Parlement européen

Développement d'un secteur des TIC indépendant et fiable dans l'Union européenne

Il est essentiel de lutter efficacement contre la cybercriminalité et de veiller à la protection de la vie privée, afin de garantir la confiance des citoyens dans un environnement numérique où les cybermenaces deviennent de plus en plus nombreuses et complexes. L'Union européenne se heurte à un certain nombre d'obstacles dans la mise en place d'un marché unique numérique fiable et cyber-résilient, à savoir: 1) un manque de fonds pour que les entreprises européennes spécialisées dans la cybersécurité puissent se développer; 2) la fragmentation du secteur européen de la cybersécurité; 3) une forte dépendance à l'égard de fournisseurs de pays tiers; 4) un décalage entre les programmes publics de recherche et développement (R & D) et les besoins du marché; 5) la fragmentation de la réglementation; et 6) l'absence d'harmonisation des exigences en matière de normalisation et de passation de marchés publics entre les États membres.

En ce qui concerne la protection de la vie privée et des données, bien que le cadre réglementaire européen régissant ces questions soit l'un des plus avancés au monde, des difficultés subsistent en vue de garantir que les citoyens européens jouissent du plus haut degré de protection de leurs données à caractère personnel. À l'échelle mondiale, les défenseurs du numérique non européens transfèrent des données à caractère personnel par l'internet vers des pays tiers soumis à une réglementation beaucoup plus laxiste en matière de protection des données.

La directive sur la sécurité des réseaux et des systèmes d'information [directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, communément appelée directive SRI], le récent train de mesures sur la cybersécurité et le nouveau cadre réglementaire sur la protection des données tentent d'apporter une solution à ces problèmes, bien que d'importantes difficultés persistent.

Dans ce contexte, l'établissement de politiques destinées à renforcer la cyber-résilience de l'Union est indispensable à la construction d'une économie et d'une société numériques fiables. Les options politiques proposées cherchent à fournir un cadre institutionnel qui permette aux organismes publics européens et nationaux d'améliorer la coopération et la coordination dans la lutte contre les cybermenaces. Elles visent également à faciliter le développement d'un secteur de la cybersécurité sain et compétitif en Europe, de façon à réduire la dépendance excessive envers les fournisseurs non européens spécialisés dans la cybersécurité. Les options politiques ciblent également les utilisateurs finaux des services numériques, qui constituent un important maillon de la chaîne de sécurité.

Les politiques sont structurées en quatre groupes: les politiques institutionnelles, les politiques commerciales, les politiques industrielles et les politiques orientées vers la demande. Les politiques institutionnelles visent à améliorer non seulement les mesures réglementaires correctrices pour combattre la cybercriminalité, mais également la coordination entre les différentes administrations publiques. Les politiques commerciales cherchent à instaurer des conditions de concurrence équitables entre les États membres, de manière à faciliter le commerce transfrontalier des produits et services de cybersécurité. Les politiques industrielles visent à établir les conditions qui permettent au secteur européen de la cybersécurité de soutenir la concurrence des fournisseurs de pays tiers. Enfin, les politiques orientées vers la demande cherchent à renforcer la participation des utilisateurs finaux [des particuliers et des entreprises, principalement des petites et moyennes entreprises (PME)] au processus de cybersécurité ainsi que leur connaissance de celui-ci.

Politiques institutionnelles

1. **Renforcer le rôle des organismes européens et nationaux dans le domaine des questions liées à la cybersécurité**

   En raison de leur nature transnationale, il est difficile de s'attaquer aux cybermenaces au niveau national. Cependant, la cybersécurité relève de la compétence des États membres, tandis que le rôle des organismes de l'Union [principalement l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA)] se limite à conseiller ces derniers et à sensibiliser les citoyens. Le règlement SRI et la proposition de règlement sur l'ENISA (COM(2017) 477) attribuent de nouvelles responsabilités à l'Agence, bien que ses compétences restent encore limitées à la fourniture de services de conseil et d'assistance. Il serait judicieux, comme le suggère la proposition de nouveau règlement relatif à l'Agence, de renforcer le rôle de l'ENISA en tant qu'agence indépendante et permanente, non subordonnée aux intérêts nationaux.

