Consultation publique sur le partenariat public-privé contractuel en matière de cybersécurité et sur d'éventuelles mesures d'accompagnement

Les champs marqués d'un * sont obligatoires.

Consultation publique sur le partenariat public-privé contractuel en matière de cybersécurité et sur d'éventuelles mesures d'accompagnement

Objet

Le 6 mai 2015, la Commission européenne a adopté la «stratégie pour un marché unique numérique », qui prévoit la création, au cours du premier semestre de 2016, d'un partenariat public-privé contractuel en matière de cybersécurité dans le domaine des technologies et des solutions pour la sécurité des réseaux en ligne.

La Commission consulte à présent les parties prenantes au sujet des domaines d'activité du futur partenariat public-privé contractuel en matière de cybersécurité. Elle souhaite également recueillir des contributions concernant les éventuelles mesures supplémentaires que les pouvoirs publics pourraient prendre pour stimuler le secteur de la cybersécurité en Europe.

En ce qui concerne la normalisation dans le secteur de la cybersécurité, la présente consultation complète la consultation publique générale relative à l'élaboration du plan en matière de normes prioritaires dans le domaine des TIC («Les normes applicables au marché unique numérique: fixer les priorités, obtenir des résultats»), dans laquelle la cybersécurité est mentionnée.

La Commission se servira des résultats de la consultation pour établir le partenariat public-privé contractuel au cours du premier semestre de 2016.

Contexte

Les politiques actuelles de l'Union européenne (UE), telles que la stratégie de cybersécurité de l'Union européenne et la proposition de directive sur la sécurité des réseaux et de l'information (SRI), présentée par la Commission, visent à faire en sorte que les réseaux et systèmes informatiques, y compris les infrastructures critiques, soient adéquatement protégés et sécurisés.

Des travaux considérables ont déjà été réalisés avec les parties prenantes du secteur au sein de la plateforme SRI. En particulier, le groupe de travail n° 3 de la plateforme SRI a mis au point un programme de recherche stratégique pour la cybersécurité qui sert de base aux questions de la présente consultation portant sur les priorités en matière de recherche et d'innovation.

La mise en place d'un partenariat public-privé contractuel relatif à la sécurité numérique constituerait une avancée supplémentaire vers une politique sectorielle en matière de cybersécurité. La Commission réfléchit à présent aux mesures sectorielles supplémentaires qui pourraient être nécessaires pour compléter ce partenariat.

Le partenariat public-privé contractuel consistera en un accord contractuel entre la Commission et un groupement d'entreprises, les parties s'engageant à soutenir, dans le cadre du programme Horizon 2020 de l'UE, des activités de recherche et d'innovation revêtant une importance stratégique en vue d'assurer la compétitivité de l'Union dans le domaine de la cybersécurité.

Un partenariat public-privé contractuel rassemblant des ressources publiques et privées se concentrerait sur l'innovation selon une feuille de route stratégique en matière de recherche et d'innovation définie conjointement. Il utiliserait les fonds disponibles au mieux en assurant une meilleure coordination avec les États membres et en mettant plus spécifiquement l'accent sur un petit nombre de priorités techniques. Il devrait mobiliser des fonds d'Horizon 2020 afin d'apporter à la fois des innovations technologiques et des avantages sociétaux aux utilisateurs de technologies (particuliers, PME, infrastructures critiques) et de faire connaître l'excellence européenne en matière de recherche et d'innovation dans les domaines de la cybersécurité et de la protection de la vie privée dans l'environnement numérique. Par ailleurs, la cybersécurité est mentionnée expressément, dans la stratégie pour un marché unique numérique, parmi les domaines prioritaires dans lesquels il convient de définir des normes technologiques manquantes.

Durée

La consultation débute le 18 décembre 2015 et se termine le 11 mars 2016 (12 semaines)

Aucune observation reçue après la date de clôture ne sera prise en considération.

Qui est invité à répondre?

- Entreprises (fournisseurs et utilisateurs de produits et services de cybersécurité)
- Associations sectorielles
- Organisations de la société civile
- Autorités publiques
- Organismes de recherche et universités
- Particuliers

Transparence

Veuillez indiquer si vous répondez en tant que particulier ou en tant que représentant d'une organisation. Nous demandons aux organisations qui répondent de s'inscrire au registre de transparence. Les contributions des organisations non inscrites seront publiées séparément de celles des organisations inscrites, avec les contributions des particuliers.

Comment répondre?

Répondez en ligne.

Vous pouvez vous interrompre à tout moment et reprendre plus tard. Vous pouvez télécharger une copie de votre contribution une fois que vous l'avez envoyée.

