COMMISSION
EUROPÉENNE

Bruxelles, le 13.9.2017
SWD(2017) 501 final

**DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION**

**RÉSUMÉ DE L'ANALYSE D'IMPACT**

***accompagnant le document:***

**Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL**

**relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) n° 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité)**

{COM(2017) 477 final}
{SWD(2017) 500 final}
{SWD(2017) 502 final}

## A. NECESSITE D'UNE ACTION

### Quel est le problème et en quoi est-ce un problème?

Les technologies numériques et l'internet constituent l'épine dorsale de la société et de l'économie européennes. Des secteurs économiques essentiels tels que les transports, l'énergie, la santé ou les services financiers dépendent de plus en plus des systèmes informatiques en réseaux pour l'exercice de leur activité principale. L'internet des objets relie les objets et les personnes par le biais de réseaux de communication. Cette nouvelle réalité crée des possibilités sans précédent, mais aussi des vulnérabilités. De fait, les incidents informatiques se multiplient. Leur complexité, leur fréquence et l'«amplitude» de leur impact - ils touchent tant l'accès aux services essentiels que les processus démocratiques - sont appelées à s'accroître encore.

Dans ce contexte, les problèmes suivants, qui sont corrélés, ont été recensés:

- multiplicité des politiques et des approches en matière de cybersécurité dans les États membres;
- dispersion des ressources et des approches de la cybersécurité au sein des institutions, organes et organismes de l'UE;
- sensibilisation insuffisante des particuliers et des entreprises à l'égard des cybermenaces et défaut d'information concernant les propriétés en matière de sécurité des produits et services TIC à la vente, associée à la multiplication des systèmes de certification nationaux et sectoriels.

Ces problèmes se répercutent de manière générale sur la cyberrésilience de l'UE, et sur le fonctionnement efficace du marché intérieur.

### Quels sont les objectifs à atteindre?

Les objectifs spécifiques de l'initiative sont les suivants:

1. développer les capacités et la préparation des États membres et des entreprises, notamment en ce qui concerne les infrastructures critiques;
2. améliorer la coopération et la coordination entre les États membres et les institutions, organes et organismes de l'UE;
3. accroître les moyens au niveau de l'UE pour compléter l'action des États membres, notamment en cas de crise transfrontière;
4. davantage sensibiliser les particuliers et les entreprises aux questions de cybersécurité;
5. accroître globalement la transparence de l'assurance de la cybersécurité des produits et services TIC pour susciter une plus grande confiance dans le marché unique numérique et l'innovation numérique;
6. éviter la multiplication des systèmes de certification dans l'UE, ainsi que des exigences de sécurité et des critères d'évaluation dans les différents États membres et secteurs d'activité.

**Quelle est la valeur ajoutée de l'action au niveau de l'Union?**

Étant donné que la numérisation et l'interconnexion de l'économie et de la société sont des phénomènes de portée mondiale, la dimension de la problématique s'étend bien au-delà du territoire d'un seul État membre. Une intervention au niveau de l'Union est, par conséquent, nécessaire. Dans le contexte actuel, et au vu des perspectives à venir, il s'avère que des mesures prises individuellement par les États membres et une approche fragmentée de la cybersécurité, compte tenu notamment de sa forte dimension transnationale, ne sauraient accroître la cyberrésilience collective de l'Union.

## B. SOLUTIONS

**Quelles sont les différentes options pour atteindre les objectifs? Y a-t-il une option privilégiée?**

La présente analyse d'impact explore un ensemble concret d'options stratégiques concernant l'avenir de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et la certification de sécurité dans le domaine des TIC.

***L'avenir de l'ENISA***

**Option 0** - **Scénario de référence** - C'est l'option qui maintient le statu quo. Le mandat de l'ENISA serait prorogé; les objectifs et les missions de l'Agence resteraient, pour l'essentiel, inchangés, mais elle intégrerait les missions qui lui seraient confiées ultérieurement par la législation de l'UE (par exemple, la directive SRI).

