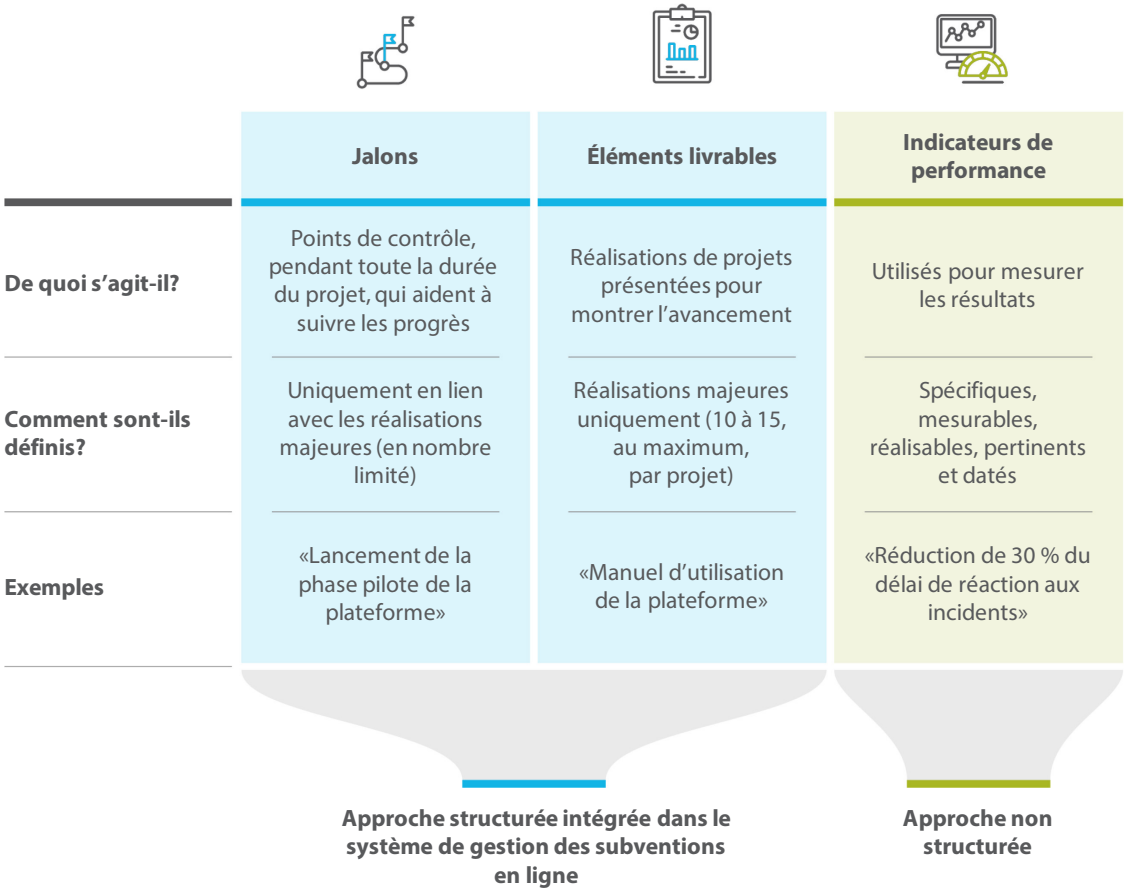
96 Dans ces conditions, il existe, selon nous, un risque non négligeable que les bénéficiaires, qui sont chargés des ECP, ne soient pas à même de les effectuer correctement. Étant donné la nature des activités financées, cette insuffisance pourrait mettre en danger des éléments sensibles, dont des infrastructures, des données opérationnelles et des technologies essentielles à la sécurité.

La plupart des projets financés par l'UE sont dotés de cadres de performance inappropriés, et les données sur la performance du programme DIGITAL en matière de cybersécurité sont erronées

Les cadres de performance de la plupart des projets financés par l'UE laissent à désirer

97 Les bénéficiaires qui gèrent des projets financés par l'UE doivent rendre compte à l'ECCC de leur avancement et de leurs résultats, mesurés en fonction de jalons, d'éléments livrables et d'indicateurs, comme le montre la ***figure 8***. Pour chaque projet, nous avons examiné si les jalons et les éléments livrables définis permettaient un suivi approprié. Nous avons également vérifié si les indicateurs de performance étaient pertinents, mesurables et assortis d'une valeur de référence ainsi que d'une valeur cible.

Figure 8 | Jalons, éléments livrables et indicateurs de performance dans les projets de DIGITAL



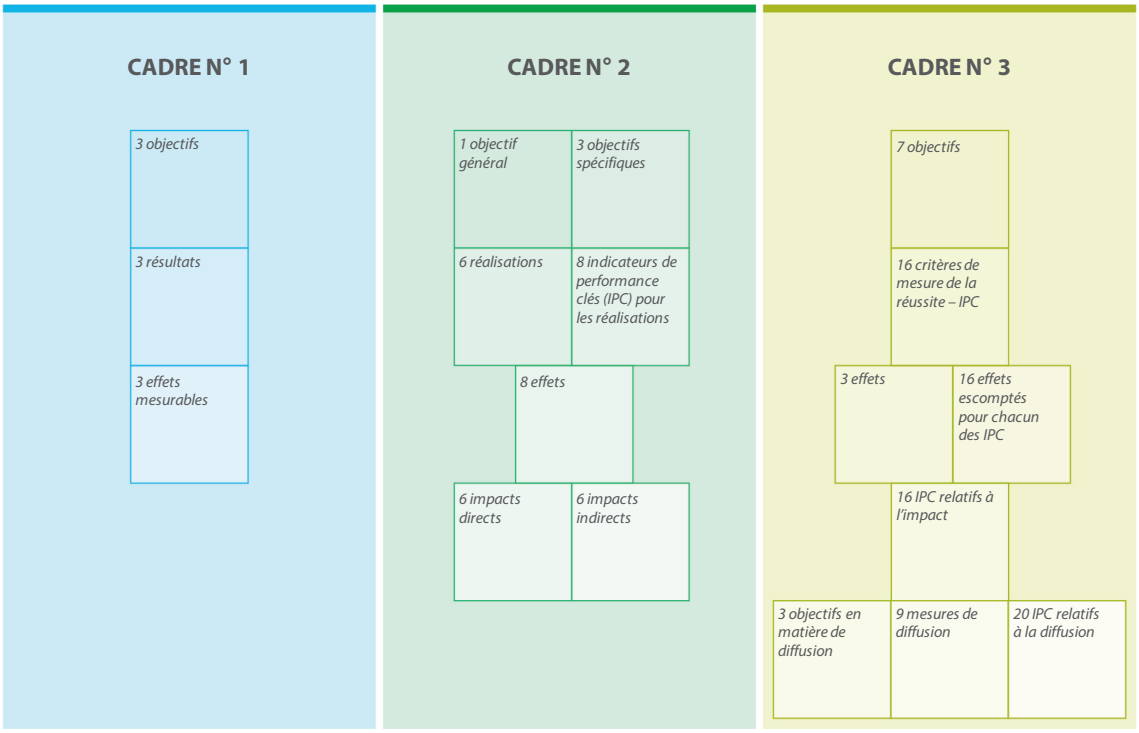
Source: Cour des comptes européenne, sur la base du formulaire de demande de subvention.