2. **Harmoniser la législation en matière de lutte contre la cybercriminalité**

   La cybercriminalité n'est pas poursuivie de façon uniforme dans l'Union, ce qui permet aux cybercriminels de bénéficier de législations plus laxistes. En outre, la nature transnationale des cyberattaques et le principe de territorialité, sur lequel repose le droit international, entravent le bon déroulement des enquêtes et poursuites pénales, ce qui favorise l'impunité des cybercriminels.

   Le réseau judiciaire européen en matière de cybercriminalité a été créé à la fin de l'année 2016 en vue de renforcer l'échange de savoir-faire et de bonnes pratiques entre les autorités judiciaires des pays de l'Union. Ce n'est pas suffisant. Une définition harmonisée de ce qui constitue un cybercrime, une description des procédures employées pour l'obtention de preuves numériques dans le cadre des poursuites pénales ainsi qu'une détermination des peines qui seront appliquées aux coupables dans les États membres pourraient certainement contribuer à améliorer la lutte contre la cybercriminalité.

Politiques commerciales

3. **Harmoniser les exigences en matière de passation de marchés publics dans le domaine des solutions de cybersécurité**

   Les marchés publics jouent un rôle clé pour stimuler le secteur de la cybersécurité. Cependant, la diversité des exigences en matière de passation de marchés publics dans le domaine des solutions de cybersécurité, principalement les systèmes de certification et les normes, appliquées par les pays de l'Union et les organismes publics au sein des pays, représente un obstacle au développement des entreprises paneuropéennes spécialisées dans la cybersécurité. Cette hétérogénéité favorise la fragmentation du marché en Europe et freine le développement des entreprises européennes.

   La création d'un ensemble commun d'exigences applicables aux organismes de l'Union et des États membres faciliterait le développement de solutions de cybersécurité européennes. La création d'un label de confiance pour les produits de cybersécurité européens renforcera davantage l'efficacité des politiques en devenant une exigence commune qui pourrait bénéficier aux fournisseurs établis en Europe.

4. **Créer des labels de confiance pour les produits de cybersécurité européens**

   La création de labels de confiance européens pour les produits de cybersécurité pourrait profiter à l'ensemble de l'écosystème. Les consommateurs pourraient facilement identifier les fournisseurs fiables lors de l'achat de solutions de cybersécurité, et les produits de cybersécurité porteurs d'un label de confiance pourraient être vendus dans toute l'Union sans que d'autres adaptations ne soient nécessaires pour satisfaire aux exigences nationales particulières. Les labels de confiance peuvent également offrir d'autres avantages commerciaux en devenant un moyen utile d'indication de la qualité et de la fiabilité des produits de cybersécurité européens.

   Le succès des labels de confiance repose sur: 1) le développement de processus de certification transparents; 2) des charges administratives qui ne soient pas excessives; et 3) l'accès de toutes les entreprises aux labels indépendamment de leur taille et de l'endroit où elles sont établies.

5. Harmoniser les procédures de normalisation et de certification des produits de cybersécurité

Actuellement, la normalisation des produits de cybersécurité est une activité en plein essor, plusieurs organisations essayant de fixer des spécifications de sécurité pour plusieurs TIC émergentes. L'Union devrait montrer la voie et harmoniser les nombreuses normes de cybersécurité déjà en place, ainsi que définir un cadre de certification cohérent au niveau européen.

La communication conjointe de la Commission européenne intitulée «Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide» peut constituer un pas dans la bonne direction en chargeant l'ENISA d'instaurer un cadre européen de certification de cybersécurité, qui spécifiera la procédure de création de systèmes de certification de cybersécurité. Bien que ces systèmes de certification seront volontaires, il s'agit d'une première étape importante.

