Conseil de
l'Union européenne

Bruxelles, le 14 septembre 2017
(OR. en)

12211/17

CYBER 132
RELEX 767
JAI 790
ENFOPOL 413
TELECOM 212
MI 633
RECH 308

NOTE DE TRANSMISSION

Origine:	Pour le Secrétaire général de la Commission européenne, Monsieur Jordi AYET PUIGARNAU, Directeur
Date de réception:	13 septembre 2017
Destinataire:	Monsieur Jeppe TRANHOLM-MIKKELSEN, Secrétaire général du Conseil de l'Union européenne
N° doc. Cion:	JOIN(2017) 450 final
Objet:	COMMUNICATION CONJOINTE AU PARLEMENT EUROPÉEN ET AU CONSEIL Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide

Les délégations trouveront ci-joint le document JOIN(2017) 450 final.

p.j.: JOIN(2017) 450 final

COMMISSION
EUROPÉENNE

LA HAUTE REPRÉSENTANTE DE
L'UNION POUR LES AFFAIRES
ÉTRANGÈRES ET LA
POLITIQUE DE SÉCURITÉ

Bruxelles, le 13.9.2017
JOIN(2017) 450 final

COMMUNICATION CONJOINTE AU PARLEMENT EUROPÉEN ET AU CONSEIL

Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide

1. INTRODUCTION

La cybersécurité est essentielle tant pour notre prospérité que pour notre sécurité. Plus nos vies quotidiennes et nos économies deviennent dépendantes des technologies numériques, plus nous sommes vulnérables. Les incidents de cybersécurité se diversifient, en ce qui concerne aussi bien leurs auteurs que leurs objectifs. La cyberactivité malveillante constitue une menace non seulement pour nos économies et la progression vers le marché unique numérique, mais aussi pour le fonctionnement même de nos démocraties, pour nos libertés et pour nos valeurs. Notre sécurité future dépend de la manière dont nous adapterons notre capacité à protéger l'UE des cybermenaces: l'infrastructure civile et les capacités militaires sont toutes deux tributaires de systèmes numériques sûrs. C'est un fait qui a été reconnu par le Conseil européen de juin 2017[1], ainsi que dans la stratégie globale sur la politique étrangère et de sécurité de l'Union européenne[2].

Les risques se multiplient de façon exponentielle. Selon certaines études, l'incidence économique de la cybercriminalité a quintuplé entre 2013 et 2017, et pourrait quadrupler encore d'ici à 2019[3]. L'utilisation de rançongiciels[4] est particulièrement en hausse et les dernières attaques[5] traduisent une augmentation spectaculaire de la cybercriminalité. Toutefois, les rançongiciels sont loin d'être la seule menace.

Les cybermenaces sont le fait d'acteurs aussi bien étatiques que non étatiques; elles sont souvent criminelles, motivées par l'appât du gain, mais elles peuvent aussi être politiques et stratégiques. La menace criminelle est accentuée par l'effacement progressif de la frontière entre cybercriminalité et criminalité «traditionnelle», les criminels utilisant l'internet à la fois pour étendre leurs activités et pour y puiser de nouvelles méthodes et de nouveaux outils en vue de commettre des délits[6]. Or, dans la grande majorité des cas, les chances de localiser les criminels sont minimes, et la probabilité de pouvoir les poursuivre en justice est encore plus faible.

Simultanément, certains acteurs étatiques poursuivent de plus en plus souvent leurs objectifs géopolitiques en employant non seulement les méthodes traditionnelles telles que la force militaire, mais aussi des outils informatiques plus discrets, y compris en interférant dans les processus démocratiques nationaux. De nos jours, l'utilisation du cyberespace comme une zone de guerre, soit exclusivement, soit dans le cadre d'approches hybrides, est de notoriété publique. Campagnes de désinformation, fausses nouvelles et cyberopérations visant des infrastructures critiques sont de plus en plus fréquentes et appellent une réaction. C'est la raison pour laquelle, dans son document de réflexion sur l'avenir de la défense européenne[7], la Commission a souligné l'importance de la coopération en matière de cyberdéfense.

À moins que nous ne renforcions notre cybersécurité, ce risque va aller croissant, parallèlement à la transformation numérique. Des dizaines de milliards de dispositifs reliés à

---

1 http://www.consilium.europa.eu/fr/press/press-releases/2017/06/23-euco-conclusions/

2 http://europa.eu/globalstrategy/fr/strategie-globale-de-lunion-europeenne

3 Voir par exemple l'étude de McAfee & Centre for Strategic and International Studies «Net losses: Estimating the Global Cost of Cybercrime» [Pertes nettes: une estimation du coût global de la cybercriminalité], 2014

4 Le rançongiciel est un type de logiciel malveillant qui empêche complètement ou partiellement les utilisateurs d'accéder à leur système, en verrouillant soit l'écran du système, soit les fichiers de l'utilisateur, jusqu'à ce qu'une rançon soit versée.

5 En mai 2017, l'attaque menée au moyen du rançongiciel WannaCry a touché plus de 400 000 ordinateurs dans plus de 150 pays. Un mois plus tard, l'attaque lancée par le rançongiciel «Petya» a frappé l'Ukraine et plusieurs entreprises dans le monde entier.

6 Europol, Évaluation de la menace que représente la grande criminalité organisée, 2017

7 https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_fr.pdf

l'«internet des objets» devraient être connectés à l'internet d'ici à 2020, mais la cybersécurité n'est pas encore une priorité dans leur conception[8]. Ne pas protéger les dispositifs qui contrôleront nos réseaux électriques, nos voitures, nos réseaux de transport, nos usines, nos finances, nos hôpitaux et nos maisons pourrait avoir des conséquences dévastatrices et fortement altérer la confiance des consommateurs dans les technologies émergentes. Le risque d'attaques visant des cibles civiles pour des motifs politiques et de lacunes de la cyberdéfense militaire aggrave encore le danger.

L'approche décrite dans la présente communication conjointe placera l'Union européenne en meilleure position pour faire face à ces menaces. Elle la dotera d'une résilience et d'une autonomie stratégique accrues, stimulera les capacités en matière de technologie et de compétences et contribuera à édifier un marché unique robuste. Pour ce faire, il convient que les bonnes structures soient en place, afin de bâtir une cybersécurité solide et de réagir en cas de besoin, avec la pleine participation de tous les acteurs clés. L'approche choisie permettra aussi de mieux prévenir les cyberattaques, grâce à une intensification des actions visant à détecter, à localiser et à traduire en justice les responsables. Elle tiendra également compte de la dimension mondiale du phénomène en développant la coopération internationale en tant que plateforme sur laquelle l'UE jouera un rôle moteur en matière de cybersécurité. Ces mesures s'inscrivent dans la droite ligne des approches adoptées dans le cadre du marché unique numérique, de la stratégie globale de l'UE, du programme européen en matière de sécurité[9], du cadre commun en matière de lutte contre les menaces hybrides[10] et de la communication intitulée «Lancement du Fonds européen de la défense»[11][12].

L'Union européenne planche déjà sur bon nombre de ces points: il est maintenant temps d'assembler les différents volets. En 2013, l'UE a présenté une stratégie de cybersécurité comportant plusieurs axes de travail essentiels destinés à améliorer la cyber-résilience[13]. Ses principaux objectifs et principes, qui sont de favoriser l'émergence d'un cyberecosystème ouvert, sûr et fiable, restent valables. Mais l'évolution et l'assombrissement constants du paysage des menaces appellent de nouvelles actions si l'on veut résister et faire obstacle à de futures attaques[14].