98 Dans leurs propositions de projets, les bénéficiaires doivent définir une série de jalons et un ensemble d'éléments livrables en suivant une approche structurée, décrite dans les instructions à l'intention des demandeurs. Tous les jalons et éléments livrables sont enregistrés dans le système de gestion des subventions en ligne, afin de faciliter leur suivi. En règle générale, l'ECCC examine deux fois chaque projet: une fois à mi-parcours et une fois après l'achèvement du projet. Lors de ces examens, des experts externes vérifient si les jalons ont été respectés et les éléments livrables, réalisés, et l'ECCC les valide le cas échéant. Dans ces conditions, les jalons et les éléments livrables sont essentiels pour le suivi des projets, et doivent être définis de manière appropriée.

99 Nous avons constaté que presque aucun projet de notre échantillon n'était conforme aux instructions en ce qui concerne le nombre de jalons et d'éléments livrables: le nombre de jalons par projet varie de 8 à 39, et le nombre d'éléments livrables, de 8 à 45. Beaucoup de jalons et d'éléments livrables, n'étant pas conformes aux instructions concernant leur libellé, ne sont pas utiles pour suivre les progrès accomplis (par exemple «réunion pour commencer à rédiger l'appel à propositions de recherche» ou «procès-verbal officiel de la réunion de projet»). Pour trois projets, le comité d'évaluation avait pointé ces problèmes avant que la convention de subvention soit signée. Dans deux cas, les bénéficiaires n'ont proposé que de petits changements (par exemple des modifications du calendrier) sans s'attaquer au problème essentiel; dans le troisième cas, le bénéficiaire n'a effectué aucune modification. Pour six autres projets de notre échantillon, notre analyse a montré que les jalons ou les éléments livrables n'étaient pas conformes aux instructions et pas toujours appropriés. Selon nous, des jalons et des éléments livrables mal définis ou en trop grand nombre engendrent des difficultés pour suivre les progrès.

100 À la différence des jalons et des éléments livrables, les indicateurs de performance ne font pas l'objet d'une approche structurée et ne sont pas réunis dans un tableau dans le système de gestion des subventions; ils sont dispersés dans diverses sections de la proposition. De ce fait, les bénéficiaires ont proposé une multitude de cadres de performance différents. Certains s'en sont tenus à fixer des objectifs de projet liés aux indicateurs de performance, mais d'autres ont mis en place des cadres de performance beaucoup plus complexes (voir exemples à la ***figure 9***).

Figure 9 | Diversité des cadres de performance conçus pour les différents projets



Source: Cour des comptes européenne.

101 Il ressort de notre analyse que nombre d'indicateurs de performance utilisés dans le cadre des projets ne sont pas pertinents ou pas mesurables, et ne sont pas assortis d'une valeur cible ou d'une valeur de référence (voir ***encadré 5***). En outre, le nombre des indicateurs définis s'élève à 20 ou plus dans sept projets, et atteint même 52 dans un projet. Les résultats de cette évaluation sont présentés à l'***annexe IV***.

Encadré 5

Exemples d'indicateurs de performance inappropriés

Indicateurs non mesurables

- «L'indicateur de compromission et les autres services fournis renforcent les capacités des PME en matière de cybersécurité»
- «Fourniture d'outils et de méthodes de réaction aux incidents permettant l'intégration avec les canaux de communication d'EU-CyCLONe»

Indicateurs dépourvus de valeur de référence ou de valeur cible

- «Amélioration d'au moins 20 % du niveau de préparation du personnel»
- «Réduction d'au moins 20 % des efforts nécessaires pour s'aligner sur les initiatives pertinentes de l'UE en matière de cybersécurité et s'y conformer»

Indicateurs sans lien avec la performance

- «Rapport final sur le projet à la fin de la phase de financement»
- «Nombre de participants à l'ensemble des sessions de formation»

Source: Cour des comptes européenne, sur la base de la documentation relative aux projets.

102 Globalement, nous estimons que la large diversité des cadres de performance, ainsi que l'inadéquation et le nombre excessif des indicateurs compliquent considérablement le suivi de la performance. Il n'est dès lors pas possible d'évaluer correctement la performance des projets. À cela s'ajoute que, le modèle de rapport ne comportant pas de section spéciale consacrée aux indicateurs de performance des projets, aucune information sur ces indicateurs n'a été transmise pour la plupart des projets de notre échantillon.

Les données sur la performance du volet «cybersécurité» de DIGITAL sont erronées

103 Aux fins du suivi des réalisations de DIGITAL, le règlement définit des indicateurs de programme sur lesquels des informations doivent être communiquées dans le cadre chaque projet (voir ***encadré 6***).

Encadré 6

Indicateurs du programme DIGITAL relatifs à la cybersécurité

1.a. Le nombre d'infrastructures ou d'outils de cybersécurité, ou les deux, faisant l'objet de marchés publics conjoints, y compris dans le cadre du système européen d'alerte en matière de cybersécurité

1.b. Le nombre d'infrastructures ou d'outils de cybersécurité, ou les deux, qui ont été déployés

2. Le nombre d'utilisateurs et de communautés d'utilisateurs ayant accès à des installations européennes de cybersécurité

3. Le nombre de mesures d'aide à la préparation et à la réaction aux incidents de cybersécurité dans le cadre du mécanisme d'urgence dans le domaine de la cybersécurité

Source: Annexe II du règlement (UE) 2021/694 établissant le programme pour une Europe numérique; cadre de suivi et d'évaluation du programme pour une Europe numérique (SWD(2024) 37).

104 Nous avons contrôlé si des informations concernant ces indicateurs avaient été communiquées pour chaque projet de notre échantillon, et examiné comment l'ECCC collecte et vérifie ces données.

105 Des informations sur les indicateurs de DIGITAL doivent être introduites dans le système de gestion des subventions pour chaque projet et ce, avant l'examen à mi-parcours et l'examen final du projet. D'après nos constatations, cela n'avait été fait que pour trois des sept projets de notre échantillon qui étaient à mi-parcours au moment de notre audit et auxquels s'appliquait donc cette obligation. Pour deux de ces trois projets, les informations communiquées étaient erronées: dans un cas, elles ne portaient pas sur le bon indicateur, dans l'autre, elles correspondaient aux valeurs cibles et non aux résultats obtenus.

