COMMISSION
EUROPÉENNE

Bruxelles, le 5.7.2016
COM(2016) 410 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS

Renforcer le système européen de cyber-résilience et promouvoir la compétitivité et l'innovation dans le secteur européen de la cybersécurité

1. INTRODUCTION/CONTEXTE

Chaque jour, des incidents liés à la cybersécurité causent d'importants dommages économiques aux entreprises européennes et à l'économie au sens large. De tels incidents ébranlent la confiance des citoyens et des entreprises dans la société numérique. Vol de secrets commerciaux, de données commerciales et de données à caractère personnel, interruption de services, y compris de ceux qui sont essentiels, et interruption d'infrastructures se traduisent par des pertes économiques de l'ordre de centaines de milliards d'euros par an[1]. Ils peuvent également avoir des répercussions sur les droits fondamentaux des citoyens et sur la société dans son ensemble.

La stratégie de cybersécurité de l'Union européenne pour 2013[2] (ci-après «stratégie de cybersécurité de l'UE») et sa composante principale, la directive sur la sécurité des réseaux et de l'information (SRI)[3] qui doit être adoptée prochainement, forment, avec la directive 2013/40/UE relative aux attaques visant les systèmes d'information, le noyau dur des mesures prises à ce jour par l'Union européenne pour répondre à ces défis en matière de cybersécurité. L'UE a également à sa disposition des entités spécialisées telles que l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), le Centre européen de lutte contre la cybercriminalité (EC3) au sein d'Europol et l'équipe d'intervention en cas d'urgence informatique de l'UE (CERT-UE). Récemment, plusieurs initiatives sectorielles ont également été lancées (par exemple, dans le domaine de l'énergie et des transports) afin de renforcer la cybersécurité dans différents secteurs cruciaux.

En dépit de ces résultats positifs, l'UE reste vulnérable en cas de cyberincident, ce qui pourrait nuire au marché unique numérique et à la vie économique et sociale dans son ensemble. Des cyberincidents peuvent aussi avoir des répercussions au-delà du secteur économique. En cas de menaces hybrides[4], les cyberattaques peuvent être utilisées en coordination avec d'autres activités pour déstabiliser un pays ou contester les institutions politiques.

Dans ce contexte, gérer des cyberincidents de grande ampleur impliquant plusieurs États membres simultanément pourrait s'avérer difficile pour l'UE. En s'appuyant sur les communications concernant la lutte contre les menaces hybrides, d'une part, et la mise en œuvre du programme européen en matière de sécurité[5], d'autre part, la Commission étudie les moyens de faire face à l'évolution de la situation en matière de cybersécurité et de déterminer quelles mesures supplémentaires peuvent être nécessaires pour améliorer la résilience et la réponse de l'UE en cas d'incident dans ce domaine.

La Commission s'intéresse en outre aux capacités sectorielles en matière de cybersécurité dans l'UE. Même si l'on ne maîtrise pas l'ensemble de la chaîne de valeur des technologies numériques en Europe, il faut au moins préserver et développer certaines capacités

[1] *Net Losses: Estimating the Global Cost of Cybercrime - Economic impact of cybercrime II; Center for Strategic and International Studies; June 2014.*
[2] JOIN(2013) 1 final.
[3] COM(2013) 48 final
[4] JOIN(2016) 18 final.
[5] COM(2016) 230 final

indispensables. La fourniture de produits et de services apportant le plus haut niveau de cybersécurité est une opportunité majeure pour le secteur de la cybersécurité en Europe et pourrait constituer un avantage concurrentiel important; Le marché mondial de la cybersécurité devrait figurer parmi les segments à croissance très rapide du secteur des TIC[6]. Pour faire de l'UE un acteur de premier plan dans ce domaine, il faut s'appuyer sur une solide culture de la sécurité des données, y compris les données à caractère personnel, et une réaction efficace aux incidents. Cela sera perçu comme un argument fort pour investir dans l'UE, et contribuera dès lors à la réalisation des objectifs ambitieux du marché unique numérique en matière de création de croissance et d'emplois.

Un engagement ferme est nécessaire pour réaliser les objectifs mentionnés ci-dessus, notamment:

i) en intensifiant la coopération en vue d'améliorer la préparation aux cyberincidents et leur gestion

Les mécanismes de coopération existants et convenus doivent être renforcés pour accroître la résilience et la préparation de l'UE, notamment face à une éventuelle crise paneuropéenne en matière de cybersécurité. Ces mécanismes de coopération doivent être complets, c'est-à-dire couvrir le cycle de vie d'un incident, de la prévention jusqu'aux poursuites. Une coopération efficace entre les États membres et la mise en œuvre pratique des exigences de sécurité pour les exploitants les plus importants requerront également des solutions techniques robustes de la part du secteur de la cybersécurité.