Vu la portée de ses politiques et les instruments, les structures et les capacités à sa disposition, l'Union européenne est bien placée pour traiter les problèmes de cybersécurité. Si les États membres demeurent responsables de la sécurité nationale, l'ampleur et la nature transfrontière de la menace plaident nettement en faveur d'une action de l'UE fournissant encouragement et soutien aux États membres afin qu'ils développent et maintiennent des capacités nationales en matière de cybersécurité à la fois plus nombreuses et de meilleure qualité, tout en renforçant les capacités au niveau de l'Union. Cette approche est conçue pour inciter tous les acteurs — l'Union européenne, les États membres, les entreprises et les particuliers — à donner à la

---

8 IDC and TXT Solutions (2014), SMART 2013/0037 Cloud and IoT combination [Solutions IDC et TXT (2014), SMART 2013/0037, combinaison Nuage et Internet des objets], étude pour la Commission.

9 COM(2015) 185 final

10 JOIN(2016) 18 final

11 COM(2017) 295

12 L'approche envisagée est étayée par les avis scientifiques indépendants fournis par le groupe de conseillers scientifiques à haut niveau du mécanisme de conseil scientifique de la Commission européenne (voir les références ci-dessous).

13 JOIN(2013) 1 final. Une évaluation de cette stratégie est disponible dans le document SWD (2017) 295.

14 Sauf indication expresse, les propositions figurant dans la présente communication sont neutres du point de vue budgétaire. Toute initiative ayant des implications budgétaires suivra en bonne et due forme les procédures budgétaires annuelles et ne saurait préjuger du prochain cadre financier pluriannuel pour l'après-2020.

cybersécurité la priorité requise afin de développer la résilience et de permettre à l'UE de mieux réagir aux cyberattaques. Elle comportera des mesures concrètes d'aide à la détection, à l'instruction et éventuellement aux poursuites judiciaires, pour tous les types de cyberincidents visant l'UE et ses États membres. Elle permettra à l'Union d'entreprendre des actions extérieures afin de promouvoir efficacement la cybersécurité à l'échelle mondiale. L'UE passera ainsi du mode réactif au mode proactif dans sa protection de la prospérité, de la société et des valeurs européennes ainsi que des libertés et des droits fondamentaux, en répondant aux menaces à la fois actuelles et à venir.

2 DÉVELOPPER LA RÉSILIENCE DE L'UNION EUROPÉENNE FACE AUX CYBERATTAQUES

Une cyber-résilience forte passe par une approche collective et de grande envergure. Celle-ci nécessite des structures plus solides et plus efficaces pour promouvoir la cybersécurité et réagir aux cyberattaques dans les États membres mais aussi dans les institutions, les agences et les organes de l'Union elle-même. Elle exige aussi une stratégie transsectorielle plus globale pour le développement de la cyber-résilience et de l'autonomie stratégique, avec un marché unique fort, des avancées majeures dans la capacité technologique de l'UE, et un nombre beaucoup plus élevé d'experts qualifiés. Au cœur de cette approche, on trouve une plus grande acceptation du fait que la cybersécurité constitue, pour notre société, un enjeu qui nous concerne tous, au point que le gouvernement, l'économie et la société devraient y être associés à de multiples niveaux.

2.1 Renforcer l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)

L'**Agence européenne chargée de la sécurité des réseaux et de l'information** (ENISA) a un rôle essentiel à jouer dans le renforcement de la cyber-résilience et de la réaction de l'UE, mais elle est limitée par son mandat actuel. C'est pourquoi la Commission présente une proposition de réforme ambitieuse, comprenant **un mandat permanent pour l'agence**[15]. L'ENISA pourra ainsi apporter son soutien aux États membres, aux institutions de l'Union et aux entreprises dans des domaines clés, parmi lesquels la mise en œuvre de la directive sur la sécurité des réseaux et des systèmes d'information[16] («directive SRI») ainsi que du cadre de certification de cybersécurité proposé.

L'ENISA réformée jouera un rôle consultatif de premier plan dans l'élaboration et la mise en œuvre des politiques et devra aussi promouvoir la cohérence entre les initiatives sectorielles et la directive SRI et aider à mettre en place des centres d'échange et d'analyse d'informations dans les secteurs critiques. L'ENISA placera la barre plus haut et améliorera la capacité de l'Europe à faire face en organisant des exercices paneuropéens annuels de cybersécurité combinant les réactions à différents niveaux. Elle soutiendra également l'élaboration d'une politique européenne de certification de cybersécurité pour les technologies de l'information et de la communication (TIC) et jouera un rôle important dans le renforcement de la coopération opérationnelle et de la gestion des crises à travers l'UE. L'agence servira aussi de point de contact à la communauté de la cybersécurité, qui pourra y trouver informations et connaissances.

[15] COM(2017) 477

[16] Directive 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

Une compréhension rapide et commune des menaces et des incidents au moment où ils ont lieu est indispensable pour décider si des mesures d'atténuation ou de réaction communes, soutenues par l'UE, sont nécessaires. Un tel échange d'informations nécessite la participation de tous les acteurs concernés — agences et organes de l'Union, ainsi qu'États membres — aux niveaux technique, opérationnel et stratégique. L'ENISA, en collaboration avec les organes compétents au niveau des États membres et de l'Union, notamment le réseau des centresde réponse aux incidents de sécurité informatiques[17], la CERT-UE, Europol et le Centre de situation et du renseignement de l'Union européenne (INTCEN), contribuera également à l'appréciation de la situation à l'échelle de l'Union. Celle-ci alimentera l'activité de renseignement sur les menaces et l'élaboration de politiques dans le cadre, d'une part, d'un suivi régulier du paysage des menaces et d'une coopération opérationnelle efficace, et, d'autre part, de la réaction aux incidents transfrontières à grande échelle.

2.2 Vers un marché unique de la cybersécurité

La croissance du marché de la cybersécurité dans l'Union - en termes de produits, de services et de processus - est freinée de diverses façons. L'un des principaux facteurs est l'absence de systèmes de certification de cybersécurité reconnus dans toute l'Union, qui permettraient d'incorporer des normes de résilience plus strictes dans les produits et de consolider la confiance du marché à l'échelle de l'UE. C'est pourquoi la Commission présente une proposition visant à instaurer un **cadre européen de certification de cybersécurité**[18]. Ce cadre spécifierait la procédure de création de systèmes de certification de cybersécurité à l'échelle de l'UE, portant sur les produits, les services et/ou les systèmes et adaptant le niveau d'assurance à l'utilisation prévue (qu'il s'agisse d'infrastructures critiques ou d'appareils grand public)[19]. Il serait porteur d'avantages évidents pour les entreprises puisqu'il leur éviterait de devoir subir plusieurs processus de certification dans le cadre de leurs activités commerciales à l'international, limitant les coûts administratifs et financiers. L'utilisation de systèmes élaborés en application de ce cadre de certification contribuerait aussi à renforcer la confiance des consommateurs, grâce à un certificat de conformité qui informera et rassurera les acheteurs et les utilisateurs en ce qui concerne les propriétés des produits et des services en matière de sécurité. Cela transformerait des normes de cybersécurité élevées en source d'avantage concurrentiel. Il en résulterait une résilience accrue puisque les produits et les services TIC feraient l'objet d'une évaluation formelle à l'aune d'un ensemble déterminé de normes de cybersécurité, qui pourrait être élaboré en s'inspirant étroitement des travaux plus généraux en cours au sujet des normes TIC[20].

