



## Cybersécurité: vers un renforcement des capacités de l'UE à des fins de coopération opérationnelle effective, de solidarité et de résilience

Strasbourg, le 18 avril 2023

La Commission a adopté aujourd'hui une proposition de **règlement de l'UE sur la cybersolidarité** visant à renforcer les capacités de l'Union en matière de cybersécurité. Ce règlement soutiendra la détection des menaces et des incidents de cybersécurité et la sensibilisation à ceux-ci, ainsi que la préparation des entités critiques, et renforcera la solidarité ainsi que les capacités de gestion et de réaction concertées en cas de crise dans l'ensemble des États membres. Le règlement sur la cybersolidarité établit les capacités dont l'Union a besoin pour rendre l'Europe plus résiliente et plus à même de réagir aux cybermenaces, tout en renforçant le mécanisme de coopération existant. Il contribuera à garantir un paysage numérique sûr et sécurisé pour les citoyens et les entreprises et à protéger les entités critiques et les services essentiels, tels que les hôpitaux et les services publics.

La Commission a également présenté une **académie des compétences en matière de cybersécurité**, dans le cadre de l'[Année européenne des compétences 2023](#), afin de garantir une approche plus coordonnée pour remédier à la pénurie de talents dans le secteur de la cybersécurité, condition préalable au renforcement de la résilience de l'Europe. L'académie regroupera diverses initiatives existantes visant à promouvoir les compétences en matière de cybersécurité et les mettra à disposition sur une plateforme en ligne, ce qui renforcera leur visibilité et permettra d'accroître le nombre de professionnels qualifiés en cybersécurité dans l'Union.

Dans le cadre de l'[union européenne de la sécurité](#), l'UE est déterminée à veiller à ce que tous les citoyens et entreprises européens soient bien protégés, tant en ligne que hors ligne, et à promouvoir un cyberspace ouvert, sûr et stable. Toutefois, l'ampleur, la fréquence et l'incidence croissantes des incidents de cybersécurité représentent une menace majeure pour le fonctionnement des réseaux et des systèmes d'information et pour le marché unique européen. L'agression militaire de la Russie contre l'Ukraine a encore exacerbé cette menace, compte tenu de la multiplicité des acteurs criminels et hacktivistes proches de l'État qui sont impliqués dans les tensions géopolitiques actuelles.

En s'appuyant sur un [cadre stratégique et législatif solide](#) déjà en place, la proposition de règlement de l'UE sur la cybersolidarité et l'académie des compétences en matière de cybersécurité contribueront davantage à améliorer la détection des cybermenaces ainsi que la résilience et la préparation à tous les niveaux de l'écosystème européen de cybersécurité.

### Règlement de l'UE sur la cybersolidarité

Le règlement de l'UE sur la cybersolidarité renforcera la solidarité au niveau de l'Union afin de mieux **détecter, anticiper et contrer** les incidents de cybersécurité importants ou de grande ampleur, en créant un «bouclier européen de cybersécurité» et un mécanisme global de réaction d'urgence dans le domaine de la cybersécurité.

Afin de détecter rapidement et efficacement les cybermenaces majeures, la Commission propose la création d'un **cyberbouclier européen, soit une infrastructure paneuropéenne composée de centres d'opérations de sécurité (SOC) nationaux et transfrontières dans l'ensemble de l'Union**. Il s'agit d'entités chargées de détecter et de contrer les cybermenaces. Ces centres utiliseront des technologies de pointe, telles que l'intelligence artificielle (IA) et l'analyse avancée des données, pour détecter les menaces et incidents de cybersécurité et alerter en temps utile par-delà les frontières. À leur tour, les autorités et les entités concernées seront en mesure de réagir de manière plus efficace et plus efficiente aux incidents majeurs.

Ces centres pourraient être opérationnels début 2024. À titre de phase préparatoire du cyberbouclier européen, en avril 2023, la Commission a sélectionné, dans le cadre du programme pour une Europe numérique, [trois consortiums de centres d'opérations de sécurité transfrontières](#) (SOC), réunissant des organismes publics de 17 États membres et d'Islande.