Garantir, dans le même temps, la résilience des cyberinfrastructures critiques dans l'ensemble de l'UE exigera des efforts soutenus pour trouver des synergies intersectorielles et intégrer les exigences en matière de cybersécurité dans toutes les politiques pertinentes de l'UE. La Commission réfléchira à la nécessité d'une mise à jour prochaine de la stratégie de cybersécurité de l'UE de 2013;

ii) en résolvant les problèmes majeurs auxquels est confronté le marché unique européen de la cybersécurité

La stratégie pour un marché unique numérique[7] reconnaît qu'il subsiste des failles spécifiques dans le secteur en rapide mutation des technologies et des solutions pour la sécurité des réseaux en ligne. Des études de marché montrent, parallèlement, que le marché intérieur de l'UE reste fragmenté sur le plan géographique en ce qui concerne l'offre de produits et de services dans le domaine de la cybersécurité[8]. La présente communication définit un certain nombre de mesures axées sur le marché pour résoudre ces problèmes et pallier les défaillances du marché unique;

iii) en favorisant la création de capacités industrielles dans le domaine de la cybersécurité

Dans la stratégie de cybersécurité de l'UE et dans la stratégie pour le marché unique numérique, la Commission s'est engagée à favoriser une augmentation de l'offre de produits

[6] Voir SWD(2016) 216
[7] COM(2015) 192 final
[8] Voir SWD(2016) 216

et de services par le secteur de la cybersécurité de l'UE. Par conséquent, la Commission va également adopter une décision ouvrant la voie à un accord contractuel concernant un partenariat public-privé (PPP) sur la cybersécurité avec comme objectif de promouvoir un programme européen de recherche et d'innovation de pointe sur la cybersécurité en vue d'accroître la compétitivité.

2. AMENER LA COOPERATION, LES CONNAISSANCES ET LES CAPACITES AU NIVEAU SUPERIEUR

La stratégie de cybersécurité de l'UE et, en particulier, la prochaine directive SRI[9], ouvriront la voie à l'amélioration de la coopération entre les États membres au niveau de l'UE. La mise en œuvre rapide et efficace de la directive sera essentielle compte tenu de l'importance croissante du numérique dans la vie économique et sociale (compte tenu également de l'informatique en nuage, de l'internet des objets et de la communication de machine à machine), de l'interconnexion transfrontalière accrue et de l'évolution rapide des menaces sur les systèmes informatiques[10]. Dans ce contexte, l'UE doit se préparer à l'éventualité d'une crise de grande ampleur dans le domaine de la cybersécurité[11], y compris, par exemple, des attaques simultanées majeures sur des systèmes d'information critiques dans plusieurs États membres[12].

La coopération au niveau de l'UE est dès lors indispensable pour gérer des cyberincidents à plus petite échelle mais susceptibles de se multiplier, ainsi qu'une éventuelle cyberattaque à grande échelle dans plusieurs États membres. L'UE doit intégrer la dimension cybernétique dans les mécanismes actuels de gestion des crises. Elle doit aussi faire en sorte que les secteurs et les États membres coopèrent efficacement et disposent de mécanismes rapides d'échange d'informations afin de répondre à de tels incidents et de les contenir. Ces mécanismes devraient de surcroît fonctionner comme un système cohérent, contribuant ainsi à la lutte contre le terrorisme, le crime organisé et la cybercriminalité. Cela permettrait aussi de renforcer la capacité de l'UE à coordonner son action avec ses partenaires internationaux pour répondre efficacement aux menaces et incidents à l'échelle mondiale.

2.1. Tirer le meilleur parti des mécanismes de coopération en matière de SRI et s'orienter vers l'ENISA 2.0

Les équipes de réaction aux incidents touchant la sécurité informatique (CSIRT) chargées de réagir rapidement en cas de cybermenaces et de cyberincidents sont une composante essentielle des capacités nationales que requiert la directive SRI. Elles formeront le réseau des CSIRT dans le but de promouvoir une véritable coopération opérationnelle en matière d'incidents spécifiques liés à la cybersécurité et de partager des informations sur les risques. La directive créera en outre un groupe de coopération dont le rôle sera de soutenir et de

[9] La directive SRI exigera des États membres qu'ils recensent un certain nombre d'exploitants de services essentiels dans des domaines tels que l'énergie, les transports, la finance et la santé, qu'ils gèrent les risques en matière de cybersécurité, et qu'ils s'assurent aussi que certains prestataires de services numériques prennent les mesures qui s'imposent pour faire face à de tels risques.
[10] Voir SWD(2016) 216.
[11] Voir, par exemple, le rapport de l'ENISA: Common practices of EU-level crisis management and applicability to cyber crises (April 2016).
[12] Voir SWD(2016) 216.

faciliter la coopération stratégique entre les États membres et d'instaurer des relations de confiance entre eux.

Étant donné la nature et la multitude des cybermenaces, la Commission encourage les États membres à tirer le meilleur parti possible des mécanismes de coopération prévus par la directive SRI et à renforcer la coopération transfrontalière en matière de préparation à un cyberincident de grande ampleur. Cette coopération plus poussée en vue d'un cyberincident majeur bénéficierait d'une approche coordonnée de la coopération en cas de crise entre les différents éléments du cyberécosystème. Une telle approche peut être définie dans un «plan d'action», qui devrait également garantir des synergies et une cohérence avec les mécanismes existants de gestion des crises[13]. Ce plan d'action devrait ensuite être régulièrement éprouvé dans le cadre d'exercices de gestion de crises dans le domaine de la cybersécurité et autres. Il préciserait le rôle des organismes européens tels que l'ENISA, la CERT-EU et le Centre européen de lutte contre la cybercriminalité (EC3, au sein d'Europol), ainsi que l'utilisation d'outils développés dans le cadre du réseau des CSIRT. Au premier semestre 2017, la Commission présentera ce plan de coopération pour examen au groupe de coopération, au réseau des CSIRT et aux autres parties intéressées.