Les systèmes relevant du cadre de certification seraient volontaires et ne créeraient pas d'obligations réglementaires immédiates pour les vendeurs ou les prestataires de services. Ils ne seraient contraires à aucune obligation légale applicable, par exemple à la législation de l'UE sur la protection des données.

Une fois le cadre établi, la Commission invitera les parties prenantes concernées à mettre l'accent sur trois domaines prioritaires:

---

[17] Institué par l'article 9 de la directive SRI.

[18] COM(2017) 477.

[19] Un niveau d'assurance indique le degré de rigueur de l'évaluation de sécurité et il est généralement proportionnel au niveau de risque associé au domaine d'application ou à la fonction examinés (en d'autres termes, le degré d'assurance requis est plus élevé lorsqu'il s'agit de produits ou de services TIC utilisés dans des domaines d'application ou des fonctions à haut risque).

[20] COM(2016) 176.

- la sécurité dans les applications critiques ou à haut risque[21]: les systèmes dont nous dépendons au quotidien deviennent de plus en plus numériques et interconnectés, des voitures particulières aux machines industrielles, du plus grand, tels que les avions ou les centrales électriques, au plus petit, comme les dispositifs médicaux. C'est pourquoi les composants TIC essentiels qui se trouvent dans ces produits et ces systèmes devraient faire l'objet d'évaluations de sécurité rigoureuses.

- la cybersécurité dans les produits, réseaux, systèmes et services numériques courants, utilisés par le secteur public comme par le secteur privé, pour se protéger des attaques et se conformer à des obligations réglementaires[22] - cryptage de courrier électronique, pare-feux et réseaux privés virtuels par exemple; il est essentiel que l'utilisation croissante de ces outils ne crée pas de nouvelles sources de risques ou de nouvelles failles.

- l'utilisation de méthodes reposant sur la «sécurité dès la conception» dans les dispositifs interconnectés, numériques, bon marché et vendus en masse qui forment l'internet des objets: les systèmes relevant du cadre de certification pourraient être utilisés pour indiquer que les produits sont élaborés en recourant aux méthodes de développement sécurisées les plus récentes, qu'ils ont subi des tests de sécurité adéquats et que les vendeurs se sont engagés à mettre leur logiciel à jour si de nouvelles menaces ou de nouvelles failles sont découvertes.

Ces priorités devraient tenir particulièrement compte de l'évolution du paysage des menaces en matière de cybersécurité, ainsi que de l'importance des services essentiels tels que les transports, l'énergie, le secteur de la santé, les banques, les infrastructures des marchés financiers, l'eau potable ou l'infrastructure numérique[23].

Bien qu'aucun produit, système ou service TIC ne puisse être garanti sûr à «100 %», il existe plusieurs défauts connus et bien documentés dans la conception des produits TIC qui peuvent être exploités pour lancer des attaques. L'adoption, par les producteurs de dispositifs connectés, de logiciels et de matériel informatiques, d'une approche fondée sur le principe de la «sécurité dès la conception» garantirait la prise en compte de la cybersécurité avant la mise sur le marché de nouveaux produits. Cela pourrait faire partie de l'«obligation de diligence», dont le développement doit se poursuivre en collaboration avec les entreprises, qui pourrait limiter la vulnérabilité des produits et des logiciels grâce à tout un éventail de méthodes à appliquer depuis la conception jusqu'aux essais et à la vérification, y compris la vérification formelle le cas échéant, grâce à la maintenance à long terme et à l'utilisation de processus de développement sécurisés tout au long du cycle de vie du produit ainsi qu'à travers des mises à jour et des correctifs pour remédier aux failles restées cachées jusque-là et assurer une mise à jour et une réparation rapides[24]. La confiance des consommateurs dans les produits numériques s'en trouverait aussi renforcée.

---

[21] Avec une exception pour les cas où la certification obligatoire ou volontaire est régie par d'autres actes de l'Union.

[22] Par exemple, la directive (UE) 2016/1148, le règlement (UE) 2016/679, la directive (UE) 2015/2366 et d'autres propositions de textes réglementaires, comme le code européen des communications électroniques, exigent tous que les organisations mettent en place des mesures de sécurité adaptées afin de contrer les risques pour la cybersécurité les concernant.

[23] Autrement dit, les domaines relevant de la directive 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.

[24] Cybersecurity in the European Digital Single Market [La cybersécurité dans le marché unique numérique européen], groupe de conseillers scientifiques à haut niveau, mars 2017.

En outre, il conviendrait de reconnaître l'importance du rôle des chercheurs tiers spécialisés en sécurité dans la détection de failles dans les produits et les services existants et de créer les conditions nécessaires à une divulgation coordonnée des failles dans l'ensemble des États membres[25], en s'inspirant des bonnes pratiques[26] et des normes en la matière[27].

Par ailleurs, **certains secteurs** sont confrontés à des problèmes spécifiques et devraient être encouragés à développer leur propre approche. Les stratégies de cybersécurité générales se verraient ainsi complétées par des stratégies de cybersécurité sectorielles dans des domaines tels que les services financiers[28], l'énergie, les transports et la santé[29].

La Commission a déjà mis en évidence les questions de **responsabilité** spécifiquement liées aux nouvelles technologies numériques[30] et le travail d'analyse des implications est en cours; les prochaines étapes seront achevées d'ici juin 2018. La cybersécurité soulève des questions relatives à l'imputation de la responsabilité en cas de dommage pour les entreprises et les chaînes d'approvisionnement et ne pas y répondre entravera le développement d'un marché unique solide pour les produits et les services de cybersécurité.

Pour finir, le développement du marché unique de l'UE dépend également de l'intégration de la cybersécurité dans la politique de commerce et d'investissement. L'incidence des prises de participation étrangères sur les technologies critiques — dont la cybersécurité est un exemple important — est un élément clé du cadre relatif au **filtrage de l'investissement direct étranger dans l'Union européenne**[31], qui vise à permettre le filtrage des investissements en provenance de pays tiers sous l'angle de la sécurité et de l'ordre public. D'ailleurs, dans les économies de plusieurs pays tiers, les exigences en matière de cybersécurité ont déjà créé des obstacles aux échanges de biens et de services de l'Union dans des secteurs importants. Le cadre de certification de cybersécurité de l'UE consolidera encore la position internationale de l'Europe et devrait être complété par la poursuite des efforts consentis pour élaborer des normes de haute sécurité générales et l'adoption d'accords de reconnaissance mutuelle.

2.3 Mettre pleinement en œuvre la directive sur la sécurité des réseaux et des systèmes d'information

Les principaux outils en matière de cybersécurité relevant actuellement des autorités nationales, l'UE a reconnu la nécessité de fixer des normes plus élevées. Il est rare que les incidents de cybersécurité de grande ampleur ne touchent qu'un seul État membre en raison du caractère de plus en plus mondialisé, dépendant du numérique et interconnecté de secteurs clés tels que la banque, l'énergie ou les transports.

---

[25] La divulgation coordonnée des failles est une forme de coopération qui donne aux chercheurs spécialisés dans la sécurité l'occasion et les moyens de signaler les failles au propriétaire ou au vendeur du système d'information, permettant ainsi à l'organisation concernée de diagnostiquer la faille et d'y remédier de manière correcte et rapide avant que les détails à ce sujet ne soient communiqués à des tiers ou au public.