106 Chaque année, la Commission rend compte de ces indicateurs dans ses fiches de performance des programmes. Cela permet aux parties prenantes d'évaluer si le programme atteint ses objectifs. D'après les fiches de performance relatives à 2024, les valeurs cibles des indicateurs de DIGITAL relatifs à la cybersécurité sont en voie d'être atteintes. Les représentants de l'ECCC nous ont expliqué que, pour compiler ces indicateurs, ils n'utilisaient pas le système de gestion des subventions, mais une série de questionnaires adressés aux bénéficiaires des projets. Nous avons examiné les données désagrégées fournies par l'ECCC et relevé de nombreuses insuffisances dans leurs modalités de collecte et dans leur qualité générale. Nous avons en outre constaté que les données réunies ne correspondaient pas aux valeurs figurant dans la fiche de performance du programme, si bien qu'il est difficile de savoir comment les valeurs publiées ont été calculées. Nous n'avons trouvé aucun élément probant attestant que l'ECCC ait vérifié l'exactitude des données communiquées. À la lumière de nos contrôles relatifs aux projets de notre échantillon, la plupart des valeurs étant inexactes ou faisant défaut, nous estimons que les données fournies ne rendent pas fidèlement compte des résultats obtenus.

Le présent rapport a été adopté par la Chambre III, présidée par George Marius Hyzler, Membre de la Cour des comptes, à Luxembourg en sa réunion du 16 juin 2026.

Par la Cour des comptes

Tony Murphy
Président

Annexes

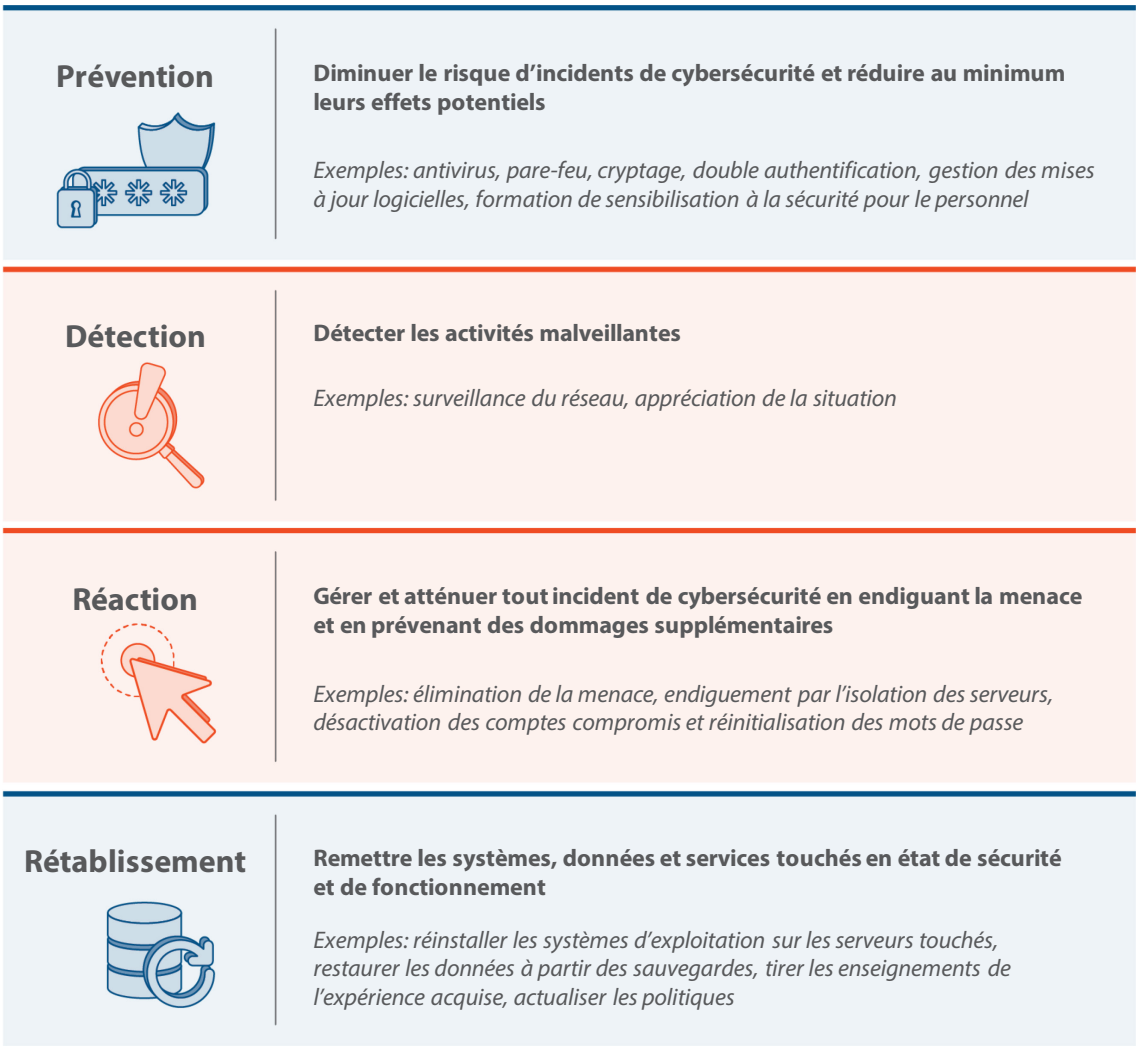
Annexe I – À propos de l'audit

01 Par cybersécurité, on entend «les actions nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces»[1], c'est-à-dire à «toute circonstance, tout événement ou toute action potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes, ou encore de provoquer des interruptions de ces réseaux et systèmes»[2]. La cybersécurité nécessite d'adopter une approche globale qui consiste en un ensemble d'activités liées entre elles et destinées à prévenir les cybermenaces, à les détecter, à y réagir et à s'en rétablir (voir ***figure 1***).

[1] Règlement (UE) 2019/881 (règlement sur la cybersécurité).

[2] Article 2 du règlement sur la cybersécurité.