Seules les réponses transmises au moyen du questionnaire en ligne seront prises en compte et intégrées dans le rapport de synthèse, exception faite des réponses des malvoyants.

Accessibilité aux malvoyants

Nous accepterons les questionnaires que les malvoyants et les organisations les représentant nous transmettront par courrier électronique ou sur papier, par voie postale: télécharger le questionnaire.

Par courrier électronique: joignez votre contribution sous forme de fichier Word, PDF ou ODF.

Ou

Par voie postale: adressez votre courrier à l'adresse ci-dessous:

Commission européenne

DG Réseaux de communication, contenu et technologies

Unité H4 – Confiance et sécurité
Avenue Beaulieu 25
1049 Bruxelles – Belgique

Réponses et commentaires

Nous publierons sur cette page une analyse des résultats de la consultation un mois après la clôture de celle-ci.

Protection des données à caractère personnel

À des fins de transparence, l'ensemble des réponses à la présente consultation seront rendues publiques.

Veuillez lire la déclaration spécifique relative à la protection de la vie privée qui figure ci-dessous pour savoir comment nous traitons vos données à caractère personnel et vos contributions.

- Protection des données à caractère personnel
- Déclaration spécifique relative à la protection de la vie privée

Références

Politiques actuelles de l'UE dans le domaine:

- stratégie de cybersécurité de l'UE
- proposition de directive sur la sécurité des réseaux et de l'information, présentée par la Commission européenne
  - travaux sur la protection de la vie privée en ligne
  - travaux réalisés avec les parties prenantes au sein de la plateforme sur la sécurité des réseaux et de l'information

Contact

CNECT-FEEDBACK-CYBERSECURITY-DSM@ec.europa.eu

Informations générales vous concernant

Veuillez noter que les champs marqués d’un astérisque (*) sont obligatoires.

* Souhaitez-vous que votre contribution soit publiée?

Veuillez indiquer clairement si vous ne souhaitez pas que votre contribution soit publiée.

- Oui
- Non

Les contributions transmises de manière anonyme ne seront ni publiées, ni prises en considération.

* Il est possible que la Commission prenne contact avec vous si une clarification est nécessaire concernant votre contribution, en fonction de votre réponse à la question suivante.

Souhaitez-vous être contacté?

- Oui
- Non

* Vous répondez en tant que:

- particulier, à titre personnel
- représentant d'une organisation/entreprise/institution

* Quelle est votre nationalité?

- Autrichienne
- Belge
- Bulgare
- Croate
- Chypriote
- Tchèque
- Danoise
- Estonienne
- Finlandaise
- Française
- Allemande
- Grecque
- Hongroise
- Italienne
- Irlandaise
- Lettone
- Lituanienne
- Luxembourgeoise
- Maltaise
- Néerlandaise
- Polonaise
- Portugaise
- Roumaine
- Slovaque
- Slovène
- Espagnole
- Suédoise
- Britannique
- Autre

Si vous avez répondu «Autre», veuillez préciser.

200 caractère(s) maximum

Votre organisation est-elle inscrite au registre de transparence de la Commission européenne et du Parlement européen?

- Oui
- Non

Veuillez indiquer votre numéro d'inscription au registre de transparence. Nous vous encourageons à vous inscrire au registre de transparence avant de répondre au présent questionnaire. Si votre organisation/institution répond au questionnaire sans s'être inscrite au registre, la Commission considérera ses réponses comme celles d'un particulier et les publiera comme telles.

Veuillez cocher la case correspondant à votre organisation et secteur d'activité.

- Administration nationale
- Autorité nationale de régulation
- Autorité régionale
- Organisation non gouvernementale
- Petite ou moyenne entreprise
- Microentreprise
- Plateforme ou association représentative au niveau européen
- Association représentative au niveau national
- Organisme de recherche/université
- Presse
- Autre

Si vous avez répondu «Autre», veuillez préciser.

Pays où votre institution/organisation/entreprise exerce son activité:

- [ ] Tous les États membres de l'UE
- [ ] Autriche
- [ ] Belgique
- [ ] Bulgarie
- [ ] République tchèque
- [ ] Croatie
- [ ] Chypre
- [ ] Danemark
- [ ] Estonie
- [ ] France
- [ ] Finlande
- [ ] Allemagne
- [ ] Grèce
- [ ] Hongrie
- [ ] Italie
- [ ] Irlande
- [ ] Lettonie
- [ ] Lituanie
- [ ] Luxembourg
- [ ] Malte
- [ ] Pays-Bas
- [ ] Pologne
- [ ] Portugal
- [ ] Roumanie
- [ ] Espagne
- [ ] Slovénie
- [ ] Slovaquie
- [ ] Suède
- [ ] Royaume-Uni
- [ ] Autre

* Veuillez indiquer le nom de votre institution/organisation/entreprise.