[26] Voir par exemple, Good Practice Guide on Vulnerability Disclosure. From Challenges to recommendations [Guide de bonnes pratiques sur la divulgation des failles. Des défis aux recommandations], ENISA, 2016

[27] ISO/IEC 29147: 2014 — Technologies de l'information — Techniques de sécurité — Divulgation de vulnérabilité

[28] Les futurs travaux de la Commission sur la technologie financière porteront aussi sur la cybersécurité pour le secteur financier.

[29] Dans le secteur de l'énergie, par exemple, en combinant des technologies de l'information de pointe et d'autres très anciennes, en particulier avec les besoins en temps réel du réseau électrique.

[30] COM(2017) 228.

[31] COM(2017) 478.

La directive sur la sécurité des réseaux et des systèmes d'information (la «directive SRI») est le premier acte législatif concernant la cybersécurité à l'échelle de l'UE[32]. Elle est destinée à renforcer la résilience en améliorant les capacités nationales en matière de cybersécurité, à favoriser une meilleure coopération entre les États membres et à exiger des entreprises actives dans des secteurs économiques importants qu'elles adoptent des pratiques efficaces de gestion des risques et signalent les incidents graves aux autorités nationales. Ces obligations s'appliquent également à trois types de fournisseurs de services internet clés: l'informatique en nuage, les moteurs de recherche et les places de marché en ligne. La directive vise une approche plus solide et plus systématique ainsi qu'un meilleur flux d'informations.

Une mise en œuvre complète de la directive par tous les États membres d'ici à mai 2018 est essentielle pour la cyber-résilience de l'UE. Ce processus est soutenu par le travail collectif des États membres qui se traduira, d'ici à l'automne 2017, par des lignes directrices visant à promouvoir une mise en œuvre plus homogène, notamment en ce qui concerne les opérateurs de services essentiels. Dans le cadre du présent paquet «Cybersécurité», la Commission publie également une communication[33] destinée à soutenir leurs efforts en mettant à leur disposition les bonnes pratiques des États membres pertinentes pour la mise en œuvre de la directive et des orientations sur la manière dont la directive devrait fonctionner dans la pratique.

Un domaine dans lequel la directive devra être complétée est le flux d'informations. Par exemple, la directive ne couvre que les secteurs stratégiques essentiels, mais, en toute logique, il serait nécessaire que toutes les parties prenantes touchées par des cyberattaques adoptent une approche similaire afin de pouvoir disposer d'une appréciation systématique des failles et des points d'entrée pour les auteurs de cyberattaques. En outre, la coopération et l'échange d'informations entre le secteur public et le secteur privé sont confrontés à plusieurs obstacles. Les gouvernements et les autorités publiques sont réticents lorsqu'il s'agit de partager des informations pertinentes pour la cybersécurité par crainte de compromettre la sécurité ou la compétitivité de leur pays. Les entreprises privées rechignent quant à elles à partager des informations sur leurs failles en matière de cybersécurité et les pertes qui en résultent par crainte de compromettre des informations commerciales sensibles, de mettre en péril leur réputation ou de risquer d'enfreindre les règles en matière de protection des données[34]. La confiance doit être renforcée pour que les partenariats public-privé soutiennent une plus grande coopération et un plus grand échange d'informations entre un plus grand nombre de secteurs. Le rôle des centres d'échange et d'analyse d'informations est particulièrement important pour ce qui est de créer le climat de confiance nécessaire à l'échange d'informations entre le secteur privé et le secteur public. Une première série de mesures ont été prises en ce qui concerne certains secteurs critiques comme l'aviation, par la création du Centre européen pour la cybersécurité dans l'aviation[35], et l'énergie, par la mise sur pied de centres d'échange et d'analyse d'informations[36]. La Commission contribuera pleinement à

---

[32] Directive 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.

[33] COM(2017) 476.

[34] Cybersecurity in the European Digital Single Market [La cybersécurité dans le marché unique numérique européen], groupe de conseillers scientifiques à haut niveau, mars 2017. Un problème spécifique concerne les secrets d'affaires; ainsi, la réticence à signaler le vol électronique de secrets d'affaires et l'importance de l'existence de canaux de communication sûrs, garantissant la confidentialité sont mentionnées dans la communication de juillet 2016 intitulée «Renforcer le système européen de cyber-résilience».

[35] https://www.easa.europa.eu/newsroom-and-events/news/implementation-european-centre-cyber-security-aviationeccsa.

[36] Il s'agit d'organisations sans but lucratif, dirigées par leurs membres, constituées d'entités privées et publiques, ayant pour objet l'échange d'informations sur les cybermenaces ainsi que sur les risques, la

cette approche, avec le soutien de l'ENISA, et un coup d'accélérateur devra être donné tout particulièrement en ce qui concerne les secteurs fournissant les services essentiels définis dans la directive SRI.

2.4 La résilience grâce à une réaction d'urgence rapide

Lorsqu'une cyberattaque se produit, une réaction rapide et efficace peut en atténuer les effets. Une telle réaction peut également montrer que les autorités publiques ne sont pas impuissantes face aux cyberattaques, et ainsi contribuer à instaurer un climat de confiance. En ce qui concerne la réaction des institutions de l'UE, il convient en premier lieu que les aspects relatifs à la cybersécurité soient intégrés dans les mécanismes de gestion des crises qui existent déjà au niveau de l'UE: le dispositif intégré de l'UE pour une réaction au niveau politique dans les situations de crise, coordonné par la présidence du Conseil[37], et les systèmes généraux d'alerte rapide de l'UE[38]. La nécessité de réagir à un cyberincident ou à une cyberattaque de nature particulièrement grave pourrait constituer un motif suffisant pour qu'un État membre invoque la clause de solidarité de l'UE[39].

Une réaction rapide et efficace s'appuie également sur un mécanisme d'échange rapide des informations entre tous les acteurs clés au niveau national et européen, ce qui exige de la clarté en ce qui concerne leurs responsabilités et leurs rôles respectifs. La Commission a consulté les institutions et les États membres sur un «plan d'action» («Blueprint») visant à fournir un processus efficace de réaction opérationnelle, au niveau de l'Union et des États membres, à un cyberincident de grande ampleur. Ce **plan d'action**, présenté dans une recommandation[40] faisant partie du présent paquet, explique comment la cybersécurité est intégrée dans les mécanismes de gestion des crises qui existent à l'échelle de l'UE et expose les objectifs et les modalités de la coopération entre les États membres ainsi qu'entre les États membres et les institutions, services, organes et organismes compétents de l'UE[41] lors d'une réaction à des incidents et à des crises de grande ampleur en matière de cybersécurité. La recommandation demande également aux États membres et aux institutions de l'UE de créer un cadre de l'UE pour la réaction aux crises de cybersécurité afin de traduire le plan d'action en mesures concrètes. Celui-ci sera régulièrement testé lors d'exercices de gestion de crises dans le domaine de la cybersécurité et dans d'autres domaines[42], et mis à jour si nécessaire.

Étant donné que les incidents de cybersécurité sont susceptibles d'avoir des répercussions importantes sur le fonctionnement des économies et sur la vie quotidienne des citoyens, une option consisterait à examiner la possibilité de créer un **fonds d'intervention pour les urgences en matière de cybersécurité**, sur l'exemple d'autres mécanismes de crise de cette nature dans d'autres domaines d'action de l'UE. Ce fonds permettrait aux États membres de

---

prévention, l'atténuation et la réaction en la matière. Voir, par exemple, les centres européens d'échange et d'analyse d'informations dans le domaine de l'énergie (European Energy Information Sharing and Analysis Centres, http://www.ee-isac.eu).