Actuellement, les connaissances et l'expertise en matière de cybersécurité existent au niveau de l'Union, mais d'une manière dispersée et non structurée. Pour soutenir les mécanismes de coopération prévus par la directive SRI, les informations devraient être regroupées au sein d'un «pôle d'information» de façon que tous les États membres puissent y accéder rapidement sur demande. Ce «pôle» deviendrait un point central permettant aux institutions de l'UE et aux États membres d'échanger au besoin des informations. Faciliter l'accès à une information mieux structurée sur les risques en matière de cybersécurité et les solutions possibles devrait aider les États membres à accroître leurs capacités et à coordonner leurs pratiques, renforçant ainsi la résilience générale face aux attaques. La Commission, avec le soutien de l'ENISA et de la CERT-EU, ainsi que l'expertise de son Centre commun de recherche, facilitera la création et assurera la viabilité de ce pôle.

En outre, un groupe consultatif régulier de haut niveau sur la cybersécurité[14] – composé d'experts et de décideurs du secteur privé, du monde universitaire, de la société civile et d'autres organisations concernées – devrait être mis en place au niveau de l'UE. Son rôle sera d'offrir à la Commission une expertise et des contributions externes, de manière ouverte et transparente, à l'appui de ses stratégies en matière de cybersécurité et sur d'éventuelles mesures réglementaires ou d'autres mesures de politique publique. Il compléterait et ferait le lien avec d'autres structures en matière de cybersécurité.[15]

La Commission est en outre tenue de procéder à une évaluation de l'ENISA au plus tard le 20 juin 2018 et toute modification ou tout renouvellement de son mandat doit être adopté au

[13] Notamment le dispositif intégré de l'UE pour une réaction au niveau politique dans les situations de crise (IPCR), y compris la décision concernant les modalités de mise en œuvre par l'Union de la clause de solidarité (24 juillet 2014) et les procédures décisionnelles de la politique de sécurité et de défense commune.

[14] Des règles horizontales établies dans la décision C(2016) 3301 de la Commission s'appliquent aux groupes d'experts de la Commission.

[15] Par exemple, la plateforme SRI, le PPPc sur la cybersécurité et les plateformes sectorielles telles que la plateforme EECSP (Energy Expert Cyber Security Platform). Il devrait également faire le lien avec la table ronde de haut niveau annoncée dans la communication sur le passage au numérique des entreprises européennes: COM(2016) 180 final.

plus tard le 19 juin 2020[16]. Compte tenu du paysage actuel en matière de cybersécurité, la Commission entend avancer l'évaluation et, en fonction de ses conclusions, présenter une proposition dès que possible

Lorsqu'elle étudiera la nécessité d'une modification éventuelle du mandat de l'ENISA, la Commission prendra en compte les problèmes en matière de cybersécurité décrits ci-dessus et l'effort global visant à intensifier la coopération et le partage des connaissances. Ce processus sera l'occasion d'examiner la possibilité de renforcer les compétences et les moyens de l'Agence pour aider de manière durable les États membres à atteindre la résilience en matière de cybersécurité. La réflexion sur le mandat de l'ENISA tiendrait également compte des nouvelles responsabilités dévolues à l'Agence en vertu de la directive SRI, des nouveaux objectifs stratégiques de soutien à l'industrie de la cybersécurité (la stratégie pour le marché unique numérique et, en particulier, le PPP contractuel), de l'évolution des besoins dans la sécurisation des secteurs critiques et des nouveaux défis liés à des incidents transfrontières, y compris une réponse coordonnée aux cybercrises.

La Commission entend:

- présenter pour examen un plan de coopération pour la gestion des cyberincidents de grande ampleur au niveau de l'UE au cours du premier semestre de 2017;
- faciliter la création d'un «pôle d'information», afin de favoriser l'échange d'informations entre les organes de l'UE et les États membres;
- créer un groupe consultatif de haut niveau sur la cybersécurité; et
- finaliser l'évaluation de l'ENISA d'ici la fin de 2017. Cette évaluation portera sur la nécessité de modifier ou de prolonger le mandat de l'ENISA en vue de présenter une éventuelle proposition dès que possible.

2.2 Intensifier les efforts dans les domaines de l'enseignement, de la formation et des exercices en matière de cybersécurité

Les compétences et la formation adéquates, en ce qui concerne à la fois la prévention des cyberincidents ainsi que leur gestion et l'atténuation de leurs impacts, font partie des aspects fondamentaux pour parvenir à la résilience en matière de cybersécurité.

À l'heure actuelle, l'ENISA, le groupe européen de formation et d'enseignement sur la cybercriminalité («European Cybercrime Training and Education Group», ECTEG), en coopération avec le Centre européen de lutte contre la cybercriminalité à Europol et le Collège européen de police (CEPOL) jouent tous un rôle important en apportant un soutien en matière de renforcement des capacités — y compris en cybercriminalistique — par l'élaboration de manuels et l'organisation de formations et d'exercices de cybersécurité.

Par ailleurs, le cyberespace est un domaine en évolution rapide dans lequel les capacités à double usage jouent un rôle essentiel. Il est nécessaire, par conséquent, de développer la

[16] Règlement (UE) n° 526/2013 abrogeant le règlement (CE) n° 460/2004.

coopération et les synergies entre civils et militaires dans le domaine de la formation et des exercices pour accroître la résilience de l'UE et sa capacité à réagir aux incidents.

Pour répondre à ce besoin, et dans le prolongement de l'adoption de la directive SRI et du cadre stratégique de cyberdéfense de l'UE[17], les services de la Commission coopéreront avec les États membres, le service européen pour l'action extérieure (SEAE), l'ENISA et d'autres organes compétents de l'UE[18] pour mettre en place un enseignement, des exercices et une plateforme de formation en matière de cybersécurité qui favoriseront les synergies entre la formation dispensée par le secteur civil et celle du secteur de la défense.