* Veuillez indiquer votre nom.

* Veuillez indiquer l'adresse de votre institution/organisation/entreprise.

Veuillez indiquer votre numéro de téléphone.

* Veuillez indiquer votre adresse électronique.

* Quel est votre lieu d'établissement principal ou le lieu d'établissement principal de l'entité que vous représentez (siège)?

Consultation

Remarques

- *En fonction de la question, veuillez choisir une seule ou plusieurs réponses.*
- *Veuillez noter qu'un nombre maximal de caractères a été défini pour la plupart des questions ouvertes.*

I. Définition de vos priorités en matière de cybersécurité

* 1. Quelle partie de la chaîne de valeur des services et produits de cybersécurité représentez-vous?

- ☐ Chercheur
- ☐ Client/utilisateur
- ☐ Fournisseur de produits et/ou services de cybersécurité
- ☐ Autorité ou organisme public chargé(e) de la cybersécurité/recherche

Si vous avez répondu «Chercheur», veuillez préciser.

400 caractère(s) maximum

Si vous avez répondu «Client/utilisateur», veuillez préciser.

- [ ] Agent de certification/d'audit ou de normalisation
- [ ] Utilisateur individuel
- [ ] PME utilisatrice
- [ ] Entreprise privée
- [ ] Utilisateur public
- [ ] Société civile
- [ ] Autre

Si vous avez répondu «Autre», veuillez préciser.

400 caractère(s) maximum

2. En quoi consistent les activités de votre institution/organisation/entreprise dans le domaine de la cybersécurité? (plusieurs réponses possibles)

2.1. Cybersécurité pure -> produits/services de cybersécurité

- [ ] Gestion des identités et des accès
- [ ] Sécurité des données
- [ ] Sécurité des applications
- [ ] Sécurité des infrastructures (réseaux)
- [ ] Sécurité du matériel (appareils)
- [ ] Services d'audit, de planification et de conseil en matière de sécurité informatique
- [ ] Formation à la sécurité informatique
- [ ] Autre

Si vous avez répondu «Autre», veuillez préciser.

400 caractère(s) maximum

2.2. Cybersécurité appliquée -> domaines d'application dans lesquels des produits/services de cybersécurité sont nécessaires

- [ ] Infrastructures critiques en général
- [ ] Énergie
- [ ] Transports
- [ ] Santé
- [ ] Activités financières et bancaires
- [ ] Administration publique
- [ ] Villes intelligentes
- [ ] Fournisseurs de services numériques
- [ ] Protection des utilisateurs individuels
- [ ] Protection des PME
- [ ] Autre

Veuillez préciser:

400 caractère(s) maximum

2.3. Cybersécurité appliquée -> domaines informatiques spécifiques dans lesquels la cybersécurité est une exigence fonctionnelle

- [ ] Internet des objets
- [ ] Systèmes embarqués
- [ ] Informatique en nuage
- [ ] 5G
- [ ] Données massives
- [ ] Smartphones
- [ ] Ingénierie logicielle
- [ ] Ingénierie matérielle
- [ ] Autre

Veuillez préciser.

400 caractère(s) maximum

II. Évaluation des risques et des menaces pour la cybersécurité

1. Détermination des risques

* 1.1. Quels sont les défis les plus urgents en matière de cybersécurité pour les utilisateurs (particuliers, entreprises, secteur public)?

entre 1 et 3 choix

- [ ] La perte de savoir-faire et d'informations commerciales confidentielles (secrets d'affaires) et d'autres types d'informations confidentielles — espionnage industriel et économique
- [ ] Le sabotage industriel ou économique (la perturbation ou le ralentissement du fonctionnement des réseaux et des ordinateurs, par exemple)
- [ ] L'extraction et l'utilisation de données d'identité et de paiement à des fins frauduleuses
- [ ] L'intrusion dans la vie privée
- [ ] Autre

* Veuillez préciser.

1200 caractère(s) maximum

* 1.2. Dans quels secteurs/domaines les risques sont-ils les plus marqués? (Veuillez en choisir 3 à 5.)

entre 3 et 5 choix

- [ ] Infrastructures critiques en général
- [ ] Énergie
- [ ] Transports
- [ ] Santé
- [ ] Activités financières et bancaires
- [ ] Administration publique
- [ ] Villes intelligentes
- [ ] Fournisseurs de services numériques
- [ ] Protection des utilisateurs individuels
- [ ] Protection des PME
- [ ] Autre
- [ ] Je ne sais pas.

Veuillez préciser.