37 Ce dispositif permet de coordonner les réactions aux crises transsectorielles majeures au plus haut niveau politique.

38 Ces systèmes permettent un échange interne d'informations et une coordination sur les crises multisectorielles émergentes ou sur des menaces prévisibles ou imminentes nécessitant une action au niveau de l'UE.

39 Au titre de l'article 222 du traité sur le fonctionnement de l'Union européenne.

40 C(2017) 6100.

41 Y compris Europol, l'ENISA, l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et organismes de l'Union européenne (CERT-EU) et le Centre de situation et du renseignement de l'Union européenne (INTCEN).

42 Par exemple, ceux gérés par l'ENISA: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

solliciter une aide au niveau de l'UE lors ou à la suite d'un incident majeur, pour autant que l'État membre concerné ait mis en place un système prudent de cybersécurité avant l'incident, ce qui comprend la mise en œuvre intégrale de la directive SRI et des cadres bien développés de gestion des risques et de surveillance au niveau national. Un tel fonds, qui compléterait les mécanismes de gestion des crises qui existent déjà au niveau de l'UE, pourrait permettre le déploiement d'une capacité de réaction rapide dans un souci de solidarité et financer des actions spécifiques d'intervention d'urgence telles que le remplacement du matériel compromis ou le déploiement d'outils d'atténuation ou de réaction, en tirant parti de l'expertise nationale comme dans le cas du mécanisme de protection civile de l'UE.

2.5 Un réseau de compétences en cybersécurité et un centre européen de recherche et de compétences en cybersécurité

Les outils technologiques liés à la cybersécurité sont des atouts stratégiques et constituent des technologies clés pour la croissance à l'avenir. Il est de l'intérêt stratégique de l'Union de maintenir et développer les capacités essentielles lui permettant de défendre son économie, sa société et sa démocratie numériques, de protéger le matériel et les logiciels critiques et d'offrir des services fondamentaux en matière de cybersécurité.

Le partenariat public-privé sur la cybersécurité[43] lancé en 2016 a constitué une première étape importante en donnant lieu à des investissements de 1,8 milliard d'EUR d'ici à 2020. L'ampleur des investissements en cours dans d'autres parties du monde[44] permet toutefois de penser que l'UE doit redoubler d'efforts en termes d'investissement et surmonter la fragmentation des capacités à travers l'Union.

L'Union européenne a apporté une valeur ajoutée, en raison du degré de sophistication de la technologie en matière de cybersécurité, de l'ampleur des investissements requis et de la nécessité de trouver des solutions qui fonctionnent dans tous les pays de l'Union. Sur la base des travaux effectués par les États membres et le partenariat public-privé, une nouvelle étape consisterait à renforcer les capacités de l'UE en matière de cybersécurité en la dotant d'un **réseau de centres de compétences en cybersécurité**[45], au cœur duquel figurerait un **centre européen de recherche et de compétences en cybersécurité**. Ce réseau et ce centre stimuleraient le développement et le déploiement de technologies dans le domaine de la cybersécurité et compléteraient les efforts de renforcement des capacités dans ce domaine au niveau national et de l'Union. La Commission entamera une analyse d'impact afin d'étudier les différentes options – y compris la possibilité de mettre en place une entreprise commune – afin de mettre cette structure sur pied en 2018.

Dans un premier temps, et afin d'alimenter les réflexions ultérieures, la Commission proposera une étape pilote dans le cadre d'Horizon 2020 afin de réunir les centres nationaux au sein d'un réseau permettant de donner un nouvel élan au renforcement des compétences en cybersécurité et au développement de la technologie en la matière. Elle devrait proposer d'injecter à court terme un financement de 50 millions d'EUR à cet effet. Cela complétera la mise en œuvre actuelle du partenariat public-privé sur la cybersécurité.

---

[43] C(2016) 4400 final.

[44] Les États-Unis investiront 19 milliards d'USD dans la cybersécurité durant la seule année 2017, soit une augmentation de 35 % par rapport à l'année précédente. La Maison Blanche, bureau du «Press Secretary»: «Fact Sheet: Cybersecurity National Action Plan», 9 février 2016.

[45] Ce réseau réunirait des centres consacrés à la cybersécurité, qu'ils existent déjà dans les États membres ou soient encore à créer, et dont les membres seraient essentiellement des laboratoires et des organismes publics de recherche.

La mise en commun et la configuration des efforts de recherche seraient au cœur des préoccupations initiales du centre et du réseau. Pour soutenir le développement des capacités industrielles, le centre de compétences pourrait agir en tant que gestionnaire pour s'occuper des projets multinationaux. Cela donnerait également un nouvel élan à l'innovation et à la compétitivité de l'industrie de l'Union sur la scène mondiale dans le développement de la prochaine génération de technologies numériques, y compris l'intelligence artificielle, l'informatique quantique, les chaînes de blocs et les identités numériques sécurisées, ainsi que pour assurer aux entreprises établies dans l'UE un accès aux données de masse, autant d'éléments clés pour la cybersécurité à l'avenir. Le centre pourrait également s'appuyer sur les travaux de l'UE en vue de consolider l'infrastructure de calcul à haute performance, ce qui est essentiel pour l'analyse de grandes quantités de données, le cryptage et le décryptage rapides de données, la vérification des identités, la simulation de cyberattaques et l'analyse de matériel vidéo[46].

Le réseau de centres de compétences pourrait également disposer de capacités pour soutenir l'industrie en procédant à des tests et des simulations permettant d'assurer la certification de cybersécurité décrite au point 2.2. Son implication dans tout l'éventail des activités de l'Union en matière de cybersécurité permettrait d'assurer la mise à jour continue des activités en fonction des besoins. Le centre viserait à assurer des normes de cybersécurité rigoureuses non seulement dans les systèmes technologiques et de cybersécurité mais aussi dans le développement des compétences de haut niveau pour les professionnels, en offrant des solutions et des modèles servant pour les efforts nationaux visant à déployer les compétences numériques. À cet effet, il renforcerait les capacités en cybersécurité au niveau de l'UE et s'appuierait sur des synergies, notamment avec l'ENISA, la CERT-EU, Europol, l'éventuel futur Fonds d'intervention pour les urgences de cybersécurité et les centres nationaux de réponses aux urgences informatiques (CSIRT).

L'un des points sur lesquels les travaux du réseau de compétence doivent mettre l'accent est le manque de capacités européennes en matière de **cryptage** des produits et des services utilisés par les citoyens, les entreprises et les administrations au sein du marché unique numérique. Un cryptage fort est essentiel pour disposer de systèmes d'identification numérique sûrs qui jouent un rôle clé dans la cybersécurité[47]. Il permet également d'assurer la sécurité de la propriété intellectuelle, protège les droits fondamentaux comme la liberté d'expression et la protection des données à caractère personnel et garantit la sécurité du commerce en ligne[48].

Étant donné que les marchés de la cybersécurité civils et militaires de l'UE font face à des défis communs[49] et partagent une technologie à double usage qui nécessite une étroite collaboration dans des domaines critiques, une deuxième phase permettra de compléter le réseau et son centre en y ajoutant une dimension «cyberdéfense», dans le strict respect des dispositions du traité liées à la politique de sécurité et de défense commune. En plus de son axe technologique, cette dimension pourrait contribuer à la coopération entre les États membres dans le domaine de la cyberdéfense, notamment par le partage d'informations, la conscience situationnelle, le renforcement de l'expertise et des réactions coordonnées, et par le soutien au développement de capacités communes aux États membres. Elle pourrait également servir de plateforme permettant aux États membres de définir les priorités de l'UE

[46] COM(2012) 45 final et COM(2016) 178 final.