Politiques industrielles

6. Favoriser le développement de produits de cybersécurité libres

Les produits de cybersécurité peuvent être développés comme des logiciels propriétaires ou des logiciels libres. Les premiers consistent généralement en des solutions dites de la «boîte noire», qui ne permettent pas aux utilisateurs de contrôler comment elles fonctionnent réellement. En revanche, les seconds permettent aux chercheurs d'examiner le code afin de détecter les éventuelles erreurs et vulnérabilités, et d'améliorer ainsi en permanence la fiabilité et la crédibilité des produits de cybersécurité. Ils ne garantissent toutefois pas entièrement l'impossibilité de cyberattaques et peuvent ne pas être appropriés lorsqu'un certain niveau de confidentialité est requis (détection et prévention des attaques, renseignements sur les menaces, etc.). Étant donné que le code peut être analysé et modifié par tout un chacun, il pourrait aussi être exploité par des cybercriminels pour créer de nouvelles vulnérabilités.

Les organismes de l'Union peuvent encourager le développement de produits de cybersécurité libres: 1) en appliquant des exigences de «code source ouvert» aux marchés publics portant sur le développement de solutions informatiques et de cybersécurité; 2) en collaborant, au sein de communautés de développement de logiciels libres, à la mise au point de solutions innovantes libres; 3) en clarifiant les aspects juridiques liés aux questions de propriété intellectuelle; et 4) en encourageant la recherche fondée sur des technologies libres.

Bien que les solutions libres constituent une option très intéressante, elles doivent faire l'objet d'une sélection très minutieuse de manière à éviter une concurrence directe dans les domaines techniques dans lesquels l'Union possède de solides solutions propriétaires. Si les solutions libres peuvent améliorer la cyber-résilience des produits et services des TIC, elles n'offrent pas toujours un avantage concurrentiel aux fournisseurs de l'Union.

7. Élaborer une politique industrielle de cybersécurité

Les politiques industrielles actuelles de l'Union ne tiennent pas suffisamment compte de la cybersécurité. Ni la politique industrielle européenne en matière de sécurité ni la communication de la Commission intitulée «Vers une renaissance industrielle européenne» ne mentionnent ce thème parmi les domaines stratégiques qui devraient bénéficier d'un soutien.

Il conviendrait de structurer toutes les mesures axées sur le renforcement du secteur européen de la cybersécurité dans un plan d'action global, assorti d'objectifs clairs et d'une feuille de route détaillée. La priorité devrait être accordée aux domaines dans lesquels l'Union est bien positionnée pour être un chef de file mondial (à savoir, la sécurité industrielle et la cybersécurité dans les secteurs aéronautique, ferroviaire et automobile) ainsi qu'aux domaines dans lesquels l'Union doit être autonome (à savoir, la défense et la cryptographie).

La politique industrielle devrait viser la création, dans toute l'Europe, de centres de compétence susceptibles d'allier la théorie à l'innovation, où des opinions et des idées pourraient être échangées et évoluer de manière coordonnée, aboutissant à une réussite commerciale. Pour autant qu'il soit correctement mis en place, le réseau de centres de compétence en matière de cybersécurité envisagé dans la dernière stratégie de cybersécurité de la Commission peut constituer un pas dans la bonne direction. Le plan devrait également prévoir un soutien de l'Union à la promotion des exportations de solutions et de

services de cybersécurité européens en dehors de l'Union (en particulier vers les États-Unis, l'Asie et la région EMEA[1]).