Figure 1 | Exemples d'activités de cybersécurité

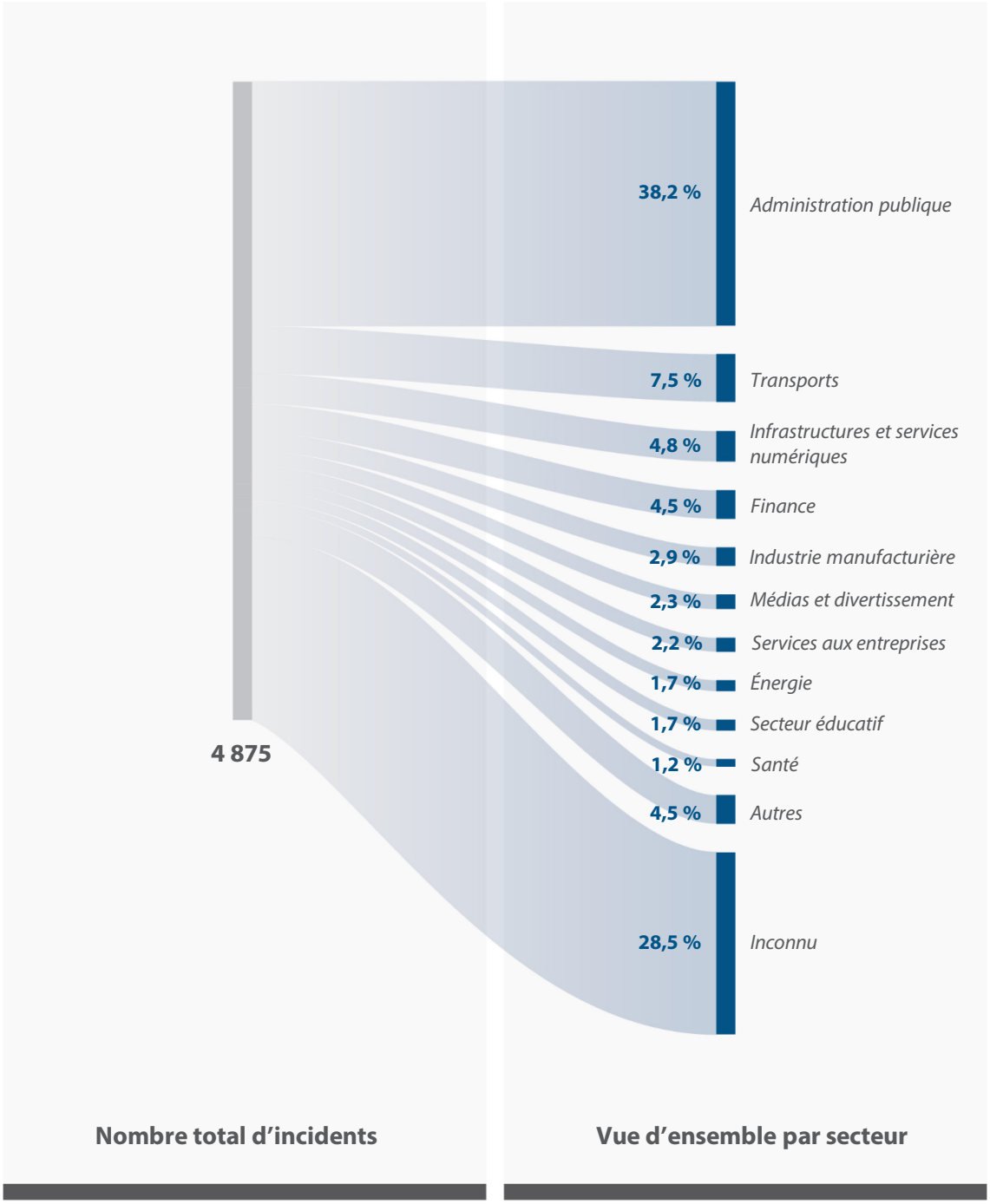


Source: Cour des comptes européenne, sur la base du considérant 78 de la directive (UE) 2022/2555 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité (directive SRI 2).

02 L'Agence de l'Union européenne pour la cybersécurité (ENISA) estime que la cybersécurité est en grand danger, tout en constatant que le paysage des cybermenaces est devenu, et reste, beaucoup plus complexe[3]. Ces menaces font ressortir l'importance capitale de la cybersécurité dans des économies et des sociétés de plus en plus numériques. Dans son rapport 2025 sur le paysage des menaces, l'ENISA a établi que le plus grave danger dans l'UE venait des rançongiciels. La ***figure 2*** montre quels secteurs sont ciblés.

[3] ENISA, rapport 2024 sur l'état de la cybersécurité dans l'Union.

Figure 2 | Secteurs ciblés par les cyberattaques



Source: Cour des comptes européenne, sur la base d'informations fournies par l'ENISA.

Incidents de cybersécurité importants et majeurs

03 Les incidents de cybersécurité, qui comprennent les cybermenaces et les événements involontaires (comme ceux mentionnés à la ***figure 3*** et au point ***40***), «peuvent entraver les services publics et […] nuire à la poursuite des activités économiques, […], entraîner de lourdes pertes financières, entamer la confiance des utilisateurs, causer un préjudice majeur à l'économie et aux systèmes démocratiques de l'Union, voire mettre en danger la santé ou la vie des personnes»[4]. Un incident de cybersécurité est considéré comme[5]:

- **important**, s'il a causé ou est susceptible de causer une perturbation opérationnelle grave des services ou des pertes financières pour l'entité concernée, ou s'il a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables;

- **majeur**, s'il a provoqué des perturbations dépassant les capacités de réaction du seul État membre concerné ou s'il a un impact important sur au moins deux États membres.

04 Un incident de cybersécurité majeur peut dégénérer en une véritable **crise de cybersécurité à l'échelle de l'UE** s'il empêche le bon fonctionnement du marché intérieur ou présente de graves risques de sûreté et de sécurité publiques pour les entités ou les citoyens dans plusieurs États membres ou dans l'Union à part entière[6].

---

[4] Considérant 2 du règlement (UE) 2025/38 (règlement sur la cybersolidarité).

[5] Articles 6 et 23 de la directive SRI 2 et précisions supplémentaires apportées dans le règlement d'exécution (UE) 2024/2690 de la Commission en ce qui concerne un certain nombre de fournisseurs dans le secteur des infrastructures numériques.

[6] Considérant 69 de la directive SRI 2.

Cadre stratégique de l'UE

05 L'écosystème de cybersécurité de l'UE est complexe et stratifié. Il englobe toute une série de domaines d'action internes, tels que la justice et les affaires intérieures, le marché unique numérique et les politiques de recherche[7]. En politique extérieure, la cybersécurité se retrouve dans la diplomatie, et devient progressivement partie intégrante de la politique de défense de l'Union[8].

06 Ces dernières années, l'UE a renforcé son cadre réglementaire en matière de cybersécurité. La ***figure 3*** montre les actes législatifs et les instruments de politique les plus pertinents au niveau de l'UE. Eu égard à l'étendue de l'audit (voir points ***13*** et ***14***), nous nous sommes plus particulièrement intéressés aux instruments en lien avec la détection des incidents de cybersécurité importants et majeurs et avec la réaction à ces incidents.