Le règlement de l'UE sur la cybersolidarité prévoit également la création d'un **mécanisme de réaction d'urgence dans le domaine de la cybersécurité** destiné à améliorer la préparation et à renforcer les capacités de réaction aux incidents dans l'Union. Il soutiendra:

- des **mesures de préparation**, notamment la soumission des entités actives dans des secteurs hautement critiques (soins de santé, transports, énergie, etc.) à des tests en vue de détecter d'éventuelles vulnérabilités, sur la base de méthodes et de scénarios de risque communs;
- la **création d'une réserve de cybersécurité de l'UE** consistant en des services de réaction aux incidents, assurés par des fournisseurs de confiance sous contrat et donc prêts à intervenir à la demande d'un État membre ou des institutions, organes et agences de l'Union, en cas d'incident de cybersécurité important ou de grande ampleur;
- la **fourniture d'un soutien financier à l'assistance mutuelle**, lorsqu'un État membre pourrait offrir un soutien à un autre État membre.

En outre, la proposition de règlement établit le **mécanisme d'analyse des incidents de cybersécurité** afin de renforcer la résilience de l'Union en analysant et en évaluant les incidents de cybersécurité importants ou de grande ampleur qui sont survenus et, au besoin, d'émettre des recommandations destinées à améliorer la posture de cybersécurité de l'Union.

Le budget total de toutes les actions relevant du règlement de l'UE sur la cybersolidarité s'élève à **1,1 milliard d'euros**, dont les deux tiers environ seront financés par l'Union au titre du programme pour une Europe numérique.

## Académie européenne des compétences en matière de cybersécurité

L'**académie européenne des compétences en matière de cybersécurité** réunira des initiatives privées et publiques visant à renforcer les compétences en matière de cybersécurité aux niveaux européen et national, en les rendant plus visibles et en contribuant à combler les lacunes des professionnels du secteur de la cybersécurité.

L'académie sera dans un premier temps hébergée en ligne sur la [plateforme de la Commission pour les compétences et les emplois numériques](#). Les citoyens intéressés par une carrière dans le domaine de la cybersécurité pourront trouver sur un site unique en ligne les possibilités de formation et de certification offertes dans toute l'Union. Les parties prenantes pourront également s'engager à soutenir l'amélioration des compétences en matière de cybersécurité dans l'Union en prenant des mesures spécifiques, par exemple en proposant des formations et des certifications en cybersécurité.

L'académie se développera de manière à pouvoir offrir un espace commun aux universités, aux prestataires de formation et aux entreprises du secteur, ce qui les aidera à coordonner les programmes d'enseignement, les formations et les financements ainsi qu'à suivre l'évolution du marché du travail dans le domaine de la cybersécurité.

## Schémas de certification pour les services de sécurité gérés

La Commission a également proposé aujourd'hui une **modification ciblée du règlement sur la cybersécurité**, afin de permettre l'adoption future de schémas européens de certification pour les «services de sécurité gérés». Il s'agit de services hautement critiques et sensibles offerts par des fournisseurs de services de cybersécurité, tels que la réaction aux incidents, les tests de pénétration, les audits et les services de conseil en matière de sécurité, afin d'aider les entreprises et d'autres organisations à prévenir, détecter et contrer les cyberincidents et à se rétablir après de tels incidents.

La certification est essentielle et peut jouer un rôle important dans le contexte de la réserve de cybersécurité de l'UE et de la [directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union](#) (directive SRI 2), facilitant également la fourniture transfrontière de ces services.

## Prochaines étapes

Le Parlement européen et le Conseil vont à présent examiner la **proposition de règlement de l'UE sur la cybersolidarité** ainsi que la **modification ciblée du règlement sur la cybersécurité**.

Le Centre de compétences européen en matière de cybersécurité organisera des acquisitions conjointes d'outils et d'infrastructures avec les **centres d'opérations de sécurité transfrontières** sélectionnés en vue de renforcer les capacités de cyberdéttection.

L'Agence de l'UE pour la cybersécurité (ENISA) et le Centre de compétences européen en matière de cybersécurité continueront de travailler au renforcement des compétences en matière de cybersécurité, contribuant ainsi à la mise en œuvre de l'**académie des compétences en matière de cybersécurité**, conformément à leurs mandats respectifs, et en étroite coopération avec la Commission et les États membres.