La Commission entend:

- travailler en étroite coopération avec les États membres, l'ENISA, le SEAE et les autres organes compétents de l'UE en vue de la mise en place d'une plateforme de formation en matière de cybersécurité.

2.3. Traiter les interdépendances intersectorielles et la résilience des infrastructures de réseau publiques essentielles

Le degré d'interdépendances transnationales et intersectorielles est un facteur important dans l'évaluation du risque et de l'impact d'un cyberincident de grande ampleur. Un cyberincident grave dans un secteur ou dans un État membre peut avoir des répercussions directes ou indirectes sur ou se propager à d'autres secteurs ou à d'autres États membres.

La coopération transfrontalière et intersectorielle facilite l'échange d'informations et d'expertise et améliore donc la préparation et la résilience. La Commission soutient les travaux entrepris dans différents secteurs pour mieux comprendre les interdépendances dans le cadre de la mise en œuvre du programme européen de protection des infrastructures critiques[19].

La capacité de chaque secteur à détecter les cyberincidents, à s'y préparer et à y réagir est, par ailleurs, une condition préalable et nécessaire pour faire face aux risques intersectoriels, La Commission évaluera le risque résultant de cyberincidents dans des secteurs hautement interdépendants à l'intérieur et au-delà des frontières nationales, en particulier dans les secteurs couverts par la directive SRI, compte tenu également des évolutions sur le plan international[20]. Une fois cette évaluation effectuée, la Commission déterminera s'il est nécessaire d'établir des dispositions spécifiques et/ou des lignes directrices supplémentaires concernant la préparation aux cyber-risques pour ces secteurs cruciaux.

Au niveau européen, des centres sectoriels d'échange et d'analyse d'informations[21] (ISAC) et les CSIRT correspondants peuvent jouer un rôle clé dans la préparation et la réaction aux cyberincidents. Afin de garantir une bonne circulation des informations sur l'évolution des

[17] Adopté par le Conseil «Affaires étrangères» de l'Union européenne du 18 novembre 2014 (doc. 15585/14).
[18] Tels que le Collège européen de sécurité et de défense, EC3, CEPOL et l'Agence européenne de défense (AED)
[19] SWD(2013) 318
[20] Par exemple, une feuille de route pour la cybersécurité adoptée par l'Agence européenne de la sécurité aérienne, et les travaux de l'Organisation de l'aviation civile internationale et de l'Organisation maritime internationale
[21] Voir, par exemple, «European Energy ISAC» (http://www.ee-isac.eu).

menaces et de faciliter la réaction aux cyberincidents, les centres ISAC devraient être encouragés à dialoguer avec le réseau des CSIRT mis en place en vertu de la directive SRI, ainsi qu'avec le Centre européen de lutte contre la cybercriminalité à Europol, la CERT-EU et les organismes répressifs compétents.

L'échange d'informations entre les parties prenantes ainsi qu'avec les autorités pendant tout le cycle de vie des cyber-risques suppose que les participants sont assurés que leur responsabilité ne sera pas engagée du fait de ces échanges. La Commission a constaté plusieurs préoccupations de ce type, qui empêchent les entreprises de partager des renseignements précieux sur des menaces avec leurs pairs, entre secteurs ou avec les autorités, notamment d'un pays à l'autre. La Commission s'efforcera de répondre à ces craintes et de les apaiser en vue d'améliorer l'échange d'informations sur les cybermenaces.

L'existence de canaux de communication sûrs, garantissant la confidentialité, est également primordiale pour encourager les entreprises à rendre compte du vol électronique de secrets d'affaires. Ceci permettrait de contrôler et d'évaluer le préjudice subi par l'industrie européenne (qui se traduit aussi par des pertes en termes de ventes et d'emplois) et les organismes de recherche, et serait utile pour élaborer une réponse politique appropriée. Avec le soutien de l'ENISA, de l'Office de la propriété intellectuelle de l'Union européenne (EUIPO) et d'EC3, la Commission, en concertation avec les intervenants du secteur privé, mettra en place des canaux sécurisés pour la déclaration volontaire de vol électronique de secrets d'affaires. De tels canaux devraient permettre la compilation de données anonymisées et agrégées au niveau de l'UE, qui pourront alors être partagées avec les États membres pour soutenir les efforts diplomatiques et les actions de sensibilisation et contribuer ainsi à la protection contre le cyberespionnage des actifs incorporels dans l'Union européenne.

Pour soutenir la cybersécurité au niveau sectoriel, la Commission encouragera également l'intégration de la cybersécurité dans l'élaboration de diverses politiques sectorielles de l'UE présentant des enjeux en termes de cybersécurité.

Dernier point, mais non le moindre, les pouvoirs publics ont un rôle à jouer dans la vérification de l'intégrité des infrastructures clés de l'internet afin de déceler tout problème, d'informer la partie responsable de ces réseaux et — si nécessaire — de fournir une aide pour remédier aux vulnérabilités connues. Les autorités réglementaires nationales pourraient utiliser les capacités des CSIRT pour soumettre régulièrement les infrastructures de réseaux publics à un examen attentif et, sur cette base, encourager les exploitants à remédier aux défaillances ou vulnérabilités détectées par ces examens.

