Conseil de
l'Union européenne

Bruxelles, le 17 octobre 2022
(OR. en)

13664/22

CYBER 327
TELECOM 410
COSI 247
COPEN 354
DATAPROTECT 280
IND 413
RECH 547
HYBRID 99
JAI 1326
POLMIL 225
RELEX 1357

RÉSULTATS DES TRAVAUX

Origine:	Secrétariat général du Conseil
en date du:	17 octobre 2022
Destinataire:	délégations
Nº doc. préc.:	12930/22
Objet:	Conclusions du Conseil sur la sécurité de la chaîne d'approvisionnement des TIC - Conclusions du Conseil approuvées par le Conseil lors de sa session du 17 octobre 2022

Les délégations trouveront en annexe les conclusions du Conseil sur la chaîne d'approvisionnement des TIC, approuvées par le Conseil lors de sa session qui s'est tenue le 17 octobre 2022.

ANNEXE

Conclusions du Conseil sur la sécurité de la chaîne d'approvisionnement des TIC

LE CONSEIL DE L'UNION EUROPÉENNE,

RAPPELANT ses conclusions:

– du 20 novembre 2017 sur la communication conjointe au Parlement européen et au Conseil intitulée: "Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide",

– sur le renforcement des capacités en matière de cybersécurité dans l'UE,

– sur l'importance de la 5G pour l'économie européenne et sur la nécessité d'atténuer les risques pour la sécurité liés à la 5G,

– intitulées "Façonner l'avenir numérique de l'Europe",

– intitulées "Une relance au service de la transition vers une industrie européenne plus dynamique, résiliente et compétitive",

– sur la cybersécurité des dispositifs connectés,

– sur la stratégie de cybersécurité de l'UE pour la décennie numérique,

– sur la mise en place d'une posture cyber de l'Union européenne,

– sur le rapport spécial 03/2022 de la Cour des comptes européenne intitulé "Déploiement des réseaux 5G au sein de l'UE: des retards et des questions de sécurité encore sans réponse";

RAPPELANT les conclusions du Conseil européen sur les thèmes suivants:

– la COVID-19, le marché unique, la politique industrielle, la dimension numérique et les relations extérieures (conclusions des 1er et 2 octobre 2020),

– l'agression militaire russe contre l'Ukraine, la sécurité et la défense, l'énergie, les questions économiques, la COVID-19 et les relations extérieures (conclusions des 24 et 25 mars 2022),

– l'Ukraine, la sécurité alimentaire, la sécurité et la défense ainsi que l'énergie (conclusions des 30 et 31 mai 2022).

1. Compte tenu de l'importance croissante de la géopolitique pour la cybersécurité, SOULIGNE que l'Union européenne et ses États membres doivent aborder la cybersécurité de manière globale et stratégique. L'agression militaire de la Russie contre l'Ukraine a entraîné un bouleversement de l'environnement stratégique et de sécurité de l'Union européenne et a mis en évidence la nécessité de rendre l'Union européenne plus forte et plus capable dans le domaine de la sécurité et de la défense. Elle a montré qu'il était de la plus haute importance de prendre dûment en compte l'environnement géopolitique non seulement lorsqu'il s'agit de réagir à des actes de cybermalveillance, mais aussi pour assurer et maintenir la résilience des technologies de l'information et de la communication (TIC). Cette considération revêt une importance particulière pour les chaînes d'approvisionnement des produits et services TIC (chaînes d'approvisionnement des TIC), qui pourraient être à la fois compromises en raison de rivalités géopolitiques, comme l'a illustré l'attaque SolarWinds, et affectées par les tensions et l'instabilité géopolitiques, comme en témoigne la menace que constitue la dépendance à l'égard des fournisseurs russes de TIC, alors que la Russie mène une agression militaire contre l'Ukraine.