[47] La Commission lancera d'ores et déjà, dans le cadre d'Horizon 2020, un nouveau prix Horizon Défi qui octroiera 4 millions d'EUR à la meilleure solution innovante parmi les méthodes d'authentification en ligne.

[48] Cybersecurity in the European Digital Single Market, High level group of Scientific Advisors, March 2017.

[49] "Study on synergies between the civilian and the defence cybersecurity markets"(Optimity; SMART 2014-0059).

en matière de cyberdéfense, de rechercher des solutions communes, de contribuer à l'élaboration de stratégies communes, de faciliter la formation et la réalisation d'exercices et d'essais en cyberdéfense de manière conjointe au niveau européen, et de soutenir les travaux effectués en matière de taxonomie et de normalisation en cyberdéfense, le centre jouant un rôle consultatif et d'appui. Pour mener à bien toutes ces activités, le centre devrait travailler en étroite collaboration et en pleine complémentarité avec l'Agence européenne de défense dans le domaine de la cyberdéfense, ainsi qu'avec l'ENISA dans le domaine de la cyber-résilience. Cette dimension Défense tiendrait compte du processus initié dans le document de réflexion de la Commission sur l'avenir de la défense européenne.

Le haut niveau de résilience requis en matière de cyberdéfense nécessite un ciblage spécifique des efforts en matière de recherche et de technologie. Les projets et technologies développés par des entreprises dans le domaine de la cyberdéfense pourraient bénéficier de financements du Fonds européen de la défense pour la phase tant de recherche que de développement[50]. Des domaines spécifiques tels que les systèmes de cryptage des systèmes basés sur les technologies quantiques, la conscience situationnelle de la cybersécurité, les systèmes biométriques de contrôle des accès, la détection avancée des menaces persistantes, ou l'exploration de données pourraient être particulièrement pertinents dans ce contexte. La haute représentante, l'Agence européenne de la défense et la Commission aideront les États membres à identifier les domaines dans lesquels des projets communs de cybersécurité pourraient faire l'objet d'un financement par le Fonds européen de la défense.

2.6 Établir une solide base de cyber-compétences européenne

Une cybersécurité efficace repose largement sur les compétences des personnes concernées. C'est pourquoi l'éducation à la cybersécurité est une nécessité. Cependant, le déficit en compétences en cybersécurité chez les professionnels travaillant dans le secteur privé en Europe est estimé à 350 000 d'ici à 2022[51]. L'éducation à la cybersécurité devrait être renforcée à tous les niveaux, aussi bien dans le cadre de la formation ordinaire des employés dans le domaine de l'informatique que de la formation complémentaire à la cybersécurité destinée à tous les spécialistes des TIC ou dans les nouveaux cursus spécifiques liés à la cybersécurité. Des centres de compétences bien dotés devraient être mis sur pied dans les universités pour répondre aux besoins d'éducation et de formation accélérées et pourraient s'appuyer sur les conseils d'un centre européen de compétences et de recherche en cybersécurité et de l'ENISA. L'objectif serait qu'il devienne naturel de concevoir des systèmes et des produits TIC qui intègrent dès le départ les principes de sécurité. L'éducation à la cybersécurité ne devrait pas être limitée aux professionnels des technologies de l'information. L'informatique devrait faire partie des cursus d'autres domaines, comme l'ingénierie, la gestion d'entreprise ou le droit, ainsi que des filières de formation sectorielles. Enfin, les enseignants et les élèves de l'éducation primaire et secondaire devraient être sensibilisés à la cybercriminalité et à la cybersécurité lorsqu'ils transmettent ou acquièrent des compétences numériques à l'école.

L'Union européenne devrait également, avec les États membres, apporter une contribution à ces travaux en s'appuyant sur les activités de la grande coalition en faveur des compétences et

[50] Le programme européen de développement industriel dans le domaine de la défense donne d'ores et déjà la priorité aux projets de cyberdéfense, et la cyberdéfense sera l'un des thèmes de l'appel à propositions qui sera publié en 2018.

[51] Global Information Security Workforce Study 2017. Au niveau mondial, ce manque est quantifié à 1,8 million.

des emplois[52] et en mettant par exemple en place des programmes d'apprentissages en cybersécurité destinés aux PME.

2.7 Promouvoir une hygiène et une sensibilisation à la cybersécurité

95 % des incidents étant réputés avoir été le résultat d'«une forme ou d'une autre d'erreur sur le plan humain, qu'elle soit intentionnelle ou non»[53], il est évident que le facteur humain est en cause. C'est pourquoi la cybersécurité est l'affaire de tous. Cela signifie que le comportement des particuliers, des entreprises et des administrations publiques doit changer afin de veiller à ce que chacun comprenne la menace et soit équipé des outils et des compétences nécessaires pour détecter rapidement les attaques et s'en protéger activement. Nous devons adopter des habitudes de cyber-hygiène et les entreprises et les organisations doivent adopter des programmes appropriés en matière de cybersécurité fondés sur le risque et les mettre à jour régulièrement pour qu'ils correspondent à la situation actuelle en termes de risque, qui évolue constamment.

La directive SRI définit les responsabilités des États membres, qui sont tenus non seulement d'échanger des informations concernant les cyberattaques au niveau de l'UE mais aussi de mettre en place au niveau national des stratégies en cybersécurité et des cadres pour la sécurité des réseaux et des systèmes d'information, qui soient éprouvés. Les administrations publiques au niveau national et de l'Union devraient jouer un rôle moteur en ce sens.

Premièrement, les États membres devraient étendre autant que possible la disponibilité d'outils en matière de cybersécurité pour les entreprises et les particuliers. Ils devraient notamment redoubler d'efforts pour prévenir et atténuer les effets de la cybercriminalité sur les utilisateurs finaux. À titre d'exemple, Europol a lancé une campagne intitulée «NoMoreRansom»[54], organisée grâce à l'étroite collaboration entre les services répressifs et des entreprises de cybersécurité afin d'aider les utilisateurs s à prévenir les infections causées par des rançongiciels et à décrypter les données lorsqu'elles sont victimes d'une attaque. Des initiatives similaires devraient être mises en place pour d'autres types de logiciels malveillants dans d'autres domaines, et l'UE devrait mettre en place un **portail unique réunissant tous les instruments de ce type au sein d'un guichet unique**, qui proposerait des conseils aux utilisateurs en matière de prévention et de détection des logiciels malveillants et comporterait des liens vers des mécanismes d'alerte.

Deuxièmement, les États membres devraient accélérer l'**utilisation d'un plus grand nombre de cyber-instruments pour le développement de l'administration en ligne** et tirer pleinement parti du réseau de compétences. L'adoption de moyens d'authentification sûrs devrait être encouragée, en s'appuyant sur le cadre réglementaire de l'UE pour l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, qui est en vigueur depuis 2016 et fournit un environnement réglementaire prévisible qui permettra d'assurer des transactions électroniques sûres et sans discontinuité entre les entreprises, les particuliers et les pouvoirs publics[55]. Par ailleurs, les institutions publiques, et

---

52 https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition.

53 IBM, «The Cybersecurity Intelligence Index» 2014, cité dans Securitymagazine.com, 19 juin 2014.

54 https://www.nomoreransom.org/.

55 Règlement (UE) nº 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (règlement eIDAS), adopté le 23 juillet 2014. En outre, la Commission européenne fournit des éléments constitutifs et des outils pour l'interopérabilité de la signature électronique et l'identification électronique (comme Trusted List Browser), par l'intermédiaire du mécanisme pour l'interconnexion en Europe.

en particulier celles qui fournissent des services de base, devraient veiller à ce que leur personnel soit formé dans les domaines liés à la cybersécurité.