La Commission étudiera dès lors les conditions juridiques et organisationnelles requises pour permettre aux autorités réglementaires nationales, en coopération avec les autorités nationales compétentes en matière de cybersécurité, de demander aux CSIRT de procéder régulièrement à des contrôles de vulnérabilité des infrastructures de réseau publiques. Les CSIRT nationaux devraient être encouragés à coopérer, dans le cadre du réseau des CSIRT, sur les meilleures pratiques en matière de surveillance des réseaux, ce qui favorisera la prévention d'accidents à grande échelle.

La Commission entend:

- favoriser la mise en place d'une coopération européenne des centres ISAC, soutenir leur collaboration avec les CSIRT et faire en sorte de supprimer les obstacles qui empêchent les acteurs du marché de partager leurs informations;
- étudier les risques stratégiques/systémiques résultant de cyberincidents dans des secteurs très interdépendants à l'intérieur et au-delà des frontières nationales;
- apprécier la nécessité de règles et/ou de lignes directrices supplémentaires concernant la préparation aux cyber-risques destinées aux secteurs critiques et, le cas échéant, réfléchir à leur définition;
- mettre en place, avec l'ENISA, l'EUIPO et l'EC3, des canaux sécurisés pour la déclaration volontaire de vol électronique de secrets d'affaires;
- promouvoir l'intégration de mesures de cybersécurité dans les politiques européennes sectorielles; et
- examiner les conditions requises pour que les autorités nationales puissent demander aux CSIRT de procéder à des contrôles réguliers des infrastructures de réseau essentielles.

3. RESOUDRE LES PROBLEMES MAJEURS AUXQUELS EST CONFRONTE LE MARCHE UNIQUE EUROPEEN DE LA CYBERSECURITE

L'Europe a besoin de produits et de solutions de très bonne qualité, abordables et interopérables en matière de cybersécurité. Cependant, la fourniture de produits et services de sécurité de TIC au sein du marché unique reste très fragmentée sur le plan géographique. Il en résulte, d'une part, qu'il est difficile pour les entreprises européennes d'être concurrentielles au niveau national, européen et mondial, et d'autre part, que le choix des technologies viables et utilisables en matière de cybersécurité qui s'offre aux citoyens et aux entreprises est restreint[22].

En effet, le secteur de la cybersécurité en Europe s'est développé principalement en fonction de la demande des gouvernements nationaux, notamment dans le domaine de la défense. La plupart des entreprises du secteur de la défense en Europe ont mis sur pied des départements consacrés à la cybersécurité[23]. En parallèle, une multitude de PME innovantes a également vu le jour, tant sur des marchés de niche/spécialisés (par exemple, systèmes de cryptage) que sur des marchés bien établis, avec de nouveaux modèles d'entreprise (par ex. antivirus).

Toutefois, les entreprises éprouvent des difficultés à se développer en dehors de leur marché national. Le manque de confiance dans les solutions «transfrontalières» est l'élément crucial qui ressort nettement dans toutes les consultations menées par la Commission[24]. En conséquence, une grande partie des marchés publics sont toujours attribués à l'intérieur d'un État membre donné et de nombreuses entreprises ont des difficultés à réaliser les économies d'échelle qui leur permettraient d'être plus compétitives, tant sur le marché intérieur que mondial.

[22] Voir SWD(2016) 216.
[23] Voir SWD(2016) 216.
[24] Voir SWD(2016) 215.

Le manque de solutions interopérables (normes techniques), de pratiques (normes de processus) et de dispositifs de certification à l'échelle de l'UE sont parmi les lacunes affectant le marché unique dans le domaine de la cybersécurité. Cela étant, la cybersécurité a été désignée comme l'une des priorités en matière de normalisation en matière de TIC dans le marché unique[25].

Les perspectives de croissance limitées des entreprises dans le domaine de la cybersécurité dans le marché unique entraînent un grand nombre de fusions et d'acquisitions par des investisseurs non européens[26]. Si cette tendance témoigne de la capacité d'innovation des entrepreneurs européens en matière de cybersécurité, elle risque également d'entraîner une perte de savoir-faire et d'expertise européens, ainsi qu'une fuite des cerveaux.

Il est urgent d'agir pour favoriser une intégration plus poussée du marché unique en ce qui concerne les produits et les services dans le domaine de la cybersécurité, et faciliter ainsi le déploiement de solutions plus pratiques et abordables.

Il peut être remédié au manque de confiance parmi les acteurs industriels et institutionnels en encourageant la coopération à un stade précoce du cycle de vie de l'innovation: au sein du secteur de la cybersécurité lui-même, entre fournisseurs et acheteurs; et entre différents secteurs faisant intervenir des entreprises qui sont déjà clientes de solutions de cybersécurité ou sont susceptibles de le devenir.

Dans le même temps, la mise au point de produits, de services et de technologies à double usage prend une importance croissante en Europe. Le marché civil apporte un nombre croissant de solutions au marché de la défense[27]. Dans le futur plan d'action européen de la défense, la Commission entend recenser les mesures visant à stimuler davantage les synergies civilo-militaires au niveau européen.

3.1 Certification et étiquetage

La certification est importante pour accroître la sécurité des produits et services et renforcer la confiance qui leur est accordée. Cela vaut également pour les nouveaux systèmes qui utilisent abondamment les technologies numériques et nécessitent un niveau de sécurité élevé, tels que les voitures connectées et automatisées, la santé électronique, les systèmes de contrôle-commande industriels (IACS) ou les réseaux intelligents.