400 caractère(s) maximum

2. Niveau de préparation

* 2.1. Les produits/services nécessaires pour assurer la sécurité de l'ensemble de la chaîne de valeur sont-ils disponibles sur le marché européen?

- ( ) Oui
- ( ) Non
- ( ) Je ne sais pas

Si votre réponse est «Non», veuillez donner des exemples des produits/services qui manquent:

400 caractère(s) maximum

2.2. Le cas échéant, d'où proviennent les produits/services de cybersécurité que vous achetez?

- ☐ Fournisseur national/de votre pays
- ☐ Fournisseur européen, d'un pays autre que le vôtre
- ☐ États-Unis
- ☐ Israël
- ☐ Russie
- ☐ Chine
- ☐ Japon
- ☐ Corée du Sud
- ☐ Autre

Si vous avez répondu «Autre», veuillez préciser.

200 caractère(s) maximum

2.3. Le cas échéant, quelles raisons vous poussent à choisir des produits/services de sécurité des TIC non européens plutôt que des produits/services européens?

- ☐ La compétitivité des prix
- ☐ Les produits/services non européens sont plus innovants
- ☐ La fiabilité
- ☐ L'interopérabilité des produits/solutions
- ☐ Le manque d'offre en Europe
- ☐ Le lieu d'origine est sans importance
- ☐ Autre

Si vous avez répondu «Autre», veuillez préciser.

800 caractère(s) maximum

2.4. Si cette question s'applique à vous, pour quelles raisons l'offre de produits/services de cybersécurité est-elle insuffisante?

- ☐ Manque de capitaux pour élaborer de nouveaux produits/services
- ☐ Demande insuffisante (au niveau national/européen/mondial) pour justifier des investissements
- ☐ Absence d'économies d'échelle pour les marchés envisagés (au niveau national/européen/mondial)
- ☐ Obstacles sur le marché
- ☐ Autre
- ☐ Je ne sais pas

Si vous avez répondu «Autre», veuillez préciser.

1200 caractère(s) maximum

Si vous avez répondu «Obstacles sur le marché» à la question 2.4, veuillez préciser.

- ☐ Dans l'État membre de l'UE où vous opérez
- ☐ Entre les États membres de l'UE
- ☐ Au niveau mondial
- ☐ Entre les secteurs d'activité
- ☐ Autre

Si vous avez répondu «Autre», veuillez préciser.

800 caractère(s) maximum

3. Incidences

* 3.1. Selon vous, dans quels domaines le préjudice socio-économique pourrait-il être le plus grave? (Veuillez en choisir 1 à 5.)

entre 1 et 5 choix

- [ ] Infrastructures critiques
- [ ] Énergie
- [ ] Transports
- [ ] Santé
- [ ] Activités financières et bancaires
- [ ] Administration publique
- [ ] Villes intelligentes
- [ ] Fournisseurs de services numériques
- [ ] Protection des utilisateurs individuels
- [ ] Protection des entreprises (grandes entreprises et/ou PME)
- [ ] Autre
- [ ] Je ne sais pas

Veuillez préciser/expliquer.

1200 caractère(s) maximum

4. Défis en matière de cybersécurité d'ici à 2020

4.1. Quels seront les trois principaux défis en matière de cybersécurité d'ici à 2020? (Veuillez expliquer.)

1200 caractère(s) maximum

III. Conditions sur le marché de la cybersécurité

1. Dans quelle mesure les marchés des produits/services de cybersécurité sont-ils concurrentiels en Europe? Veuillez donner votre appréciation de la situation générale en Europe et votre point de vue sur vos secteurs d'expertise particuliers.

1200 caractère(s) maximum

2. Si vous représentez une entreprise ayant son siège dans l'Union européenne, quelle est votre appréciation de la situation des PME et jeunes pousses (start-ups) innovantes qui opèrent dans le domaine de la cybersécurité et de la protection de la vie privée dans l'Union européenne?
a. Veuillez donner votre appréciation de la facilité d'accès aux marchés de pays de l'UE autres que le vôtre.
b. Veuillez donner votre appréciation des possibilités d'exercer des activités au sein du marché unique européen.

1200 caractère(s) maximum

3. Si vous représentez une entreprise ayant son siège en dehors de l'Union européenne, veuillez:
a. donner votre appréciation de la facilité d'accès au marché de l'UE;
b. donner votre appréciation des possibilités d'exercer des activités au sein du marché unique européen;
c. expliquer combien vous avez investi en Europe au cours des cinq dernières années et combien vous comptez investir en Europe au cours des cinq prochaines années.

1200 caractère(s) maximum

4. Quelle est la compétitivité de l'Europe par rapport à d'autres pays/régions? En particulier, quels sont les points forts et les points faibles des fournisseurs européens de solutions en matière de cybersécurité? (Si vous êtes un fournisseur, autoévaluez-vous.)