[7] Cour des comptes européenne, «Défis à relever pour une politique de l'UE efficace dans le domaine de la cybersécurité», document d'information, p. 13.

[8] Par exemple, la posture cyber de l'Union européenne (2022), le cadre pour une réponse coordonnée de l'UE aux campagnes hybrides (2022), la politique de cyberdéfense de l'UE (2023) et la boîte à outils cyberdiplomatique révisée (2023).

Figure 3 | Législation et instruments de politique de l'UE dans le domaine de la cybersécurité

Source: Cour des comptes européenne.

Rôles et responsabilités

07 Le paysage de la cybersécurité de l'UE englobe un grand nombre d'acteurs civils privés et publics aux niveaux régional et national ainsi qu'à celui de l'UE, y compris des entités répressives. La cybersécurité est également un rouage essentiel de la sécurité et de la défense nationales[9]. L'***annexe II*** contient une représentation de ce paysage dans son état actuel.

08 C'est aux États membres qu'il appartient au premier chef de prévenir les incidents et crises de cybersécurité, de s'y préparer et d'y réagir. Conformément à l'article 4, paragraphe 2, du traité sur l'Union européenne, la sécurité nationale reste de la seule responsabilité de chaque État membre. Les incidents de cybersécurité étant susceptibles de perturber et d'endommager certaines infrastructures d'information critiques dont dépend le bon fonctionnement du marché intérieur, l'UE a elle aussi un rôle important à jouer en cas d'incident important ou de crise[10]. La ***figure 4*** montre quelles sont les principales entités compétentes au niveau de l'UE.

[9] Avis 02/2023 sur la proposition de règlement sur la cybersolidarité.

[10] Schéma directeur de l'UE pour la gestion des crises de cybersécurité.

Figure 4 | Entités du niveau de l'UE jouant un rôle de premier plan dans la cybersécurité

Source: Cour des comptes européenne.

Financements de l'UE

09 Dans le cadre financier pluriannuel en cours, celui de la période 2021-2027, le programme pour une Europe numérique (DIGITAL) est la principale source de financement dans le domaine de la cybersécurité. Premier programme européen spécialement destiné à favoriser la transformation numérique de l'UE, il a été lancé en 2021 et est doté d'un budget total de 8,1 milliards d'euros[11].

10 Au sein du programme DIGITAL, les actions en faveur de la cybersécurité sont financées au titre de l'objectif spécifique 3 «Cybersécurité et confiance». Plus précisément, une enveloppe de 1,4 milliard d'euros est destinée à:

- renforcer la coordination en matière de cybersécurité entre les outils et les infrastructures de données des États membres;
- soutenir le déploiement généralisé de solutions de cybersécurité dans l'ensemble de l'économie.

11 Dans DIGITAL, l'octroi des financements en faveur de la cybersécurité repose principalement sur des appels à propositions. De novembre 2021 à décembre 2025, 12 appels de ce type ont été lancés pour un montant total de financement disponible de 825 millions d'euros. De nouveaux appels visant à l'octroi de 212 millions d'euros de subventions supplémentaires sont prévus pour 2026 et 2027.

12 Horizon Europe est un autre programme important de l'UE qui permet de soutenir la cybersécurité. Dans ce programme, les projets de cybersécurité sont principalement financés au titre du pôle 3 «Sécurité civile pour la société» et sont généralement à un niveau de maturité technologique assez bas, Horizon Europe étant axé sur la recherche et l'innovation. Enfin, les mesures de cybersécurité peuvent également bénéficier de financements au titre de la facilité pour la reprise et la résilience.

[11] Page «Digital Europe Programme».

Étendue et approche de l'audit

13 L'augmentation des cybermenaces et de leurs incidences potentielles a montré combien il est nécessaire de renforcer notre cyberrésilience collective. Notre audit a visé à évaluer si l'action de l'UE facilitait efficacement la détection des incidents de cybersécurité importants et majeurs et la réaction à ces incidents. Nous avons en particulier examiné si tel était le cas:

- des réseaux et mécanismes au niveau de l'UE, à savoir le réseau des CSIRT, EU-CyCLONe, le système européen d'alerte en matière de cybersécurité, le *Cyber Situation Centre* et la réserve de cybersécurité de l'Union;
- des actions financées au titre du programme DIGITAL.

Nous ne nous sommes pas penchés sur la coopération des services répressifs au niveau de l'UE, ni sur les actions de cyberdissuasion entreprises à ce même niveau par le canal de mesures diplomatiques ou d'activités de défense.

14 L'audit couvre la période allant de 2022 à 2025. Il repose sur un contrôle sur pièces, une analyse de documents pertinents, des visites d'audit dans trois États membres (l'Irlande, la Grèce et l'Italie), des questionnaires écrits et des entretiens avec des parties prenantes du domaine. La ***figure 5*** montre par quels moyens nous avons obtenu les éléments probants sous-tendant nos observations.

Figure 5 | Travaux d'audit effectués

Nous avons examiné

- le **cadre juridique** applicable à la détection des incidents de cybersécurité importants et majeurs et la réaction à ces incidents
- les **rôles et responsabilités** des réseaux et structures mis en place au niveau de l'UE

Nous avons analysé

- des documents sur le fonctionnement du **réseau des CSIRT** et d'**EU-CyCLONe**
- de la documentation sur le **cadre de programmation et de suivi de la performance de DIGITAL**
- les documents sur **une sélection de 13 actions financées par l'UE** (11 subventions et 2 marchés – voir la liste détaillée à l'annexe III)

* Nous avons sélectionné des actions financées par l'UE dans trois pays (l'Irlande, la Grèce et l'Italie) où les montants de fonds apportés au titre de DIGITAL étaient parmi les plus élevés. Nous avons choisi les 11 subventions dans une liste de 137 projets financés par l'UE en lien avec la détection des menaces et la réaction à ces menaces, dans le but de couvrir des projets divers.