2. NOTE que la nature des risques associés à la chaîne d'approvisionnement des TIC, qui se compose d'un ensemble de ressources et de processus liés, associant des opérateurs économiques (au sens du règlement (UE) 2019/1020) et allant de l'obtention de matières premières à la fabrication, au traitement, à la gestion et à la livraison de produits et services TIC, en passant par la fourniture d'un soutien pendant le cycle de vie de ces produits et services, entraîne des difficultés uniques et des conséquences potentiellement considérables. Outre les risques liés à l'indisponibilité des produits TIC, par exemple en raison de pénuries de matières premières et semi-conducteurs critiques nécessaires à leur production, les chaînes d'approvisionnement des produits et services TIC sont exposées à d'autres menaces. Elles peuvent notamment être ciblées ou utilisées à mauvais escient par des acteurs malveillants usant de procédés sophistiqués, souvent dissimulés qui ont une incidence sur la confidentialité, l'intégrité et la disponibilité des données sensibles transmises et stockées.

3. Conscient qu'une approche "tous risques" est indispensable pour sécuriser les actifs TIC, MESURE l'intérêt de la proposition de directive sur la résilience des entités critiques pour améliorer la sécurité physique de ces entités, et SOULIGNE que, outre le renforcement de la résilience face aux attaques contre la chaîne d'approvisionnement menées par des moyens cybernétiques, il est tout aussi important d'accroître la résilience et la sécurité générales des chaînes d'approvisionnement des TIC face à la diversité des facteurs de menace, par exemple les catastrophes naturelles, les défaillances systémiques, les menaces internes ou les erreurs humaines. En ce sens, EST CONSCIENT que la sécurité de la chaîne d'approvisionnement des TIC nécessite aussi d'assurer la protection des produits et services TIC produits, fournis, achetés et utilisés dans les chaînes d'approvisionnement des TIC, y compris en protégeant les composants individuels et les données transmises.

4. S'appuyant sur les enseignements tirés des conséquences des dépendances stratégiques de l'Union européenne à l'égard des combustibles fossiles russes ainsi que de l'impact des perturbations des chaînes d'approvisionnement pendant la pandémie de COVID-19, notamment en ce qui concerne les produits pharmaceutiques et les semi-conducteurs, domaines dans lesquels les dépendances stratégiques de l'UE ont été mises en évidence, ENCOURAGE les États membres à s'efforcer d'éviter des situations similaires de dépendances stratégiques externes indésirables pour ce qui est des produits et services TIC. En raison de la numérisation croissante de la société et du recours toujours plus important aux TIC dans les infrastructures critiques, les dépendances stratégiques externes liées aux produits et services TIC et à leurs chaînes d'approvisionnement devraient être évaluées en permanence et, le cas échéant, combattues.

5. RAPPELLE que parvenir à l'autonomie stratégique tout en préservant une économie ouverte est un objectif majeur de l'Union, ce qui nécessite notamment de recenser et de réduire les dépendances stratégiques et d'accroître la résilience dans les écosystèmes industriels les plus sensibles et dans des domaines spécifiques, notamment le numérique. Cela suppose notamment de développer et de déployer des capacités et des infrastructures numériques stratégiques ainsi que de renforcer la capacité à faire des choix technologiques autonomes et de disposer, parmi les principaux piliers, d'infrastructures, de produits et de services résilients et sûrs pour instaurer la confiance sur le marché unique numérique et au sein de la société européenne, tout en maintenant l'ouverture, la coopération mondiale avec les partenaires partageant la même optique et la compétitivité, et en tirant parti des avantages qu'elles sont susceptibles d'offrir. Les valeurs fondamentales de l'Union européenne préservent en particulier la vie privée, la sécurité, l'égalité, la dignité humaine, l'État de droit et un internet ouvert, qui sont autant de conditions préalables à l'avènement d'une société, d'une économie et d'une industrie fondées sur le numérique et axées sur l'humain.