1200 caractère(s) maximum

5. Selon vous, quel niveau d'ambition l'Union européenne devrait-elle se fixer pour le développement du marché de la cybersécurité? (Veuillez cocher une case pour chaque catégorie.)

	Rester en tête au niveau mondial	Tenter d'arriver en tête au niveau mondial	Rendre l'UE plus compétitive
*Gestion des identités et des accès	○	○	○
*Sécurité des données	○	○	○
*Sécurité des applications	○	○	○
*Sécurité des infrastructures (réseaux)	○	○	○
*Sécurité du matériel (appareils)	○	○	○
*Services d'audit, de planification et de conseil en matière de sécurité informatique	○	○	○
*Services de gestion et d'exploitation en matière de sécurité informatique	○	○	○
*Formation à la sécurité informatique	○	○	○

6. Quelles incidences la législation (actuellement en vigueur ou dont l'adoption est imminente) a-t-elle ou est-elle susceptible d'avoir sur le(s) marché(s) européen(s) de la cybersécurité?

1200 caractère(s) maximum

7. Quels effets les marchés publics ont-ils sur le marché européen de la cybersécurité?

- ○ Ils stimulent le développement du marché de la cybersécurité et permettent aux entreprises d'accroître leur part du marché.
- ○ Ils constituent un obstacle à l'accès au marché.
- ○ Je ne sais pas.

Veuillez expliquer:

1200 caractère(s) maximum

8. Estimez-vous avoir un accès suffisant à des ressources financières pour financer des projets/initiatives en matière de cybersécurité?

- ◯ Oui
- ◯ Non

9. Quels sont les types de ressources financières que vous utilisez actuellement?

- ☐ Prêts bancaires
- ☐ Fonds d'actions
- ☐ Fonds de capital-risque
- ☐ Soutien de la BEI/du FEI
- ☐ Fonds souverains
- ☐ Financement participatif
- ☐ Fonds de l'UE
- ☐ Autre

Si vous avez répondu «Autre», veuillez préciser.

600 caractère(s) maximum

10. Selon vous, le secteur des équipements TIC et de la sécurité des TIC en Europe dispose-t-il de ressources humaines qualifiées en suffisance?

- ◯ Oui
- ◯ Non
- ◯ Je ne sais pas.

Veuillez expliquer.

1200 caractère(s) maximum

11. Avez-vous déjà été confronté à des obstacles pour accéder au marché et exporter au sein de l'UE et/ou en dehors de l'UE?

- ◯ Oui
- ◯ Non

Veuillez les décrire.

1200 caractère(s) maximum

12. Avez-vous connaissance de mesures des pouvoirs publics en faveur des jeunes pousses (start-ups) du secteur de la cybersécurité dans votre pays/l'Union européenne?

- Oui
- Non

Veuillez les décrire.

1200 caractère(s) maximum

IV. Nécessité d'une intervention et d'un soutien des pouvoirs publics aux fins du bon fonctionnement du marché des produits/services de cybersécurité en Europe

1. Selon vous, quels sont les domaines dans lesquels le marché européen des produits et services de cybersécurité fonctionne bien et une intervention publique serait inutile voire néfaste? (Veuillez préciser.)

1200 caractère(s) maximum

2. Quels sont les problèmes qui doivent être réglés au niveau européen pour mettre en place un marché unique numérique des produits/services de cybersécurité qui soit pleinement opérationnel? (Veuillez préciser.)

1200 caractère(s) maximum

3. Quelle est votre appréciation du soutien et de l'intervention des pouvoirs publics au niveau national en ce qui concerne le marché de la cybersécurité? Dans quelle mesure sont-ils utiles/nécessaires/adéquats? (Veuillez préciser.)

1200 caractère(s) maximum

4. Veuillez fournir des exemples de soutien fructueux grâce aux politiques des pouvoirs publics (au niveau national ou international).

1200 caractère(s) maximum

V. Mesures sectorielles spécifiques

La première question de cette section complète la consultation publique générale relative au plan en matière de normes prioritaires dans le domaine des TIC pour ce qui est des caractéristiques spécifiques de la normalisation dans le secteur de la cybersécurité. Dans ce contexte, nous entendons par «normalisation» l'élaboration de spécifications techniques, de normes ou d'architectures lorsqu'il existe un besoin/une lacune, mais aussi tout autre type de mesure de normalisation, comme l'analyse du paysage, la détection des lacunes, l'élaboration de feuilles de route ou la constitution d'écosystèmes.