Troisièmement, les États membres devraient faire de la sensibilisation à la cybersécurité une priorité grâce à des **campagnes de sensibilisation**, qui cibleraient notamment les écoles, les universités, les entreprises et les organismes de recherche. Le mois de la cybersécurité qui a lieu chaque année en octobre sous l'égide de l'ENISA sera amplifié afin d'accroître la portée de cet effort de communication au niveau national et de l'UE. La sensibilisation à l'existence en ligne de **campagnes de désinformation et de fausses informations** sur les réseaux sociaux visant en particulier à affaiblir les processus démocratiques et les valeurs européennes est tout aussi importante. Si la responsabilité en revient principalement au niveau national – y compris en lien avec les élections au Parlement européen – la mise en commun d'expertises et le partage d'expériences au niveau européen se sont avérés être une valeur ajoutée permettant de mieux cibler les actions.[56].

D'une manière générale, l'**industrie** a un rôle important à jouer, et tout particulièrement les fabricants et les fournisseurs de services numériques. Il s'agit d'apporter un soutien aux utilisateurs (particuliers, entreprises et administrations publiques) grâce à des outils qui leur permettent d'agir en ligne de manière responsable, en faisant clairement comprendre qu'entretenir une cyber-hygiène constitue un élément indispensable de l'offre proposée aux consommateurs[57]. Pour détecter les points vulnérables et y remédier, l'industrie devrait s'efforcer de se doter de procédures internes pour mener des enquêtes, faire le tri et corriger ces vulnérabilités, que la source de cette vulnérabilité potentielle soit externe ou interne à l'entreprise concernée.

Actions clés

- Mise en œuvre intégrale de la directive relative à la sécurité des réseaux et des systèmes d'information;
- Adoption rapide par le Parlement européen et le Conseil du règlement définissant un nouveau mandat pour l'ENISA et un cadre européen de certification[58];
- Une initiative conjointe entre la Commission et l'industrie pour définir un principe de «devoir de vigilance» afin de réduire les vulnérabilités des produits et logiciels et de promouvoir la «sécurité dès la conception»;
- Mise en œuvre rapide du cadre de réponse aux incidents transfrontières majeurs;
- Lancement d'une analyse d'impact afin d'étudier la possibilité pour la Commission de proposer en 2018 la mise en place d'un réseau de centres de compétence en matière de cybersécurité et d'un centre européen de recherche et de compétences en cybersécurité, sur la base d'une étape pilote prenant débutant immédiatement;
- Soutien aux États membres dans la détermination des domaines dans lesquels des projets communs en cybersécurité seraient susceptibles de recevoir un soutien du Fonds européen de la défense;
- Un guichet unique en niveau de l'Union destiné aux victimes de cyberattaques, qui leur

[56] À titre d'exemple, l'équipe de East StratCom Task Force a été créée en 2015 par les États membres et la haute représentante de l'Union pour faire face aux campagnes de désinformation véhiculées par la Russie. Elle met au point des campagnes et des produits de communication dont le but est d'expliquer les politiques de l'UE dans la région du partenariat oriental.

[57] Certains produits relèvent déjà cette approche, car certains textes législatifs européens applicable aux produits (tels que la directive 2006/42/CE relatives aux machines) énoncent des principes de «sécurité dès la conception».

[58] COM(2017) 477.

proposent des informations sur les menaces les plus récentes ainsi que des conseils pratiques et des outils de cybersécurité;
- Des mesures par les États membres visant à intégrer la cybersécurité dans les programmes d'acquisition des compétences, l'administration en ligne et les campagnes de sensibilisation;
- Des mesures par l'industrie pour améliorer la formation en matière de cybersécurité dispensée aux employés et adopter l'approche de «sécurité dès la conception» pour leurs produits, leurs services et leurs procédures.

3. CRÉER UNE CYBERDISSUASION EUROPÉENNE EFFICACE

Une dissuasion efficace implique la mise en place d'un cadre de mesures qui soient à la fois crédibles et dissuasives pour les cybercriminels et attaquants en puissance. Tant que les auteurs de cyberattaques, qu'ils agissent ou non pour un État , n'ont rien à craindre hormis l'échec, ceux-ci ont peu de raisons d'arrêter leurs tentatives. Une réponse policière plus percutante, axée sur la détection, la traçabilité et la poursuite des cybercriminels, est indispensable à l'établissement d'une dissuasion efficace. Il est en outre nécessaire que l'Union aide ses États membres à développer des capacités à double usage dans le domaine de la cybersécurité. Nous ne pourrons commencer à inverser la tendance en matière de cyberattaques qu'en augmentant les risques pour leurs auteurs d'être appréhendés et sanctionnés. Les cyberattaques doivent faire promptement l'objet d'enquêtes; il convient de traduire leurs auteurs en justice ou de prendre des mesures pour permettre d'apporter une réponse politique ou diplomatique appropriée. En cas de crise majeure ayant une importante dimension sur le plan international et de la défense, la haute représentante pourrait proposer des réponses appropriées au Conseil.

L'adoption, en 2013, de la directive relative aux attaques contre les systèmes d'information[59] a déjà permis de franchir une étape vers l'amélioration des réponses pénales aux cyberattaques. Cette directive établit des règles minimales concernant la définition des infractions pénales et des sanctions en matière d'attaques contre les systèmes d'information et prévoit des mesures opérationnelles pour renforcer la coopération entre les autorités. Elle a permis d'accomplir des progrès substantiels en matière de criminalisation des cyberattaques à un niveau comparable dans tous les États membres, ce qui facilite la coopération transfrontière entre les autorités répressives qui enquêtent sur ces types d'infractions. Toutefois, il est encore possible d'agir pour que la directive atteigne son plein potentiel par une application intégrale de toutes les dispositions par les États membres[60]. La Commission continuera de soutenir les États membres dans la mise en œuvre de la directive et ne voit pas, pour le moment, la nécessité de proposer des modifications à celle-ci.

3.1 Identifier les acteurs malveillants

Afin de renforcer nos chances de traduire les auteurs de cyberattaques devant la justice, nous devons, de toute urgence, améliorer notre capacité à identifier les responsables de ces actes. La découverte d'informations utiles pour les enquêtes sur la cybercriminalité, principalement sous la forme de traces numériques, constitue un défi majeur pour les autorités répressives. Nous devons donc améliorer nos capacités technologiques pour enquêter efficacement, notamment en renforçant l'unité de lutte contre la cybercriminalité d'Europol avec des experts

[59] Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information.
[60] COM(2017) 474.

dans ce domaine. Europol est devenu un acteur clé pour aider les États membres dans les enquêtes relevant de plusieurs juridications nationales. Il doit devenir un centre de compétences en matière d'enquêtes en ligne et de cybercriminalistique pour les autorités répressives des États membres.

En raison de la pratique répandue qui consiste à connecter de nombreux utilisateurs (parfois des milliers) derrière une adresse IP, il est techniquement très difficile d'enquêter sur les comportements malveillants en ligne. Cette pratique oblige parfois à enquêter sur un grand nombre d'utilisateurs afin d'identifier un acteur malveillant, par exemple en cas d'infractions graves telles que la pédopornographie. L'UE encouragera donc l'adoption du nouveau protocole internet (IPv6) car il permet d'attribuer une adresse IP unique à chaque utilisateur, ce qui présente des avantages évidents en matière de répression et d'enquêtes sur la cybersécurité. Dans un premier temps, afin de favoriser son adoption, la Commission intégrera l'obligation de passer à l'IPv6 dans l'ensemble de ses politiques, en prévoyant des exigences pour les marchés publics, ainsi que pour le financement de projets et de la recherche, et en finançant le matériel de formation nécessaire. En outre, les États membres devraient envisager des accords volontaires avec les fournisseurs de service internet pour encourager l'adoption du protocole IPv6.