6. NOTE que, en raison de l'évolution du paysage des cybermenaces, dont témoigne la tendance caractérisée, ces dernières années, par des attaques sophistiquées et de grand impact contre les chaînes d'approvisionnement, telles que SolarWinds, Mimecast ou Kaseya, qui sont apparues parallèlement à l'externalisation des services TIC essentiels et ont été intensifiées par la dépendance globale à l'égard des produits et services TIC fabriqués, fournis ou assurés par des tiers, une hausse du nombre d'attaques contre les chaînes d'approvisionnement entraînant des dommages considérables pour l'économie et la société est très probable. Compte tenu de ces éléments, INSISTE sur l'importance de renforcer la sécurité et la résilience des chaînes d'approvisionnement des TIC pour assurer le fonctionnement du marché unique, ainsi que sur la nécessité de garantir la disponibilité, la sécurité et la diversité des produits et services TIC au sein du marché unique. Par conséquent, EST CONSCIENT de la nécessité de maximiser et de rationaliser l'utilisation des instruments et approches existants de l'UE pour atteindre ces objectifs, ainsi que de la nécessité de s'adapter en permanence à l'évolution du paysage des cybermenaces en introduisant des mesures et des mécanismes supplémentaires appropriés, y compris en ce qui concerne les risques éventuels pour la sécurité des technologies émergentes et de rupture. ENCOURAGE les États membres à suivre à cet égard l'approche fondée sur les risques pour faire face aux nouvelles évolutions technologiques.

7. EST CONSCIENT qu'il est essentiel de comprendre l'évolution constante du paysage des cybermenaces ainsi que la complexité des attaques contre la chaîne d'approvisionnement afin d'atténuer efficacement les risques associés aux chaînes d'approvisionnement des TIC. À cet égard, SOULIGNE qu'il est nécessaire de s'adapter aux nouvelles menaces en surveillant, en analysant et en évaluant de façon active et permanente le paysage des menaces pesant sur la chaîne d'approvisionnement, d'accroître la prise de conscience et d'acquérir des connaissances sur les menaces et les vulnérabilités, ainsi que d'alerter les entités concernées de manière proactive et personnalisée. SALUE les travaux de l'Agence de l'Union européenne pour la cybersécurité (ENISA) liés à la sécurité de la chaîne d'approvisionnement des TIC, et en particulier son rapport concernant le paysage des menaces dans le cadre des attaques de la chaîne d'approvisionnement.

INSTRUMENTS ET APPROCHES INTERSECTORIELS

8. RÉAFFIRME qu'il importe que les États membres tiennent compte de la nécessité de diversifier les fournisseurs de TIC critiques de manière à éviter de créer de fortes dépendances à l'égard de fournisseurs uniques ou à limiter ces dépendances, et en particulier à l'égard de fournisseurs à haut risque, étant donné qu'une telle situation augmente l'exposition aux conséquences de potentielles perturbations. RECONNAÎT que le fait d'éviter l'effet de verrouillage et de diversifier les fournisseurs de TIC est l'un des éléments importants permettant d'assurer la stabilité et la sécurité du marché intérieur. SOULIGNE qu'il est nécessaire de promouvoir et de mettre en œuvre des stratégies appropriées facilitant la diversification et la compétitivité des fournisseurs d'une manière technologiquement neutre. En outre, ENCOURAGE l'intégration d'aspects liés à la prévention de l'effet de verrouillage dans la législation de l'UE. À cet égard, PREND ACTE de la proposition de règlement fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données), qui vise à augmenter l'interopérabilité des services de traitement de données et à supprimer les obstacles au changement de fournisseurs de services de traitement de données.

9. EST CONSCIENT du lien entre la sécurité de la chaîne d'approvisionnement des TIC et les marchés publics. SOULIGNE qu'il est nécessaire que les procédures de passation de marchés publics tiennent suffisamment compte de l'importance que revêt la sécurité de la chaîne d'approvisionnement des TIC en imposant, s'il y a lieu, des critères de sélection objectifs et fondés sur les risques concernant la capacité des soumissionnaires à garantir un niveau élevé de sécurité des services fournis. DEMANDE qu'un juste équilibre soit trouvé entre, d'une part, l'intérêt public d'une utilisation des fonds publics qui soit la plus efficace et la plus équitable possible et, d'autre part, l'intérêt public d'une sécurisation des systèmes d'information et d'une garantie de bon fonctionnement du marché unique. Afin de faciliter la mise en œuvre des règles pertinentes en matière de marchés publics dans le contexte d'une plus grande cybersécurité, INVITE la Commission à élaborer des lignes directrices méthodologiques d'ici au troisième trimestre de 2023 dans le but d'encourager les pouvoirs adjudicateurs à mettre l'accent qui convient sur les pratiques des soumissionnaires et de leurs sous-traitants en matière de cybersécurité, et à évaluer la législation applicable en matière de marchés publics et, si nécessaire, à formuler des propositions visant à la réviser ou à la compléter.