1. Comment évalueriez-vous le rôle actuel de la normalisation dans le domaine de la cybersécurité?

* 1.1. Avez-vous appliqué ou travaillez-vous actuellement avec des spécifications techniques, des normes ou des architectures particulières en lien avec la cybersécurité?

1200 caractère(s) maximum

1.2. Dans quels domaines existe-t-il un besoin/une lacune à cet égard?

1200 caractère(s) maximum

* 1.3. Selon vous, la normalisation pourrait-elle soutenir l'innovation et le marché unique numérique en matière de cybersécurité?

- Oui
- Non
- Je ne sais pas.

* Veuillez expliquer votre point de vue.

1200 caractère(s) maximum

* 1.4. La normalisation en matière de cybersécurité devrait-elle être abordée de manière générale ou cibler des secteurs spécifiques (par exemple, les transports, l'énergie, la finance) et des domaines d'application précis (par exemple, les véhicules connectés, les réseaux intelligents, les paiements électroniques)? (Veuillez préciser votre choix.)

1200 caractère(s) maximum

* 1.5. Sur quels domaines les futurs efforts de normalisation en matière de cybersécurité devraient-ils se concentrer? (Veuillez préciser.)

1200 caractère(s) maximum

2. Évaluation des systèmes de certification existants dans le domaine de la cybersécurité

* 2.1. Êtes-vous actif dans des organismes de certification publics ou privés?

- Oui
- Non

* Dans l'affirmative, veuillez préciser.

600 caractère(s) maximum

2.2. Selon vous, quels sont les systèmes de certification existants en matière de sécurité des TIC qui ont fait leurs preuves et quels enseignements faudrait-il tirer de ces systèmes pour les futures activités de certification en matière de cybersécurité?

1200 caractère(s) maximum

* 2.3. Les systèmes de certification actuels en matière de sécurité des TIC répondent-ils de manière appropriée aux besoins des entreprises européennes (qui fournissent ou achètent des solutions en matière de cybersécurité)?

- Oui
- Non
- Je ne sais pas.

Veuillez expliquer.

1200 caractère(s) maximum

* 2.4. Quelle est l'importance des systèmes de certification pour le marché unique numérique des produits et services de cybersécurité?

1200 caractère(s) maximum

* 2.5. Sur quels domaines les futurs travaux de certification devraient-ils se concentrer?

1200 caractère(s) maximum

* 2.6. Les systèmes de certification font-ils l'objet d'une vaste reconnaissance mutuelle entre les différents États membres de l'Union européenne?

- Oui
- Non
- Je ne sais pas.

* Veuillez préciser.

1200 caractère(s) maximum

* 2.7. Est-il facile de démontrer l'équivalence entre les normes, les systèmes de certification et les labels?

- Oui
- Non
- Je ne sais pas.

Veuillez expliquer.

1200 caractère(s) maximum

* 3. Avez-vous connaissance de l'existence de systèmes de labellisation des produits et services de cybersécurité en Europe ou dans le reste du monde?

- Oui
- Non

* 3.1. Dans l'affirmative, veuillez préciser si vous faites référence à des systèmes de labellisation légaux ou à des systèmes d'autolabellisation des entreprises du secteur.

600 caractère(s) maximum

3.2. Dans l'affirmative, comment évaluez-vous l'efficacité de ces labels pour ce qui est d'assurer la visibilité et la lisibilité pour les acheteurs?

800 caractère(s) maximum

* 3.3. Comment évalueriez-vous la nécessité de créer de nouveaux labels ou d'étendre les labels existants en Europe?

1200 caractère(s) maximum

* 3.4. Pour quel(s) marché(s) des labels de cybersécurité seraient-ils les plus bénéfiques?

- [ ] Marché de consommation
- [ ] Marché professionnel (PME)
- [ ] Marché professionnel (grandes entreprises)
- [ ] Je ne sais pas.

3.5. Quels sont les critères/exigences spécifiques nécessaires pour que ces labels soient fiables?

1200 caractère(s) maximum

* 4. Quelle forme d'accès au financement serait la plus utile aux acteurs européens du secteur de la cybersécurité, afin d'encourager la croissance des entreprises?

entre 1 et 5 choix

- [ ] Prêts bancaires
- [ ] Fonds d'actions
- [ ] Fonds de capital-risque
- [ ] Soutien de la BEI/du FEI
- [ ] Fonds souverains
- [ ] Financement participatif
- [ ] Fonds de l'UE (veuillez préciser)
- [ ] Autre

* Veuillez expliquer.

1200 caractère(s) maximum

5. Selon vous, quelles mesures spécifiques des pouvoirs publics en faveur des jeunes pousses (start-ups) sont utiles pour le secteur de la cybersécurité dans l'Union européenne?