**Option 1** - **Expiration du mandat de l'ENISA** (cessation de l'ENISA). Cette option entraînerait la cessation de l'ENISA au terme de son mandat (juin 2020) et, éventuellement, une redistribution de ses compétences/activités au niveau de l'UE et/ou au niveau national.

**Option 2** - **«Réforme» de l'ENISA**. Cette option s'appuie sur le mandat actuel de l'ENISA et prévoit l'adoption de modifications ponctuelles suivant l'évolution du paysage de la cybersécurité. L'Agence se verrait accorder un statut permanent, reposant sur les piliers suivants: soutien à l'élaboration et à la mise en œuvre de la politique de l'UE; renforcement des capacités; connaissances et information; missions liées au marché; recherche et innovation; coopération opérationnelle et gestion des crises.

**Option 3** - **Une agence de l'UE pour la cybersécurité disposant de moyens opérationnels complets** Cette option prévoit une réforme de l'ENISA qui entraînerait le regroupement de trois fonctions principales: 1) fonction liée aux politiques/fonction de consultation; 2) centre d'information et d'expertise; et 3) équipe d'intervention en cas d'urgence informatique (CERT). Dans une large mesure, cette option supposerait une modification du champ d'application du mandat identique à celle de l'option 2. Cependant, des missions supplémentaires seraient confiées à l'Agence en matière de réaction aux incidents et de gestion des crises, de sorte qu'elle couvrirait le cycle de vie de la cybersécurité dans son intégralité, et s'occuperait tant de la prévention et de la détection des cyberincidents que de la réaction à ces incidents.

***Certification***

**<u>Option 0</u> - Scénario de référence - Pas d'intervention** Dans le cadre de cette option, la Commission maintiendrait le statu quo et n'entreprendrait aucune action politique ou législative.

**<u>Option 1</u> - Mesures non législatives (non contraignantes)** Avec cette option, la Commission utiliserait des instruments de politique non contraignants (par exemple, communications interprétatives, soutien à des initiatives d'autorégulation à l'échelle de l'Union et activités de normalisation) en vue d'améliorer la transparence et de réduire la dispersion des efforts.

**<u>Option 2</u> - Un acte législatif de l'UE pour étendre l'accord du SOG-IS à tous les États membres**. Avec cette option, la Commission proposerait un acte législatif pour étendre, d'un point de vue juridique, l'accord du SOG-IS à tous les États membres.

**<u>Option 3</u> - Un cadre européen général de certification de sécurité en matière de TIC**. Cette option implique la mise en place d'un cadre européen de certification de sécurité en matière de TIC (comprenant un groupe d'experts composé d'autorités nationales) en partant, dans la mesure du possible, des systèmes de certification de sécurité existants en matière de TIC. En substance, le cadre devrait permettre l'établissement de systèmes européens de certification qui seraient reconnus par tous les États membres.

L'option privilégiée est une combinaison de l'option 2 pour l'ENISA et de l'option 3 pour la certification.

**Quelles sont les différentes parties prenantes? Qui soutient quelle option?**

La grande majorité des parties prenantes de toutes catégories (États membres, industrie, institutions de l'Union européenne, communauté scientifique) ayant participé à la consultation semblent favorables à l'option privilégiée car elles sont partisanes du renforcement de l'ENISA et de la création d'un cadre européen de certification de sécurité en matière de TIC.

Un consensus se dégage, en particulier, sur la nécessité de doter l'Union (au minimum) d'une agence qui fonctionne bien, dotée d'un statut permanent, disposant de moyens suffisants et d'un mandat lui permettant de faire face aux défis actuels et futurs en matière de cybersécurité. En outre, les parties prenantes approuvent globalement la création d'un cadre européen facultatif et évolutif.

Du côté de l'industrie, la solution prônée pour la certification est soutenue par des entreprises qui sont déjà soumises à des exigences en matière de certification, et qui tireraient avantage d'un mécanisme à l'échelle de l'Union européenne fondé sur la reconnaissance mutuelle des certificats. Cette solution recueille également l'adhésion des PME, qui sont les entreprises qui pâtissent déjà, ou pâtiraient, le plus d'avoir à suivre différentes procédures de certification d'un État membre à l'autre. Certains États membres, en particulier ceux qui disposent du moins de ressources, et certains représentants de l'industrie et des institutions de l'UE ont également exprimé des avis positifs concernant l'option 3 pour l'ENISA.