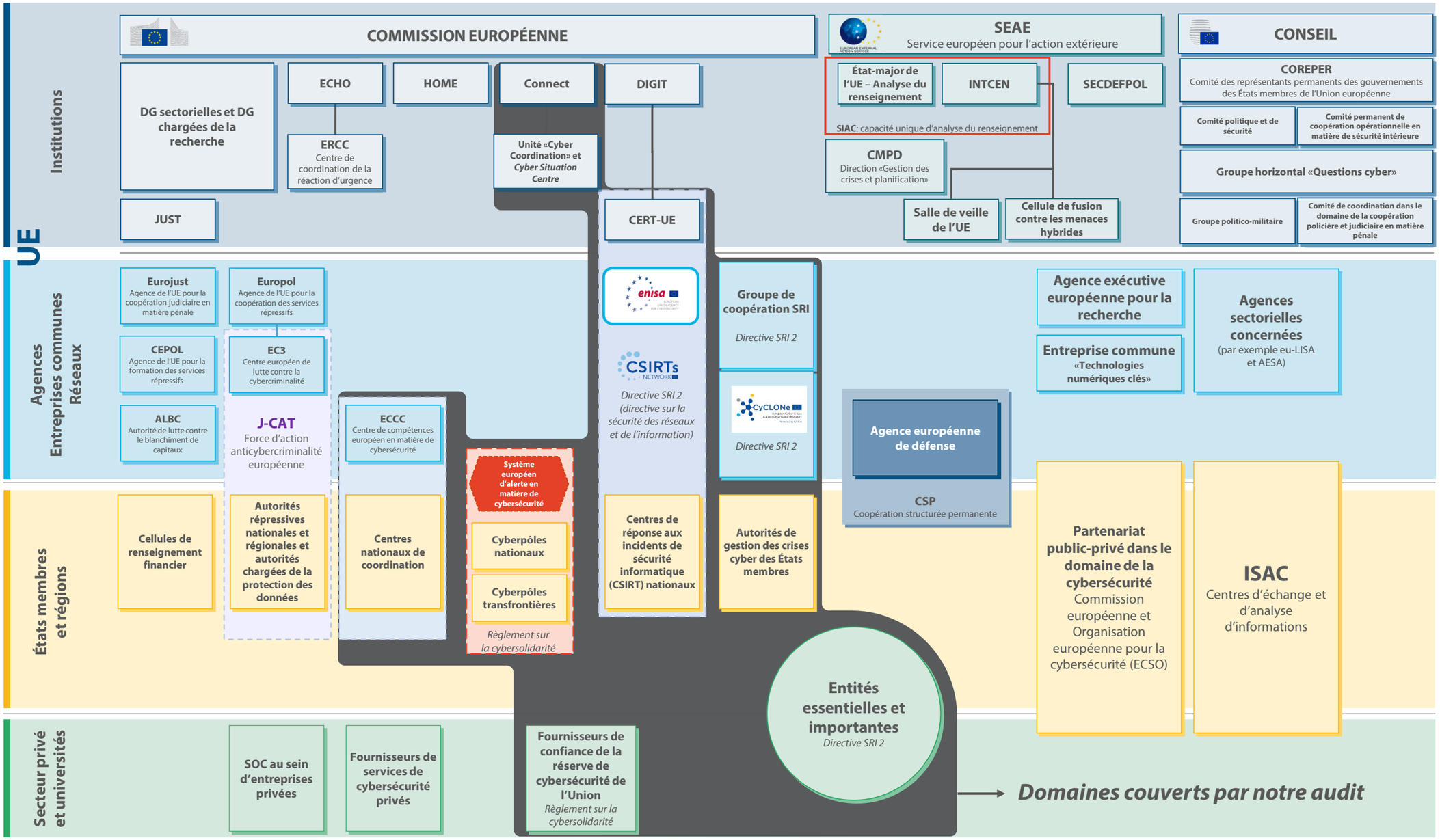
Nous nous sommes entretenus avec

- les bénéficiaires d'**un échantillon de 11 subventions financées par l'UE**
- des représentants des autorités nationales chargées de la cybersécurité dans **trois États membres** (l'Irlande, la Grèce et l'Italie)
- des représentants de la Commission européenne (**DG Connect**), de l'**ENISA** et de l'**ECCC**

Source: Cour des comptes européenne.

15 Nous pensons que nos constatations contribueront à renforcer l'efficacité et l'efficience avec lesquelles l'UE détecte les incidents de cybersécurité importants et majeurs et y réagit, ainsi qu'à améliorer la sélection et le suivi des actions qu'elle finance. Notre méthodologie d'audit est conforme aux normes internationales d'audit émises par l'Organisation internationale des institutions supérieures de contrôle des finances publiques (INTOSAI).

Annexe II – Le paysage de l'UE en matière de cybersécurité



DG Connect: direction générale des réseaux de communication, du contenu et des technologies
DG ECHO: direction générale de la protection civile et des opérations d'aide humanitaire européennes
DG HOME: direction générale de la migration et des affaires intérieures

DG JUST: direction générale de la justice et des consommateurs
DIGIT: direction générale des services numériques
AESA: Agence de l'Union européenne pour la sécurité aérienne
EU-CyCLONe: réseau européen pour la préparation et la gestion des crises cyber

eu-LISA: Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice
INTCEN: Centre de situation et du renseignement de l'Union européenne

SECDEFPOL: Politique de sécurité et de défense
SOC: Centre d'opérations de sécurité

Annexe III – Sélection d'actions en faveur de la cybersécurité

N°	Intitulé	Pays	Date de début	Date de fin	Coût total (en millions d'euros) et contribution de l'UE (en pourcentage)	Lien vers le portail «Financements et appels d'offres» de l'UE
Subventions destinées à des cyberpôles transfrontières appartenant au système européen d'alerte en matière de cybersécurité						
1	***Establishing Cross-border SOCs (ATHENA)***	Bulgarie, Grèce, Chypre et Malte	1.1.2024	31.3.2028	4,7 (50 %)	
2	***ENSOC-CROSSBORDER PLATFORM (ENSOC)***	Espagne, Italie, Luxembourg, Pays-Bas, Autriche, Portugal et Roumanie	1.1.2024	30.6.2028	10,4 (50 %)	
Subventions destinées au déploiement du réseau de centres nationaux de coordination dans les États membres						
3	***Development and Implementation of the National Cyber Security Coordination and Development Centre for Ireland (NCC-IE)***	Irlande	2.10.2023	1.10.2026	4,2 (47 %)	
4	***Italian National Coordination Centre (NCC-IT)***	Italie	1.11.2023	31.10.2025	2,0 (50 %)	