On voit apparaître des initiatives nationales visant à fixer des exigences élevées en matière de cybersécurité applicables aux composants TIC des infrastructures traditionnelles, et notamment des exigences de certification. Aussi importantes soient-elles, elles risquent de morceler le marché unique et de créer des problèmes d'interopérabilité. Seul un petit nombre d'États membres est doté de systèmes de certification efficaces en matière de sécurité des produits TIC[28]. Un fournisseur de TIC pourrait donc être obligé de se soumettre à plusieurs

[25] COM(2016) 2 final
[26] Voir SWD(2016) 216.
[27] En 2013, le secteur des exportations des biens à double usages représentait déjà presque 20 % du total des exportations de l'UE (en valeur). Ce chiffre couvre le commerce intra-EU.
[28] Voir le SWD (2016)216 pour l'accord sur le comité de hauts fonctionnaires chargé de conseiller la Commission sur les actions à mener dans le domaine de la sécurité des systèmes d'information [décision du Conseil du 31 mars 1992 (92/242/CEE)] et d'autres systèmes existants, tels que le *Commercial Product Assurance* au Royaume-Uni ou la Certification de sécurité de premier niveau en France.

processus de certification pour pouvoir vendre dans plusieurs États membres. Dans le pire des cas, un produit ou service TIC conçu pour répondre aux exigences de cybersécurité dans un État membre donné pourrait ne pas pouvoir être mis sur le marché dans un autre.

Pour mettre en place un marché unique opérationnel de la cybersécurité, un éventuel cadre pour la certification en matière de sécurité des produits et services TIC devrait avoir les ambitions suivantes: i) couvrir une large gamme de systèmes, produits et services TIC; ii) être applicable à l'ensemble des 28 États membres; et iii) concerner tous les niveaux de cybersécurité; tout en tenant compte des évolutions au niveau international.

À cette fin, la Commission va créer un groupe de travail spécifique sur la certification en matière de sécurité des produits et services TIC, composé d'experts des États membres et des entreprises. Il sera chargé de mettre au point avant la fin 2016, en coopération avec l'ENISA et le Centre commun de recherche, une feuille de route étudiant les possibilités d'élaborer, d'ici à la fin de 2017, un projet de cadre européen pour la certification en matière de sécurité dans le domaine des TIC. À cet égard, la Commission tiendra également compte du règlement (CE) n° 765/2008 et des dispositions en matière de certification figurant dans le règlement 2016/679 (règlement général sur la protection des données)[29].

Le processus comprendra une vaste consultation et une analyse d'impact qui permettront à la Commission d'étudier différentes options en vue de la création d'un cadre pour la certification en matière de sécurité des produits et services TIC. La Commission examinera aussi la certification en matière de sécurité dans le domaine des TIC pour le secteur des infrastructures (par exemple dans l'aviation, les chemins de fer ou l'automobile) et les mécanismes spécifiques de validation et de certification prêts à être déployés (la cybersécurité des systèmes de contrôle-commande industriels[30], l'internet des objets, le nuage). Elle remédiera aux lacunes constatées dans le système européen en matière de sécurité dans le domaine des TIC précité.

Les travaux de certification se fonderont, dans la mesure du possible, sur des normes internationalement reconnues et à mettre au point avec des partenaires internationaux.

La Commission se penchera également sur les moyens d'intégrer au mieux la certification en matière de sécurité des TIC dans la future législation sectorielle, qui concernera aussi la sûreté.

Outre les possibilités réglementaires envisageables, la Commission étudiera aussi l'éventuelle création, pour l'étiquetage en matière de sécurité des produits TIC, d'un système européen volontaire, axé sur le circuit commercial et ne représentant pas une charge trop lourde. Utilisé en complément de la certification, il améliorera la visibilité de la cybersécurité dans les produits commerciaux de manière à accroître leur compétitivité, sur le marché unique et sur le

[29] Le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données prévoit à la fois des codes de conduite destinés à contribuer à l'application correcte des règles relatives à la protection de données et des mécanismes de certification couvrant tous les principes de la protection des données, et plus particulièrement la sécurité des données dans le cadre du traitement des données à caractère personnel.

[30] Voir le groupe thématique de l'ERNCIP sur la cybersécurité des systèmes de commande industriels, disponible à l'adresse suivante https://erncip-project.jrc.ec.europa.eu/download-area/category/16-case-studies-for-industrial-automation-and-control-systems.

marché mondial. Il sera dûment tenu compte des initiatives sectorielles et horizontales actuelles lancées par les entreprises, du côté de l'offre comme du côté de la demande.

Les administrations publiques seront étroitement associées à la démarche pour qu'il soit possible d'utiliser des spécifications communes et de faire référence à la certification dans les marchés publics. La Commission suivra aussi l'utilisation des exigences pertinentes en matière de certification dans les marchés publics, au niveau national, notamment pour les systèmes relevant de secteurs particuliers (énergie, transports, santé, administration publique, etc.) et présentera un rapport à ce sujet.

La Commission entend:

- mettre au point, avant la fin 2016, une feuille de route en vue de proposer, d'ici à la fin de 2017, un cadre européen pour la certification en matière de sécurité dans le domaine des TIC et évaluer la faisabilité et l'incidence d'un cadre européen en matière d'étiquetage relatif à la cybersécurité ne représentant pas une trop lourde charge;
- étudier la nécessité d'une éventuelle certification en matière de sécurité dans le domaine des TIC dans les mécanismes sectoriels de validation/certification existants et, le cas échéant, remédier aux lacunes de ces derniers.
- intégrer, s'il y a lieu, la certification en matière de sécurité des produits TIC dans les futures propositions législatives sectorielles;
- stimuler la participation des administrations publiques pour faciliter l'utilisation de la certification et des spécifications communes dans les marchés publics; et
- assurer le suivi de l'utilisation des exigences pertinentes en matière de certification dans les marchés publics et dans les achats des entreprises et présenter un rapport sur l'état du marché dans trois ans.