10. EST CONSCIENT que les investissements directs étrangers liés aux produits et services TIC, tout en apportant des avantages économiques et sociaux aux États membres, aux entreprises et aux citoyens, pourraient présenter des risques pour la sécurité et l'ordre public et NOTE que le mécanisme de filtrage des investissements directs étrangers de l'UE, ainsi que les différents systèmes de filtrage nationaux, qui donnent les moyens de faire face à ces risques, pourraient également être utilisés; ils constituent un outil utile pour préserver la sécurité et la résilience de la chaîne d'approvisionnement des TIC en contribuant à l'élimination des investissements à haut risque susceptibles de porter atteinte à cette sécurité et à cette résilience. RECONNAÎT que les informations échangées et partagées via ce mécanisme peuvent aider les États membres à mieux évaluer les menaces pouvant peser sur la sécurité des chaînes d'approvisionnement des TIC et à prendre les mesures nécessaires en conséquence. INVITE les acteurs nationaux concernés à tenir également compte de cette dimension du mécanisme de filtrage, le cas échéant.

11. En ce qui concerne la défense, RÉITÈRE l'invitation qu'il a adressée à la Commission pour qu'elle évalue en 2023, en coopération avec les États membres, les risques pesant sur les chaînes d'approvisionnement des infrastructures critiques dans divers domaines, y compris le domaine numérique, liés aux intérêts de l'UE en matière de sécurité et de défense, et qu'elle étudie les possibilités de renforcement de la cybersécurité tout au long de la chaîne d'approvisionnement de la base industrielle et technologique de défense de l'UE. En outre, INVITE les États membres et la Commission à avoir une réflexion sur la sécurité de la chaîne d'approvisionnement des TIC dans le cadre de la mise en œuvre des engagements et des actions relevant de la boussole stratégique.

12. Reconnaissant l'importance des matières premières critiques ainsi que de tous les types de semi-conducteurs en tant qu'éléments de base des produits TIC, ENCOURAGE des négociations constructives sur la proposition de règlement établissant un cadre de mesures pour renforcer l'écosystème européen des semi-conducteurs (règlement sur les semi-conducteurs) et sur la proposition de règlement du Conseil modifiant le règlement (UE) 2021/2085 établissant les entreprises communes dans le cadre d'Horizon Europe, en ce qui concerne l'entreprise commune "Semi-conducteurs".

INSTRUMENTS SPÉCIFIQUES AU CYBERESPACE

13. En ce qui concerne plus particulièrement les infrastructures de télécommunications, PREND ACTE des résultats obtenus au niveau de l'Union pour améliorer la sécurité de la chaîne d'approvisionnement des réseaux 5G, en particulier grâce à la boîte à outils de l'UE pour la sécurité des réseaux 5G (boîte à outils 5G de l'UE). APPELLE les États membres à continuer d'échanger des informations sur les meilleures pratiques et méthodologies pour la mise en œuvre des mesures recommandées dans la boîte à outils 5G de l'UE et, en particulier, à appliquer les restrictions pertinentes aux fournisseurs à haut risque d'actifs essentiels, définis comme critiques et sensibles dans l'évaluation coordonnée des risques au niveau de l'UE. SOULIGNE que la boîte à outils 5G de l'UE constitue un instrument souple fondé sur les risques pour relever les défis recensés en matière de sécurité, qui permet de traiter les aspects liés à la cybersécurité de la 5G de manière rapide et efficace, tout en respectant les compétences des États membres, et RECONNAÎT qu'il s'agit d'un instrument précieux pour renforcer encore, en toute transparence, la sécurité de la chaîne d'approvisionnement des réseaux de télécommunications d'une manière coordonnée, qui pourrait servir d'inspiration pour les outils d'évaluation et d'atténuation des risques liés à d'autres secteurs vitaux. RAPPELLE que les autorités compétentes ont été invitées à formuler des recommandations, fondées sur des évaluations des risques, à l'intention des États membres et de la Commission afin de renforcer la résilience des réseaux et infrastructures de communication au sein de l'Union européenne, y compris la mise en œuvre continue de la boîte à outils 5G de l'UE.