8. Soutenir la création d'instruments d'investissement axés sur le secteur de la cybersécurité

Les entreprises européennes spécialisées dans la cybersécurité bénéficient d'un soutien financier préalable à leur création (capital d'amorçage), avant de le voir pratiquement disparaître lorsqu'elles cherchent à consolider et à développer leurs activités. Ce manque de fonds entrave deux processus opérationnels cruciaux pour les entreprises: 1) les activités de marketing destinées à améliorer leur visibilité; et 2) l'adaptation de leurs produits et services pour conquérir de nouveaux marchés. Il est donc nécessaire de mettre au point et de financer des instruments financiers couvrant toutes les étapes de la vie d'une entreprise, en particulier dans un secteur à l'égard duquel les partenaires financiers traditionnels (les banques) peuvent se montrer réticents.

L'Union dispose de plusieurs instruments financiers qui pourraient être orientés vers le secteur de la cybersécurité. Par exemple, le Fonds européen pour les investissements stratégiques (EFSI), une initiative conjointe du Groupe BEI[2] et de la Commission européenne, pourrait allouer des fonds non seulement au secteur numérique en général, mais également au secteur de la cybersécurité. L'accès au financement pourrait être facilité par la création d'une plateforme d'investissement en matière de cybersécurité, qui financerait ensuite les projets de cybersécurité dans toute l'Union. Cette plateforme se chargerait non seulement de la gestion des fonds alloués par l'EFSI, mais également de la collecte et de la gestion des fonds provenant d'autres sources (à savoir, les fonds publics des organismes nationaux et les fonds privés), afin de configurer plusieurs instruments de financement conformément aux besoins des entreprises spécialisées dans la cybersécurité.

Les fonds privés devraient aussi contribuer à la croissance du secteur, mais ils requièrent toutefois un environnement stable et prévisible dans lequel investir. Les organismes européens pourraient encourager indirectement les investissements privés dans le secteur en harmonisant et en unifiant des questions cruciales, telles que la normalisation ou l'étiquetage, ainsi qu'en co-investissant dans des initiatives de financement mixtes et en exploitant la capacité d'investissement d'institutions comme la BEI.

9. Encourager les activités de recherche orientées vers le marché

Plusieurs éléments indiquent l'existence d'un décalage entre les besoins du marché et les travaux de recherche menés dans l'Union dans le domaine de la cybersécurité. La longue durée des programmes de l'Union (de trois à cinq ans entre la conception et la finalisation d'un projet) explique en partie ce problème. Le secteur européen de la cybersécurité a tendance à adopter une démarche progressive, en mettant l'accent sur le renforcement des capacités opérationnelles plutôt que sur la poursuite d'une planification stratégique à long terme. Les travaux de recherche sont actuellement motivés par l'envie de faire progresser la science plutôt que par la demande du marché. En conséquence, les résultats des recherches scientifiques de l'Union finissent par être des solutions développées par des entreprises de pays tiers. Il semble également que les fonds disponibles en Europe pour les activités de R & D ne permettent guère d'exercer une incidence significative sur le secteur.

La lutte contre le nombre croissant de cyberattaques nécessiterait une meilleure coordination entre les organismes publics chargés de définir les thèmes de recherche et les fournisseurs de solutions de cybersécurité qui connaissent par expérience les difficultés rencontrées par leurs clients. Il convient en outre d'augmenter les fonds alloués aux activités de R & D et de surveiller de près les contributions des partenaires privés prévues par le nouvel accord sur les partenariats contractuels public-privé dans le cadre du programme Horizon 2020.

10. Augmenter la main-d'œuvre dans le domaine de la cybersécurité

L'Europe manque de professionnels dans le domaine de la cybersécurité. C'est généralement le cas dans de nombreux domaines de l'économie numérique, mais ça l'est particulièrement dans les secteurs qui, comme celui de la cybersécurité, évoluent et innovent davantage.

Plusieurs mesures peuvent être prises pour résoudre ce problème: 1) analyser, en collaboration avec les établissements de recherche et les entreprises, les besoins actuels de l'éducation formelle et non formelle

[1] Europe, Moyen-Orient et Afrique.