La Commission propose que l'académie prenne la forme d'un Consortium pour une infrastructure

numérique européenne (EDIC), c'est-à-dire un nouveau cadre juridique pour la mise en œuvre des projets multinationaux. Cette possibilité va à présent être examinée avec les États membres.

Il est également nécessaire de veiller à ce que les professionnels suivent les formations de qualité requises. À cet égard, l'ENISA élaborera un projet pilote afin d'étudier la possibilité de mettre en place un système européen d'attestation des compétences en matière de cybersécurité.

## Contexte

En proposant un règlement de l'UE sur la cybersolidarité, la Commission répond à l'[invitation des États membres](#) à renforcer la cyberrésilience de l'Union et tient son engagement, pris dans la récente [communication conjointe sur la cyberdéfense](#), de préparer une initiative de l'UE en matière de cybersolidarité.

Le règlement de l'UE sur la cybersolidarité et l'académie des compétences en matière de cybersécurité s'appuient sur la [stratégie de cybersécurité de l'UE](#) ainsi que sur le cadre législatif de l'UE visant à renforcer la résilience collective de l'Union face aux cybermenaces croissantes. Il s'agit notamment de la [directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union](#) (SRI 2) et du [règlement sur la cybersécurité](#).

## Pour en savoir plus

[Questions et réponses](#) - Cybersécurité: vers un renforcement des capacités de l'UE à des fins de coopération opérationnelle effective, de solidarité et de résilience

[Fiche d'information](#) - Règlement de l'UE sur la cybersolidarité

[Fiche d'information](#) - Académie des compétences en matière de cybersécurité

[Proposition de règlement](#) sur la cybersolidarité

[Communication de la Commission](#) sur l'académie des compétences en matière de cybersécurité

[Proposition de règlement](#) modifiant le règlement sur la cybersécurité en ce qui concerne les «services de sécurité gérés»

[Fiche d'information](#) - Stratégie de cybersécurité de l'UE

[Page thématique](#) sur le règlement de l'UE sur la cybersolidarité

[Académie européenne des compétences en matière de cybersécurité — Plateforme pour les compétences et les emplois numériques](#)

IP/23/2243

Quotes:

Avec le train de mesures sur la cybersécurité présenté aujourd'hui, nous montrons qu'en agissant de manière solidaire, nous pouvons bâtir les infrastructures, les compétences et les capacités dont nous avons besoin pour faire face à la multiplication des cybermenaces qui nous touchent tous.

Margrethe Vestager, vice-présidente exécutive pour une Europe adaptée à l'ère du numérique - 18/04/2023

Le règlement de l'UE sur la cybersolidarité et l'académie des compétences en matière de cybersécurité sont nos deux nouveaux instruments concrets pour répondre aux besoins opérationnels de l'Union en matière de cybersécurité: le règlement prévoit des mesures concrètes qui permettront à l'Union de réagir aux menaces et aux attaques, tandis que l'académie vise à renforcer notre socle de compétences de manière à ce que nous disposions des personnes qualifiées dont nous avons besoin à cette fin.

Margaritis Schinas, vice-président chargé de la promotion de notre mode de vie européen - 18/04/2023

Ce jour marque la proposition d'un cyberbouclier européen. Afin de détecter et de contrer efficacement les cybermenaces de grande ampleur et de pouvoir nous rétablir après des incidents de cybersécurité, il est impératif d'investir de toute urgence et de manière substantielle dans les capacités en matière de cybersécurité. Le règlement sur la cybersolidarité constitue une étape essentielle dans notre progression vers la réalisation de cet objectif.

Thierry Breton, commissaire au marché intérieur - 18/04/2023

Personnes de contact pour la presse:

[Johannes BAHRKE](#) (+32 2 295 86 15)

[Marietta GRAMMENO](#) (+32 2 298 35 83)

Renseignements au public: [Europe Direct](#) par téléphone au [00 800 67 89 10 11](#) ou par [courriel](#)

Related media

 [Cybersecurity](#)