## C. INCIDENCE DE L'OPTION PRIVILEGIEE.

### Quels sont les avantages de l'option privilégiée (ou, à défaut, des options principales)?

Dans le cadre de l'option privilégiée, l'UE disposerait d'une agence dont la principale finalité serait de prêter son soutien aux États membres, aux institutions de l'UE et aux entreprises dans les domaines où elle apporterait la plus forte valeur ajoutée. Ces domaines seraient les suivants: soutien à la mise en œuvre de la directive SRI; élaboration et mise en œuvre de la politique; information, connaissances et sensibilisation; recherche; coopération opérationnelle et gestion des crises; marché. En particulier, l'ENISA appuierait la politique de l'Union dans le domaine de la certification de sécurité en matière de TIC, en assurant l'administration et la gestion technique d'un cadre européen de certification de sécurité en matière de TIC. Un tel cadre mettra effectivement en place un ensemble de règles concernant la gouvernance de la certification de sécurité en matière de TIC dans l'UE, qui agirait en faveur d'un système de reconnaissance mutuelle des certificats délivrés dans les différents États membres. La combinaison de ces options est considérée comme étant la solution la plus efficace pour atteindre les objectifs déclarés, à savoir: accroître les capacités en matière de cybersécurité, la préparation, la coopération et la transparence, et éviter le morcellement du marché. Elle a également été jugée la plus conforme aux priorités d'action de l'UE, puisqu'elle est bien ancrée dans la stratégie de cybersécurité et les politiques qui s'y rapportent (p. ex. la directive SRI), et dans la stratégie pour le marché unique numérique. De plus, cette solution permettrait d'atteindre les objectifs fixés grâce à une utilisation raisonnable des ressources.

### Quels sont les coûts de l'option privilégiée (le cas échéant, sinon des options principales)?

Malgré les nouveaux rôles qu'elle se verrait confier, l'«ENISA réformée» resterait une organisation souple. La contribution financière du budget de l'UE serait supérieure à ce qu'elle est actuellement, mais resterait passablement moins élevée que celle requise pour d'autres agences qui opèrent également dans des domaines critiques.

La création d'un cadre européen de certification de sécurité en matière de TIC ne devrait pas entraîner de coûts initiaux supplémentaires pour l'industrie (y compris les PME). Au contraire, elle permettrait aux entreprises qui certifient déjà leurs produits ou souhaitent mettre en place une certification de sécurité de réaliser des économies considérables, ce qui aurait des effets positifs sur leur compétitivité au niveau mondial. Par contre, elle nécessiterait certains engagements budgétaires afin d'assurer la logistique du cadre européen, lesquels seraient essentiellement assumés par l'«ENISA réformée», pour ce qui est de l'assistance technique et des tâches de secrétariat.

### Y aura-t-il une incidence notable sur les budgets nationaux et les administrations nationales?

Non. Les coûts liés au renforcement de l'ENISA devraient principalement être pris en charge par le budget de l'UE, mais les États membres seraient toujours en mesure de fournir à titre volontaire des contributions financières à l'Agence. En ce qui concerne la certification, les principales répercussions sur les budgets nationaux et les administrations nationales viendraient, le cas échéant, de la mise en place d'une autorité de certification.

**Y aura-t-il d'autres incidences notables?**

Non.

**Proportionnalité**

L'option privilégiée prévoit des mesures équilibrées, toutes jugées nécessaires pour atteindre les objectifs visés, sans imposer de charges excessives aux acteurs concernés. Dès lors, l'initiative est jugée conforme au principe de proportionnalité.

## D. SUIVI

**Quand la législation sera-t-elle réexaminée?**

Il est maintenant proposé que la première évaluation ait lieu cinq ans après l'entrée en vigueur de l'instrument juridique. La Commission transmettra ensuite au Parlement européen et au Conseil un rapport sur son évaluation, accompagné le cas échéant d'une proposition en vue de sa révision. De nouvelles évaluations devront avoir lieu tous les cinq ans.