14. RELÈVE l'importance que revêtent des approches interopérables pouvant contrer l'effet de verrouillage et diluer le risque de concentration, tout en améliorant la sécurité de la chaîne d'approvisionnement dans l'ensemble des infrastructures et des services TIC. En particulier en ce qui concerne les réseaux 5G, EST CONSCIENT des avantages potentiels du concept de RAN ouvert à cet égard et, en même temps, RAPPELLE le rapport sur la cybersécurité du RAN ouvert publié par le groupe de coopération SRI notant que ce concept est toujours en cours d'élaboration et que sa sécurité, sa transparence et sa normalisation en sont à un stade précoce de développement, et SOULIGNE qu'il importe d'évaluer les risques avant toute transition vers de nouvelles normes ou architectures.

15. INSISTE sur la pertinence des instruments législatifs horizontaux existants et à venir en matière de cybersécurité, notamment le règlement relatif à l'ENISA (l'Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications (règlement sur la cybersécurité), la future directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (SRI 2), la proposition de règlement établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union, ainsi que la proposition de règlement relatif aux exigences horizontales en matière de cybersécurité applicables aux produits comportant des éléments numériques (législation sur la cyberrésilience), pour renforcer la sécurité de la chaîne d'approvisionnement des TIC. En outre, PREND NOTE des évolutions importantes des règlements sectoriels dans le domaine de la cybersécurité, en particulier le futur règlement sur la résilience opérationnelle numérique du secteur financier (DORA), qui comprend un cadre de supervision applicable aux tiers prestataires de services informatiques qui sont essentiels pour les entités financières. Ces règlements comportent des obligations générales liées à la sécurité de la chaîne d'approvisionnement ainsi que des exigences détaillées et précises applicables au secteur concerné. Parallèlement, SOULIGNE que les fournisseurs de produits et services approvisionnent souvent différents secteurs plutôt qu'un seul. Il est par conséquent extrêmement important de veiller à ce que les exigences en matière de sécurité de la chaîne d'approvisionnement soient, dans la mesure du possible, alignées dans tous les secteurs concernés, en particulier ceux régis par la future directive SRI 2, afin d'éviter des divergences entre les obligations imposées aux fournisseurs et d'alléger la charge pesant sur les opérateurs des secteurs critiques, tenus d'évaluer le respect de ces obligations par les fournisseurs, tout en tenant compte des spécificités sectorielles.

16. SE FÉLICITE de la proposition de législation sur la cyberrésilience, qui constitue un instrument législatif important pour faire progresser le développement en toute sécurité de produits comportant des éléments numériques et pour veiller à que la cybersécurité soit prise en compte tout au long du cycle de vie des produits comportant des éléments numériques. NOTE que la proposition de législation sur la cyberrésilience est susceptible de contribuer considérablement au renforcement de la sécurité de la chaîne d'approvisionnement des TIC. ENCOURAGE des négociations constructives et l'adoption en temps utile de cette législation.

17. À cet égard, PREND ACTE des travaux en cours menés par l'ENISA, ainsi que par les États membres et d'autres parties prenantes, en vue de fournir à l'UE des schémas de certification pour les produits, services et processus TIC conformes au règlement sur la cybersécurité qui devraient contribuer à relever le niveau global de cybersécurité au sein du marché unique numérique. ENCOURAGE toutes les parties prenantes à participer aux travaux préparatoires sur les différents schémas européens de certification afin d'instaurer de la confiance à l'égard des produits, processus et services TIC sécurisés et de renforcer leur résilience et INVITE la Commission à élaborer rapidement des actes d'exécution sur les schémas européens de certification après l'achèvement des travaux préparatoires, notamment le schéma européen de certification de cybersécurité fondé sur des critères communs. NOTE que les schémas européens de certification devraient inclure, si nécessaire, des exigences en matière de sécurité de la chaîne d'approvisionnement, y compris concernant les relations avec les fournisseurs.