1200 caractère(s) maximum

6. Selon vous, quelles seraient les mesures adéquates pour soutenir la stratégie de l'UE relative à l'accès au marché et à l'exportation des produits et services de cybersécurité?

1200 caractère(s) maximum

7. Comment évalueriez-vous le rôle des groupements nationaux/régionaux en matière de cybersécurité (ou des centres d'excellence nationaux/régionaux en matière de cybersécurité) et leur efficacité pour encourager les politiques sectorielles dans le domaine de la cybersécurité?

1200 caractère(s) maximum

8. Pensez-vous à d'autres instruments spécifiques des pouvoirs publics qui pourraient être utiles pour soutenir le développement du secteur de la cybersécurité en Europe?

1200 caractère(s) maximum

VI. Le rôle de la recherche et de l'innovation dans le domaine de la cybersécurité

1. Avez-vous participé aux précédents efforts de recherche et d'innovation dans le cadre de programmes européens (7e PC, CIP)?

- Oui
- Non

* 1.1. Dans l'affirmative, quelle a été votre appréciation de cette participation et quels ont été les principaux résultats pour votre organisation?

1200 caractère(s) maximum

* 1.2. Quelles ont été les principales incidences des sujets et des projets financés dans le domaine de la cybersécurité?

1200 caractère(s) maximum

* 1.3. Quelles ont été les principales faiblesses dans la manière dont la cybersécurité a été abordée dans les précédents programmes de recherche et d'innovation?

1200 caractère(s) maximum

* 1.4. Dans quelle mesure un point de concentration unique tel qu'un partenariat public-privé contractuel remédierait-il à ces faiblesses antérieures?

1200 caractère(s) maximum

* 1.5. Quelles autres mesures pourraient faciliter la participation des PME à ce type de programmes?

1200 caractère(s) maximum

2. * Vers quels éléments orienteriez-vous le soutien public aux mesures de recherche et d'innovation?
(Veuillez répondre en % – le total devrait être égal à 100 %.)

	% (précisez: 0-5-10-15-25-50-100)
Recherche fondamentale	
Activités d'innovation	
Utilisation des résultats de la recherche et de l'innovation aux fins de la mise sur le marché de produits et services	
Création de groupements nationaux/régionaux (ou de centres d'excellence nationaux/régionaux)	
Aide aux jeunes pousses (start-ups)	
Aide aux PME	
Marchés publics dans le domaine de l'innovation ou soutien avant commercialisation au développement et à l'innovation	
Initiatives «phares» individuelles à grande échelle	
Coordination des activités de recherche et d'innovation en Europe	
Définition d'exigences communes pour les produits et services de cybersécurité dans des domaines d'application spécifiques au niveau européen (par exemple, les transports, l'énergie,...)	
Autre (veuillez préciser)	
TOTAL (100 %)	

3. Vers quels domaines serait-il le plus efficace d'orienter en priorité les mesures de soutien européennes? (Veuillez indiquer 3 à 5 domaines que vous jugez prioritaires.)

* 3.1. Priorités de recherche selon la terminologie du programme de recherche stratégique de la plateforme SRI [1]

entre 2 et 3 choix

- [ ] Droits et capacités numériques des individus (couche individuelle)
- [ ] Civilisation numérique résiliente (couche collective)
- [ ] Infrastructures (hyperconnectées) fiables (couche infrastructurelle)
- [ ] Autre

Veuillez préciser.

800 caractère(s) maximum

* 3.2. Produits et services

entre 3 et 5 choix

- [ ] Gestion des identités et des accès
- [ ] Sécurité des données
- [ ] Sécurité des applications
- [ ] Sécurité des infrastructures (réseaux)
- [ ] Sécurité du matériel (appareils)
- [ ] Services d'audit, de planification et de conseil en matière de sécurité informatique
- [ ] Services de gestion et d'exploitation en matière de sécurité informatique
- [ ] Formation à la sécurité informatique
- [ ] Autre

Veuillez expliquer.

600 caractère(s) maximum

4. Vers quels secteurs serait-il le plus efficace d'orienter en priorité les mesures de soutien européennes? (Veuillez indiquer 3 à 5 secteurs que vous jugez prioritaires et expliquer pourquoi.)

entre 3 et 5 choix

- ☐ Infrastructures critiques en général
- ☐ Énergie
- ☐ Transports
- ☐ Santé
- ☐ Activités financières et bancaires
- ☐ Fournisseurs de services numériques
- ☐ Internet des objets
- ☐ Informatique en nuage
- ☐ Administration publique
- ☐ Autre

Veuillez expliquer votre choix.