3.2. Accroître les investissements dans la cybersécurité en Europe et soutenir les PME

L'innovation dans la cybersécurité est en plein essor en Europe, mais l'Union européenne n'a pas encore de réelle culture de l'investissement dans ce domaine. Il existe de nombreuses PME innovantes dans ce secteur mais elles sont souvent incapables de développer leurs activités faute, notamment, d'obtenir le financement nécessaire pour les soutenir lors des premières étapes de leur expansion. En outre, les entreprises n'ont pas facilement accès au capital risque en Europe et les budgets dont elles disposent pour accroître leur visibilité grâce au marketing ou faire face à la disparité des exigences en matière de normalisation et de conformité sont insuffisants.

Dans le même temps, la coopération entre les acteurs de la cybersécurité est assez fragmentaire et il faut intensifier les efforts pour accroître la concentration économique et développer de nouvelles chaînes de valeur[31].

[31] Voir SWD(2016) 216.

Pour développer les investissements dans la cybersécurité en Europe et soutenir les PME, il faut faciliter l'accès au financement. Il faut aussi soutenir la création de pôles de cybersécurité compétitifs sur le plan mondial et de centres d'excellence dans des écosystèmes régionaux favorables à la croissance numérique. Ce soutien doit être lié à la mise en œuvre des stratégies de spécialisation intelligente et à d'autres instruments de l'UE afin que le secteur européen de la cybersécurité puisse en tirer le meilleur parti possible.

L'approche de la Commission consistera à sensibiliser au maximum la communauté de la cybersécurité aux possibilités de financement disponibles aux niveaux européen, national et régional (à la fois en ce qui concerne les instruments horizontaux et les appels spécifiques[32]) en ayant recours aux instruments et canaux existants tels que le réseau «Entreprise Europe».

En complément de ces efforts, la Commission étudiera, avec la Banque européenne d'investissement (BEI) et le Fonds européen d'investissement (FEI), des moyens de faciliter l'accès au financement. Il pourra s'agir de fonds propres, d'investissements en quasi-fonds propres, de prêts et de garanties pour des projets ou de contre-garanties fournies à des intermédiaires, par exemple par la création d'une plateforme d'investissement en matière de cybersécurité dans le cadre du Fonds européen pour les investissements stratégiques[33].

En outre, la Commission examinera, avec les régions et les États membres intéressés, la possibilité de créer une plateforme de spécialisation intelligente en matière de cybersécurité[34] pour aider à coordonner et à planifier les stratégies de cybersécurité et mettre en place une collaboration stratégique entre les acteurs dans les écosystèmes régionaux. Cette approche devrait aussi contribuer à libérer le potentiel des Fonds structurels et d'investissement européens existants pour le secteur de la cybersécurité.

D'une manière plus générale, la Commission entend promouvoir la sécurité en adoptant une approche fondée sur la conception et en veillant à ce que les exigences en matière de cybersécurité soient prises en considération de manière cohérente pour tous les investissements dans des infrastructures qui ont une composante numérique et qui sont cofinancées par des fonds européens. Pour ce faire, elle introduira progressivement les exigences pertinentes dans les règles relatives aux marchés publics et aux programmes.

La Commission entend:

- utiliser les outils de soutien aux PME existants pour sensibiliser davantage la

[32] Voir par exemple l'appel multisectoriel de 2016 dans le cadre du mécanisme pour l'interconnexion en Europe ou les appels COSMO 2016 au titre du programme d'internationalisation des clusters.

[33] Dans le cadre du Fonds européen pour les investissements stratégiques, les projets peuvent bénéficier d'un soutien direct ou indirect par les plateformes d'investissement. Ces plateformes permettent de financer des projets de plus petite taille et de regrouper les fonds de différentes sources pour diversifier les investissements en fonction du thème ou de la zone géographique.

[34] Voir les instruments de spécialisation intelligente (RIS3): http://s3platform.jrc.ec.europa.eu/.

communauté de la cybersécurité aux possibilités de financement existantes;

- accroître le recours aux outils et instruments de l'UE pour soutenir les PME innovantes dans l'étude de synergies entre les marchés civil et militaire de la cybersécurité[35];
- étudier, avec la BEI et le FEI, la possibilité de faciliter l'accès aux investissements, par exemple en créant une plateforme d'investissement en matière de cybersécurité ou d'autres outils;
- mettre en place une plateforme de spécialisation intelligente en matière de sécurité pour prodiguer des conseils d'experts aux pays et régions intéressés par des investissements dans le secteur de la cybersécurité (RIS3); et
- promouvoir une approche de la sécurité fondée sur la conception pour tous les investissements dans des infrastructures qui ont une composante numérique et sont cofinancées par des fonds de l'UE.

4. STIMULER ET FAIRE PROSPERER LE SECTEUR EUROPEEN DE LA CYBERSECURITE PAR L'INNOVATION - CREATION DU PPPC SUR LA CYBERSECURITE

Un partenariat public-privé contractuel sur la cybersécurité sera signé pour stimuler la compétitivité et l'innovation dans le secteur européen de la cybersécurité. Il regroupera les ressources sectorielles et publiques nécessaires pour garantir l'excellence dans la recherche et l'innovation.