18. INSISTE sur la nécessité d'une mise en œuvre complète de toutes les dispositions à venir de la directive SRI 2 relatives à la sécurité de la chaîne d'approvisionnement des TIC. À cet égard, SOULIGNE la pertinence des évaluations coordonnées au niveau de l'UE des risques liés aux chaînes d'approvisionnement critiques (évaluations coordonnées des risques liés aux chaînes d'approvisionnement), des politiques nationales en matière de sécurité de la chaîne d'approvisionnement et des mesures de sécurité pour la chaîne d'approvisionnement. NOTE qu'il convient de prêter attention non seulement aux fournisseurs principaux, mais aussi aux sous-traitants concernés, en ce qui concerne les risques liés à la sécurité du fournisseur principal ou du client final. Afin de faciliter la mise en œuvre de mesures de gestion des risques pesant sur la chaîne d'approvisionnement, ENCOURAGE l'ENISA à procéder, avec l'aide du groupe de coopération SRI, à un inventaire des meilleures pratiques disponibles en matière de gestion des risques pesant sur la chaîne d'approvisionnement et à les rassembler dans des lignes directrices méthodologiques. En outre, ENCOURAGE l'ENISA à assurer un suivi des investissements dans la sécurité de la chaîne d'approvisionnement des TIC pour les entités régies par la future directive SRI 2.

19. SOULIGNE également les avantages et les risques associés au recours à des fournisseurs de services gérés et à des fournisseurs de services gérés de sécurité dans le contexte de la sécurité de la chaîne d'approvisionnement. Bien que le recours à ces fournisseurs puisse considérablement renforcer la sécurité au sein des organisations et conduire à un niveau de cybersécurité plus élevé, la gestion à distance des systèmes et services TIC ainsi que l'accès privilégié à l'environnement TIC des clients, dont pourraient avoir besoin les fournisseurs de services gérés et de services gérés de sécurité, peuvent, si ces fournisseurs sont compromis, donner lieu à des effets en cascade significatifs pour un grand nombre de clients. Par conséquent, il est de la plus haute importance que les fournisseurs de services gérés et de services gérés de sécurité maintiennent un niveau élevé de sécurité, que ce soit leur propre sécurité interne ou celle des services qu'ils fournissent, et adoptent une approche transparente à l'égard de leurs clients en ce qui concerne la sécurité des services qu'ils fournissent. À cet égard, SE FÉLICITE de leur inclusion prévue dans le champ d'application de la future directive SRI 2.

20. En ce qui concerne la mise en œuvre du mécanisme d'évaluations coordonnées des risques liés aux chaînes d'approvisionnement en vertu de la future directive SRI 2, CONSTATE la pertinence des facteurs de risque non techniques dans ce cadre, tels que l'influence injustifiée d'un État tiers sur les fournisseurs et les prestataires de services, et, dans ce contexte, EST CONSCIENT des facteurs qui peuvent être utilisés pour évaluer le profil de risque tels qu'ils sont mentionnés dans l'évaluation coordonnée pour l'UE des risques liés à la cybersécurité des réseaux 5G. INVITE la Commission à recenser, d'ici au deuxième trimestre de 2023, après consultation du groupe de coopération SRI et de l'ENISA, les services, systèmes ou produits TIC qui pourraient être soumis en priorité aux évaluations coordonnées des risques liés aux chaînes d'approvisionnement.

21. NOTE que la dépendance à l'égard des fournisseurs à haut risque de produits et services TIC utilisés pour l'exploitation de réseaux et de systèmes critiques constitue une menace stratégique qu'il convient d'atténuer au moyen de politiques appropriées au niveau national et au niveau de l'UE ainsi que par une coopération entre les États membres et avec des partenaires internationaux partageant la même optique. Afin de faciliter l'atténuation de ce risque stratégique et de soutenir les évaluations coordonnées des risques liés aux chaînes d'approvisionnement, INVITE le groupe de coopération SRI, en coopération avec la Commission et l'ENISA, à élaborer une "boîte à outils" de mesures visant à réduire les risques pour les chaînes d'approvisionnement des TIC critiques (boîte à outils pour les chaînes d'approvisionnement des TIC). Cette boîte à outils devrait s'appuyer sur les scénarios de menaces stratégiques recensés en ce qui concerne les chaînes d'approvisionnement des TIC et prévoir des mesures visant à remédier à ces scénarios en tirant parti de l'expérience acquise dans le cadre de la boîte à outils 5G et au niveau national. Elle devrait compléter, de manière transparente, les évaluations coordonnées des risques liés aux chaînes d'approvisionnement des différents services, systèmes ou produits TIC au titre de la future directive SRI 2 en proposant des mesures génériques de réduction des risques qui puissent être adaptées aux services, systèmes ou produits TIC spécifiques de façon modulable, sur la base des risques recensés dans les différentes évaluations coordonnées des risques liés aux chaînes d'approvisionnement.