1200 caractère(s) maximum

5. Selon vous, quelles entités méritent une attention particulière? (Veuillez expliquer pourquoi, pour chaque catégorie vous sélectionnez.)

- ☐ Universités et instituts de recherche
- ☐ PME
- ☐ Jeunes pousses (start-ups)
- ☐ Entreprises détenant une importante part de marché sur les marchés nationaux («champions nationaux»)
- ☐ Entreprises disposant d'une position forte sur les marchés mondiaux («acteurs mondiaux»)
- ☐ Autre

Veuillez expliquer:

1200 caractère(s) maximum

6. Quels sont les besoins spécifiques des PME innovantes en matière de cybersécurité pour stimuler la compétitivité? Quel type particulier de soutien public serait le plus utile à ces entreprises?

1200 caractère(s) maximum

* 7. Quelle serait votre contribution à la promotion de l'innovation et de la compétitivité du secteur de la cybersécurité en Europe?

- [ ] Soutien à l'alignement des programmes de recherche nationaux et européens
- [ ] Soutien aux PME
- [ ] Cofinancement d'activités à l'échelle nationale ou européenne
- [ ] Fourniture d'infrastructures d'expérimentation et d'essai
- [ ] Soutien par l'apport d'une expertise dans le domaine de la normalisation
- [ ] Contribution aux systèmes de certification
- [ ] Autre

Veuillez expliquer.

1200 caractère(s) maximum

VII. La plateforme SRI

La présente section constitue un volet distinct de la consultation, sans rapport avec le partenariat public-privé contractuel et les mesures d'accompagnement. Elle vise à recueillir l'avis des parties prenantes intéressées concernant la plateforme public-privé en matière de sécurité des réseaux et de l'information (SRI).

La plateforme SRI, qui était l'une des actions prévues par la stratégie de cybersécurité de l'UE, a été mise sur pied en juin 2013. Son objectif était de recenser les bonnes pratiques en matière de cybersécurité que les organisations peuvent appliquer afin d'accroître leur résilience. Ces pratiques devaient faciliter la mise en œuvre future de la directive SRI, mais sont également pertinentes pour un large éventail d'organisations qui ne sont pas visées par la directive.

La plateforme a réuni près de 600 parties prenantes représentant le monde des entreprises, la société civile, le milieu universitaire, les chercheurs et les États membres. Les travaux de la plateforme SRI ont été répartis entre trois sous-groupes chargés de la gestion des risques, de l'échange volontaire d'informations et de la coordination des incidents, ainsi que de la recherche et de l'innovation en matière de TIC sécurisées. En deux ans, les groupes de travail ont élaboré un certain nombre de produits, dont le programme de recherche stratégique, qui inspire le processus de création du partenariat public-privé contractuel en matière de cybersécurité dont il est question dans les sections précédentes de la présente consultation.

La Commission souhaite profiter de cette occasion pour inviter les parties prenantes qui ont participé aux travaux de la plateforme SRI à donner leur avis sur lesdits travaux à ce jour. Elle aimerait aussi connaître le point de vue de toutes les parties intéressées sur l'avenir de la plateforme SRI. Elle tiendra compte de ces contributions lors de l'élaboration du nouveau programme de travail de la plateforme SRI, à la suite de l'adoption de la directive SRI, prévue pour le début de l'année 2016.

1. Format de la plateforme SRI: qu'avez-vous aimé dans la structure et les méthodes de travail de la plateforme SRI et que proposeriez-vous de modifier (le cas échéant)?

1200 caractère(s) maximum

Question destinée aux parties prenantes qui ont participé aux travaux de la plateforme SRI

2. Quels sont les éventuels domaines de travail sur lesquels la plateforme SRI devrait se concentrer à la suite de l'adoption de la directive SRI?

1200 caractère(s) maximum

Question destinée à l'ensemble des parties prenantes

3. Pour quelles raisons avez-vous décidé de participer/de ne pas participer aux travaux de la plateforme SRI jusqu'à présent?

1200 caractère(s) maximum

Question destinée à l'ensemble des parties prenantes

4. Qu'est-ce qui vous motiverait à participer aux travaux de la plateforme SRI après l'adoption de la directive SRI et quelles attentes auriez-vous?

1200 caractère(s) maximum

Question destinée à l'ensemble des parties prenantes

VIII. Communication de données et d'avis

* Veuillez charger ici toutes données et informations supplémentaires pertinentes dans le cadre de la présente enquête.

2000 caractère(s) maximum

Veuillez charger votre fichier.

[1] Pour de plus amples informations, veuillez consulter le programme de recherche stratégique du groupe de travail n° 3 de la plateforme sur la sécurité des réseaux et de l'information (SRI) (en anglais):
https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/strategic-research-ag