N°	Intitulé	Pays	Date de début	Date de fin	Coût total (en millions d'euros) et contribution de l'UE (en pourcentage)	Lien vers le portail «Financements et appels d'offres» de l'UE
Subventions destinées au développement des capacités des centres d'opérations de sécurité (SOC), à la promotion d'applications inédites de l'intelligence artificielle et d'autres technologies génériques destinées aux SOC, et à fournir un soutien à la préparation et une assistance mutuelle						
5	***Enhancing the capacity of the Hellenic Consolidated Security Operation Center (EL-SOC)***	Grèce et Chypre	1.1.2024	31.12.2026	9,7 (50 %)	
6	***Greek Security Operations Centre for Small and Medium Enterprises (GR-SME-SOC)***	Grèce	1.1.2024	31.12.2026	12,1 (50 %)	
7	***Next Generation Security Operation Centres (NG-SOC)***	Grèce, Espagne, Chypre, Luxembourg, Slovénie et Norvège	1.1.2024	31.12.2026	4,8 (50 %)	
8	***Irish Local Government Security Operations Centre (ILG-SOC)***	Irlande	1.10.2023	30.9.2026	8,3 (50 %)	
9	***An Interconnected Ecosystem of Cyber Security Coordination and Response Networks (Cyber-CORE-Network)***	Irlande	1.1.2024	31.12.2026	3,6 (50 %)	
10	***Harmonizing People, Processes, and Technology for Robust Cybersecurity (CYberSynchrony)***	Belgique, Grèce, Italie, Chypre et Pays-Bas	1.6.2024	31.5.2027	7,0 (100 %)	
11	***Advanced Cooperative Security Operation Centres (ACSOC)***	Grèce, Italie et Roumanie	1.1.2025	31.12.2027	3,0 (50 %)	

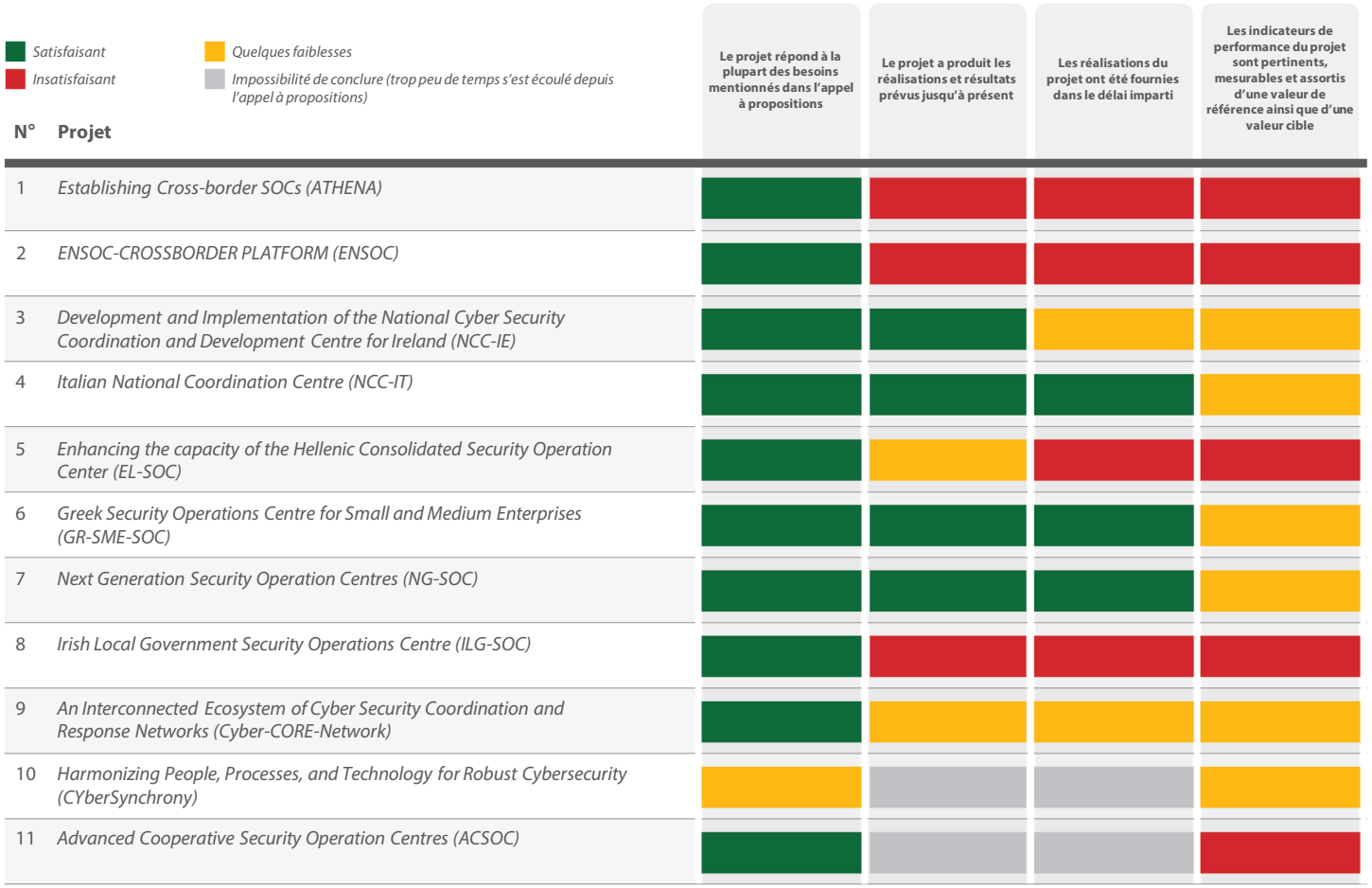
N°	Intitulé	Pays	Date de début	Date de fin	Coût total (en millions d'euros) et contribution de l'UE (en pourcentage)	Lien vers le portail «Financements et appels d'offres» de l'UE
Contrat-cadre pour l'action de soutien à la cybersécurité de l'ENISA						
12	***Supporting ENISA for the Provision of Services under the Cybersecurity Support Action* (28 lots)**	27 lots pour les différents États membres 1 lot paneuropéen	1.12.2022[1]	31.12.2025	28,3 (100 %)	
Contrat de services destiné au *Cyber Situation Centre* de la DG Connect						
13	***Bespoke Service to Support the Cyber Situation and Analysis Centre for the European Commission***	-	30.12.2022	30.12.2026	18,0 (100 %)	

Source: Cour des comptes européenne.

[1] Plusieurs contrats signés en décembre 2022.