22. SOULIGNE le rôle important que jouent les activités de recherche, d'innovation, d'investissement et entrepreneuriales dans le domaine du numérique et de la cybersécurité ainsi que le financement de ces activités pour ce qui est d'éviter d'éventuelles futures dépendances stratégiques indésirables et de renforcer la résilience globale des chaînes d'approvisionnement des TIC. Dans ce contexte, SOULIGNE le rôle et la pertinence des tâches stratégiques et de mise en œuvre du Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité et du réseau de centres nationaux de coordination pour ce qui est de contribuer à maximiser les effets des investissements visant à renforcer le leadership de l'Union et son autonomie stratégique ouverte dans le domaine de la cybersécurité, à soutenir les capacités et compétences technologiques de l'Union et à accroître la compétitivité de celle-ci au niveau mondial. À cet égard, APPELLE DE SES VŒUX la mise en place opérationnelle rapide du Centre de compétences. INVITE le Centre de compétences à tenir compte, dans son programme stratégique, des aspects relatifs à la sécurité des chaînes d'approvisionnement des TIC, y compris, par exemple, le développement de logiciels sécurisés, tout en veillant à la cohérence et à la complémentarité et en évitant toute duplication des efforts. SOUTIENT le renforcement de la compétitivité européenne dans le domaine de la cybersécurité au moyen de programmes de financement, tels que le programme pour la recherche et l'innovation "Horizon Europe" et le programme pour une Europe numérique visant à renforcer, développer et acquérir les capacités essentielles pour l'économie numérique, la société et la démocratie de l'UE.

MÉCANISMES DE SOUTIEN

23. ENCOURAGE l'augmentation des incitations financières liées aux mesures visant à renforcer la sécurité de la chaîne d'approvisionnement des TIC. INVITE, en priorité, également dans la perspective de la mise en œuvre prochaine de la directive SRI 2, le Centre de compétences, la Commission et les parties prenantes concernées à étudier les possibilités d'inclure les aspects relatifs à la sécurité de la chaîne d'approvisionnement des TIC dans les prochains appels dans le cadre des programmes de travail en matière de cybersécurité au titre du programme pour une Europe numérique et du programme "Horizon Europe", ou toute autre possibilité de financement pertinente. Ces possibilités de financement devraient notamment viser à permettre aux organisations de contribuer au maintien d'un niveau élevé de cybersécurité pour l'acquisition de produits et services TIC tout au long de la chaîne d'approvisionnement, en particulier en ce qui concerne le remplacement de services, systèmes ou produits TIC critiques spécifiques reconnus comme étant à haut risque conformément aux futures évaluations coordonnées des risques liés aux chaînes d'approvisionnement.

24. EST CONSCIENT que la mondialisation et la spécialisation des services TIC ainsi que la dépendance accrue à l'égard des produits et services de tiers rendent nécessaire une coopération étroite au sein de l'UE et au niveau international en matière de partage de connaissances et d'expertise entre les parties prenantes concernées et ENCOURAGE ces dernières à parvenir à une position forte et coordonnée assurant la sécurité de la chaîne d'approvisionnement des TIC de manière globale. EST CONSCIENT également de la nécessité d'étudier plus avant les approches et techniques pertinentes les plus récentes, en ce qui concerne tant une hygiène informatique de base appropriée que des solutions à long terme en vue de parvenir à des chaînes d'approvisionnement des TIC sûres et résilientes, ainsi que les moyens les plus appropriés de les promouvoir et éventuellement de les intégrer dans les politiques ou d'autres initiatives. ESTIME, à cet égard, qu'il convient d'accorder une attention particulière à l'étude des avantages et des inconvénients que présentent les solutions systématiques, telles que les principes de vérification systématique, la nomenclature des logiciels et des solutions similaires à long terme. RECOMMANDE de faire appel à cette fin au groupe de coopération SRI.