[2] Banque européenne d'investissement

dans le domaine de la cybersécurité; 2) promouvoir, au sein des entreprises et des centres de formation, des programmes d'apprentissage tout au long de la vie pour les professionnels actuels, dans le but de les aider à établir des plans de carrière; 3) sensibiliser les étudiants aux possibilités de carrière dans le secteur de la cybersécurité et les encourager à opter pour des études dans ce domaine; 4) promouvoir les études en cybersécurité dans les universités et les instituts de formation professionnelle; 5) définir un solide programme d'études à l'échelle européenne ainsi qu'un ensemble de domaines techniques communs en mobilisant chacune des parties prenantes (le secteur industriel, les gouvernements et le secteur de la défense); 6) renforcer la coopération entre les secteurs de l'éducation, du renseignement et de la défense afin de partager les compétences générales et spécialisées importantes; et 7) dégager des fonds pour que les candidats qualifiés de l'Union puissent suivre des études en vue d'obtenir une maîtrise ou un doctorat dans les universités en Europe ou ailleurs.

Politiques orientées vers la demande

11. Sensibiliser les utilisateurs finaux (particuliers et PME) aux cybermenaces

La cybersécurité ne concerne pas uniquement les technologies, mais également les personnes. La façon dont les personnes utilisent les services numériques a une incidence sur les cyberattaques dont elles pourraient être victimes. Les utilisateurs non formés ou peu sensibilisés aux cybermenaces deviennent des maillons vulnérables dans le processus de sécurité.

La formation des jeunes dans les écoles et le lancement de campagnes de sensibilisation à la cybersécurité, ainsi que l'organisation de cyber-exercices adaptés à différents publics cibles (mineurs, adolescents, parents, formateurs, professionnels, chercheurs, cadres dirigeants, etc.) favoriseraient des échanges en ligne sûrs et sécurisés pour tous les citoyens, indépendamment de leur niveau d'instruction ou de formation.

Cette problématique touche particulièrement les particuliers et les employés des PME qui, outre leur faible connaissance des questions liées à cybersécurité, démontrent un manque général d'informations en la matière. Pour compliquer les choses, il existe de fortes différences en fonction des caractéristiques socio-démographiques des personnes, ainsi que du secteur et de la taille des entreprises. Il convient dès lors de définir différentes politiques à l'aune de ces facteurs. Pour mettre en œuvre ces politiques, la Commission européenne devrait définir leur base et débloquer les fonds nécessaires, tandis que les gouvernements nationaux et régionaux ainsi que les associations sectorielles pourraient se charger d'adapter les politiques en fonction des spécificités locales de la population en général et des employés. Cette tâche pourrait être accompagnée d'un suivi rigoureux de la part d'autres organismes européens. L'Union pourrait également diriger la mise en place d'un portail unique rassemblant tous les outils de cybersécurité européens (un «guichet unique»), qui pourrait également offrir des conseils aux utilisateurs pour sécuriser leurs systèmes, leurs réseaux et leurs données. D'autres actions de sensibilisation, telles que le «Mois européen de la cybersécurité», pourraient être renforcées grâce, par exemple, à l'augmentation de leurs budgets publicitaires, de façon à informer un plus grand nombre de citoyens.

Le présent document se fonde sur une étude STOA intitulée «Achieving a sovereign and trustworthy ICT industry in the EU» (Développement d'un secteur des TIC indépendant et fiable dans l'Union européenne) (PE 614.531), publiée en décembre 2017. L'étude a été réalisée par Iclaves SL (Espagne), à la demande du groupe d'évaluation des choix scientifiques et techniques (STOA), et supervisée par l'unité de la prospective scientifique de la direction générale des services de recherche parlementaire du Parlement européen.

Auteurs: Rafael Rivera, Juan Pablo Villar, Carlota Tarín, Arturo Ribagorda, Juan Manuel Estévez, José María De Fuentes et Lorena González. Administrateur responsable STOA: Zsolt G. Pataki. L'étude peut être consultée sur le site web suivant: http://www.europarl.europa.eu/stoa/.