Ce partenariat est destiné à instaurer un climat de confiance parmi les États membres et les acteurs de secteur en promouvant la coopération dès les premières étapes du processus de recherche et d'innovation. Il vise aussi à contribuer à l'alignement de l'offre et de la demande pour permettre aux entreprises de connaître les futurs besoins des utilisateurs finals et de secteurs qui sont des clients importants pour les solutions de cybersécurité (énergie, santé, transports, finance, par exemple). Ces derniers seront ainsi davantage incités à définir, pour leurs activités, des exigences communes en matière de sécurité numérique et de protection de la vie privée et des données.

Le PPPc sur la cybersécurité permettra aussi d'optimiser l'utilisation des fonds disponibles. Pour ce faire, il faudra, premièrement, renforcer la coordination avec les États membres et, deuxièmement, intensifier les travaux sur certaines priorités techniques pour aider le secteur de la cybersécurité à réaliser des avancées technologiques et à maîtriser des technologies essentielles pour l'avenir. À cet égard, l'élaboration de logiciels libres et de normes ouvertes, qui peut contribuer à susciter un climat de confiance et à encourager la transparence et l'innovation de rupture, devrait aussi faire partie des investissements réalisés dans ce PPPc.

Les travaux menés au titre de ce partenariat sur la cybersécurité bénéficieront aussi de synergies avec d'autres projets européens, notamment ceux qui concernent des aspects liés à la sécurité tels que les PPP sur les usines du futur, l'efficacité énergétique des bâtiments, la 5G et

[35] Par exemple, le réseau Entreprise Europe et le réseau européen des régions ayant un lien avec la défense offriront aux régions de nouvelles perspectives en matière de coopération transfrontière en ce qui concerne le double usage et notamment la cybersécurité, et aux PME des possibilités d'entreprendre des activités de rapprochement.

les mégadonnées[36]et d'autres PPP sectoriels[37], ainsi que l'initiative sur l'internet des objets[38]. Par ailleurs, on s'efforcera d'assurer une cohérence étroite avec le nuage européen ouvert au service de la science initiative européenne et l'initiative européenne dans le domaine du calcul intensif pour les cybertechnologies quantiques (innovation dans la distribution quantique de clés, recherche sur l'informatique quantique, par exemple).

Le PPPc sur la cybersécurité est lancé au titre d'Horizon 2020[39] (H2020), le programme-cadre de l'UE pour la recherche et l'innovation pour la période 2014-2020. Il mobilisera des financements au titre de deux composantes du programme: l'objectif spécifique «Primauté dans le domaine des technologies génériques et industrielles» et le défi de société intitulé «Des sociétés sûres (SC7)». Le PPPc sera doté d'un budget total pouvant atteindre 450 millions d'euros, les ressources mobilisées auprès des entreprises grâce à l'effet multiplicateur équivalant à trois fois ce montant. Il convient aussi de traiter la cybersécurité en coordination avec d'autres parties pertinentes d'Horizon 2020 (tels que les défis de société relatifs à l'énergie, aux transports et à la santé, ainsi que le volet «Excellence» d'Horizon 2020). Les travaux réalisés à cet égard contribueront aux objectifs du PPPc sur la cybersécurité. La coordination devrait être prévue dès le stade de la définition des stratégies sectorielles.

Le PPPc sera mis en œuvre en toute transparence. Il sera doté d'une gouvernance ouverte et souple et adaptée à l'environnement de la cybersécurité, qui évolue très rapidement. Il tiendra également compte de la nécessité, pour les États membres, d'examiner les effets des modifications technologiques sur la sécurité du fonctionnement des infrastructures nationales et transfrontières. Les résultats du partenariat doivent également être viables pendant plusieurs années pour que les objectifs prévus puissent être atteints.

Le PPPc sera soutenu par l'organisation européenne pour la cybersécurité (ECSO). Les membres de cette dernière refléteront la diversité du marché de la cybersécurité en Europe et comprendront aussi des représentants d'administrations publiques nationales, régionales et locales, de centres de recherche et d'universités ainsi que d'autres parties intéressées.

La Commission entend:

- signer avec les entreprises du secteur un partenariat public-privé contractuel sur la cybersécurité qui devrait être opérationnel au troisième trimestre de 2016;
- lancer les premiers appels de propositions Horizon 2020 au titre du PPPc sur la cybersécurité au premier trimestre de 2017; et
- veiller à la coordination du PPPc sur la cybersécurité avec les stratégies sectorielles, les instruments d'Horizon 2020 et les PPP sectoriels.

5. CONCLUSION

La présente communication contient des mesures visant à renforcer le système européen de cyber-résilience et à promouvoir la compétitivité et l'innovation dans le secteur européen de la

[36] Le partenariat public-privé sur l'infrastructure 5G & le partenariat public-privé Big Data Value (consacré à la valeur des mégadonnées).
[37] Les partenariats public-privé SESAR ou Shift2Rail, par exemple.
[38] Alliance for Internet of Things Innovation (AIOTI – alliance pour l'innovation dans le domaine de l'internet des objets).
[39] http://ec.europa.eu/programmes/horizon2020/en/official-documents.

cybersécurité, comme annoncé dans la stratégie de cybersécurité de l'Union européenne et dans la stratégie pour un marché unique numérique. La Commission invite le Parlement européen et le Conseil à soutenir cette approche.