Annexe IV – Évaluation par la Cour des projets liés à la cybersécurité, financés par l'UE

Satisfaisant
Quelques faiblesses
Insatisfaisant
Impossibilité de conclure (trop peu de temps s'est écoulé depuis l'appel à propositions)



N°	Projet
1	*Establishing Cross-border SOCs (ATHENA)*
2	*ENSOC-CROSSBORDER PLATFORM (ENSOC)*
3	*Development and Implementation of the National Cyber Security Coordination and Development Centre for Ireland (NCC-IE)*
4	*Italian National Coordination Centre (NCC-IT)*
5	*Enhancing the capacity of the Hellenic Consolidated Security Operation Center (EL-SOC)*
6	*Greek Security Operations Centre for Small and Medium Enterprises (GR-SME-SOC)*
7	*Next Generation Security Operation Centres (NG-SOC)*
8	*Irish Local Government Security Operations Centre (ILG-SOC)*
9	*An Interconnected Ecosystem of Cyber Security Coordination and Response Networks (Cyber-CORE-Network)*
10	*Harmonizing People, Processes, and Technology for Robust Cybersecurity (CYberSynchrony)*
11	*Advanced Cooperative Security Operation Centres (ACSOC)*

Sigles, acronymes et abréviations

Sigle, acronyme ou abréviation	Définition/explication
CSIRT	Centre de réponse aux incidents de sécurité informatique (*Computer security incident response team*)
DG Connect	Direction générale des réseaux de communication, du contenu et des technologies
DIGITAL	Programme pour une Europe numérique
ECCC	Centre de compétences européen en matière de cybersécurité (*European Cybersecurity Competence Centre*)
ECP	Évaluation du contrôle et de la propriété
ENISA	Agence de l'Union européenne pour la cybersécurité
EU-CyCLONe	Réseau européen pour la préparation et la gestion des crises cyber (*European Cyber Crisis Liaison Organisation Network*)
NCC	Centre national de coordination (*National Coordination Centre*)
PME	Petite ou moyenne entreprise
SOC	Centre d'opérations de sécurité (*Security operations centre*)
SRI	Sécurité des réseaux et de l'information

Glossaire

Terme	Définition/explication
Acteur de menace	Personne ou groupe de personnes qui cause un préjudice, perturbe des services ou vole des données, de manière intentionnelle, en exploitant les vulnérabilités de systèmes, de réseaux et d'appareils informatiques.
Centre d'opérations de sécurité	Unité organisationnelle qui œuvre à parer aux cybermenaces et aux incidents de cybersécurité, et qui recueille des renseignements en la matière.
Cybermenace	Possibilité d'utiliser le cyberespace pour compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données ou de systèmes d'information.
Cyberpôle	Plateforme centrale qui rassemble divers services, outils et professionnels de l'informatique pour améliorer la surveillance, la détection et l'analyse des cybermenaces, prévenir les incidents de cybersécurité et contribuer à l'obtention de renseignements sur les cybermenaces.
Incident de cybersécurité (ou cyberincident)	Événement qui compromet la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données ou de systèmes d'information.
Incident de cybersécurité important	Incident de cybersécurité qui a causé ou est susceptible de causer une perturbation grave ou des pertes financières pour une organisation, ou des dommages considérables pour d'autres entités ou des individus.
Incident de cybersécurité majeur	Incident de cybersécurité trop perturbateur pour qu'un État membre puisse y faire face seul ou ayant des incidences importantes sur au moins deux États membres.
Rançongiciel	Logiciel malveillant qui bloque l'accès des victimes à un système informatique ou crypte leurs fichiers de manière à les rendre illisibles, généralement dans le but de contraindre les victimes à payer une rançon en échange du rétablissement de leur accès.
Taxonomie	Dans le domaine de la cybersécurité, classification utilisée pour organiser, catégoriser et structurer les connaissances sur des notions clés telles que celles de menace et d'incident.

Réponses de la Commission

https://www.eca.europa.eu/fr/publications/SR-2026-19

Réponses du Centre de compétences européen en matière de cybersécurité (ECCC)

https://www.eca.europa.eu/fr/publications/SR-2026-19

Réponses de l’Agence de l’Union européenne pour la cybersécurité (ENISA)

https://www.eca.europa.eu/fr/publications/SR-2026-19

Calendrier

https://www.eca.europa.eu/fr/publications/SR-2026-19

L’équipe d’audit

Les rapports spéciaux de la Cour présentent les résultats de ses audits relatifs aux politiques et programmes de l’UE ou à des questions de gestion concernant des domaines budgétaires spécifiques. La Cour sélectionne et conçoit ces activités d’audit de manière à maximiser leur impact en tenant compte des risques pour la performance ou la conformité, du niveau des recettes ou des dépenses concernées, des évolutions escomptées ainsi que de l’importance politique et de l’intérêt du public.

L’audit de la performance objet du présent rapport a été réalisé par la Chambre III (Action extérieure, sécurité et justice), présidée par George-Marius Hyzler, Membre de la Cour. L’audit a été effectué sous la responsabilité de George-Marius Hyzler, Membre de la Cour, assisté de Romuald Kayibanda, chef de cabinet; Annette Farrugia, attachée de cabinet; Cyril Messein, manager principal; Frédéric Soblet, chef de mission; Jurgen Manjé et Flavia Di Marco, auditeurs. L’assistance linguistique a été fournie par Zoe Amador Martínez. La conception graphique a été assurée par Dunja Weibel.

De gauche à droite: Frédéric Soblet, Romuald Kayibanda, George-Marius Hyzler, Jurgen Manjé, Cyril Messein.

DROITS D'AUTEUR

HTML	ISBN 978-92-849-7867-0	ISSN 1977-5695	doi:10.2865/3662378	QJ-01-26-032-FR-Q
PDF	ISBN 978-92-849-7868-7	ISSN 1977-5695	doi:10.2865/4676398	QJ-01-26-032-FR-N

POUR CITER CETTE PUBLICATION

Cour des comptes européenne, «Incidents de cybersécurité: détection et réaction – Le cadre de coopération de l'UE progresse, mais son efficacité reste partielle en raison de retards de mise en œuvre et d'un partage d'informations limité», rapport spécial 19/2026, Office des publications de l'Union européenne, 2026.

Ces dernières années, l'UE a renforcé son cadre réglementaire en matière de cybersécurité et mis en place divers réseaux et mécanismes pour lutter contre les cyberincidents. Elle finance également des projets dans ce domaine par l'intermédiaire du programme pour une Europe numérique.

Nous concluons que l'action de l'UE ne facilite que partiellement la détection des incidents de cybersécurité importants et majeurs et la réaction à ces incidents. Un cadre de coopération a été élaboré au fil des ans, mais les travaux nécessaires pour le rendre entièrement opérationnel sont toujours en cours. Un partage d'informations limité, des faiblesses dans les signalements et des retards considérables dans la mise en œuvre empêchent les réseaux et mécanismes de l'UE d'atteindre leur plein potentiel. Les projets poursuivent des objectifs pertinents, mais certains se heurtent à des difficultés opérationnelles et subissent des retards. Enfin, le cadre global de suivi de la performance présente des faiblesses. Nous formulons des recommandations pour remédier à ces insuffisances.

Rapport spécial de la Cour des comptes européenne présenté en vertu de l'article 287, paragraphe 4, deuxième alinéa, du TFUE.

COUR DES COMPTES EUROPÉENNE

Office des publications de l'Union européenne

COUR DES COMPTES EUROPÉENNE
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Tél. +352 4398-1

Contact: eca.europa.eu/fr/contact
Site web: eca.europa.eu
Réseaux sociaux: @EUauditors