25. NOTE les avantages d'un suivi et d'un partage efficace d'informations sur les cyberincidents et les cybermenaces pour la prévention, la détection et l'atténuation des effets d'attaques sur la chaîne d'approvisionnement. INSISTE sur la nécessité de continuer d'instaurer un climat de confiance entre les États membres en vue d'un partage efficace de ces informations. RAPPELLE à cet égard la proposition de la Commission visant à aider les États membres à mettre en place et à renforcer des centres des opérations de sécurité (COS) afin de créer un réseau de COS dans l'ensemble de l'UE, pour mieux surveiller et anticiper les signes d'attaques sur les réseaux. RÉAFFIRME la nécessité d'une complémentarité et d'une coordination au sein des réseaux et mécanismes existants, et SOULIGNE en particulier, à cet égard, le rôle du réseau des centres de réponse aux incidents de sécurité informatiques (CSIRT), ainsi que la nécessité de continuer d'explorer le potentiel de ces réseaux afin de promouvoir une culture de partage d'informations efficace, sûre et fiable. RAPPELLE les efforts déployés par les États membres, avec le soutien de l'UE, pour mettre en place des CSIRT sectoriels, nationaux et régionaux et des centres nationaux ou européens d'échange et d'analyse d'informations (ISAC) dans le cadre d'un réseau efficace de partenariats en matière de cybersécurité dans l'Union.

26. En raison du caractère interconnecté et mondial que revêtent les menaces pesant sur les chaînes d'approvisionnement des TIC, SOULIGNE qu'il importe d'aborder et de renforcer la sécurité des chaînes d'approvisionnement des TIC au niveau mondial. À cette fin, RECOMMANDE de recourir à des partenariats numériques, à des dialogues sur le cyberespace et à d'autres initiatives pertinentes de l'UE, notamment, le cas échéant, à des accords de libre-échange, aux fins de la promotion d'évaluations fondées sur les risques des fournisseurs de produits TIC et des prestataires de services TIC, du recours à des fournisseurs de confiance et de l'utilisation d'un écosystème numérique sûr et innovant fondé sur des normes ouvertes, interopérables et transparentes. En outre, RAPPELLE le but des partenariats relevant de la stratégie "Global Gateway" ainsi que du Conseil du commerce et des technologies UE-États-Unis, et des activités menées au sein de ses groupes de travail, consistant à promouvoir le recours à des fournisseurs de confiance/ne présentant pas de risque élevé et à mettre au point un mécanisme de financement pour permettre des projets rendant les infrastructures et services TIC d'États tiers plus sûrs, plus résilients et plus fiables, y compris en s'abstenant de financer les achats auprès de fournisseurs non dignes de confiance/à haut risque d'une manière technologiquement neutre.

27. RÉAFFIRME sa détermination à contribuer à un cyberespace ouvert, libre, mondial, stable et sûr et à le promouvoir, ainsi qu'à adhérer aux normes, aux règles et aux principes en matière de comportement responsable des États dans le cyberespace définis dans le cadre des Nations unies. En ce qui concerne en particulier la sécurité des chaînes d'approvisionnement des TIC, RAPPELLE la norme approuvée par le groupe d'experts gouvernementaux (GGE) et le groupe de travail à composition non limitée encourageant les États à prendre des mesures raisonnables pour veiller à l'intégrité de la chaîne d'approvisionnement, y compris en élaborant des mesures de coopération objectives, afin que les utilisateurs finaux puissent avoir confiance dans la sécurité des produits TIC, et pour chercher à prévenir la prolifération d'outils et de techniques TIC malveillants et l'utilisation de fonctionnalités cachées préjudiciables, et PRÉCONISE une vaste mise en œuvre de cette norme.