La Belgique enregistre le plus fort taux d'adoption du protocole IPv6 au monde[61]*, grâce notamment à une coopération entre le secteur public et le secteur privé: les parties prenantes concernées ont envisagé de limiter l'utilisation d'une adresse IP à un maximum de 16 utilisateurs dans le cadre d'une mesure volontaire d'autorégulation, ce qui a encouragé la transition vers l'IPv6*[62].

D'une manière plus générale, il convient de promouvoir davantage la responsabilité en ligne. Il faut pour cela favoriser les mesures visant à empêcher l'utilisation frauduleuse de noms de domaines dans l'intention de propager des messages non sollicités ou des attaques par hameçonnage. À cette fin, la Commission s'emploiera à améliorer le fonctionnement, la disponibilité et l'exactitude des informations contenues dans les systèmes WHOIS[63] relatifs aux noms de domaines et aux adresses IP, parallèlement aux efforts déployés par l'Internet Corporation for Assigned Names and Numbers[64].

3.2 Renforcer la répression

L'efficacité des **enquêtes** et des **poursuites** en matière de criminalité facilitée par les technologies de l'information et de la communication est un élément dissuasif fort contre les cyberattaques. Il convient toutefois d'adapter le cadre procédural actuel à l'ère de l'internet[65]. Nos procédures sont dépassées par la rapidité des cyberattaques et de nouveaux besoins apparaissent pour une coopération rapide par-delà les frontières. À cette fin, comme annoncé

---

61 https://www.google.com/intl/fr/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption.

62 http://bipt.be/public/files/nl/22027/Raadpleging_ipv6.pdf.

63 Protocole de questions et de réponses largement utilisé pour interroger des bases de données où sont conservées des informations sur les utilisateurs enregistrés ou autres intervenants auxquels est assignée une ressource internet.

64 L'Internet Corporation for Assigned Names and Numbers (ICANN) est une organisation à but non lucratif chargée de coordonner la maintenance et les procédures de plusieurs bases de données relatives aux espaces de noms de l'internet.

65 Pour ne citer qu'un exemple, le serveur (virtuel) central de commandement et de contrôle du réseau zombie Avalanche changeait de serveurs physiques et de domaines toutes les cinq minutes.

dans le programme européen en matière de sécurité, la Commission présentera, au début de 2018, des propositions visant à **faciliter l'accès transfrontière aux preuves électroniques**. Dans le même temps, la Commission mettra en œuvre des mesures concrètes visant à améliorer l'accès transfrontière aux preuves électroniques dans les enquêtes pénales, notamment en finançant la formation en matière de coopération transfrontière, en élaborant une plateforme électronique pour l'échange d'informations au sein de l'UE et en standardisant les formes de coopération judiciaire utilisées entre les États membres.

Les différences dans les procédures de police scientifique pour la collecte de preuves électroniques liées aux enquêtes sur la cybercriminalité menées dans les États membres constituent un autre obstacle à l'efficacité des poursuites. Cette difficulté pourrait être atténuée en œuvrant à l'instauration de normes de police scientifique communes. En outre, il est nécessaire de renforcer les capacités de police scientifique pour pouvoir mieux retracer les infractions et les imputer à leurs auteurs. Une première étape consisterait à développer des capacités de police scientifique au sein d'Europol, en adaptant les ressources budgétaires et humaines existantes du centre européen de lutte contre la cybercriminalité d'Europol pour répondre aux besoins de plus en plus pressants de soutien opérationnel lors des enquêtes cybercriminelles transfrontières. Une autre possibilité consisterait à reprendre l'axe technologique décrit plus haut pour le cryptage en examinant comment son utilisation abusive par les criminels pose d'importants problèmes dans le cadre de la lutte contre les formes graves de criminalité, y compris le terrorisme et la cybercriminalité. La Commission présentera les résultats des réflexions actuelles sur le **rôle du cryptage dans les enquêtes pénales**[66], d'ici octobre 2017[67].

Étant donné la nature sans frontière de l'internet, le cadre de coopération internationale prévu par la convention sur la cybercriminalité du Conseil de l'Europe[68] (la **convention de Budapest**) offre la possibilité à différents pays d'appliquer la norme juridique la plus favorable pour les différentes législations nationales en matière de lutte contre la cybercriminalité. Il est actuellement question d'ajouter un protocole à la convention[69], ce qui permettrait également d'examiner la question de l'accès transfrontière aux preuves électroniques dans un contexte international. Plutôt que de créer de nouveaux instruments juridiques internationaux pour les questions de cybercriminalité, l'UE appelle tous les pays à élaborer une législation nationale appropriée et à poursuivre la coopération dans le cadre international existant.

L'accès généralisé aux outils d'anonymisation permet aux criminels de se cacher plus facilement. Le ***«darknet»***[70] a ouvert aux criminels de nouvelles voies d'accès à des documents pédopornographiques, à des drogues ou à des armes à feu, en courant souvent peu

---

66 Présidence du Conseil, Résultats de la session du Conseil «Justice et affaires intérieures» des 8 et 9 décembre 2016, n° 15391/16.

67 Huitième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, COM(2017) 354 final, du 29 juin 2017.

68 La convention est le premier traité international consacré aux infractions commises via l'internet et d'autres réseaux informatiques; elle s'attaque en particulier aux infractions aux droits d'auteur, à la fraude informatique, à la pédopornographie et aux violations de la sécurité des réseaux: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185?_coeconventions_WAR_coeconventionsportlet_languageId=fr_FR. En 2017, 55 gouvernements ont ratifié la convention sur la cybercriminalité du Conseil de l'Europe ou y ont adhéré.

69 Mandat pour la préparation d'un projet de 2e protocole additionnel à la convention de Budapest, T-CY (2017)3.

70 Le darknet est constitué de contenu dans des réseaux superposés qui utilisent l'internet mais ont recours à des logiciels, des configurations ou des autorisations d'accès spécifiques. Le darknet forme une petite partie du web invisible («*deep web*»), la partie du web qui n'est pas indexée par les moteurs de recherche.

de risques d'être pris[71]. Il est également devenu une source essentielle d'instruments cybercriminels tels que les logiciels malveillants et les outils de piratage. La Commission, en collaboration avec les acteurs concernés, analysera les approches nationales en vue de dégager de nouvelles solutions. Europol devrait faciliter et soutenir les enquêtes sur le darknet, évaluer les menaces, aider à déterminer la compétence judiciaire et donner la priorité aux cas à haut risque , et l'Europe peut jouer un rôle de chef de file dans la coordination de l'action internationale[72].

L'utilisation frauduleuse des données des cartes de crédit ou d'autres moyens de paiement électroniques constitue une activité criminelle en plein essor. Les criminels lancent des cyberattaques contre des sites de vente en ligne ou d'autres entreprises légales afin de dérober les références de paiements. Ils les vendent ensuite en ligne à des criminels, qui peuvent les utiliser pour commettre des fraudes[73]. La Commission présente une proposition visant à renforcer la dissuasion au moyen d'une **directive concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces**[74]. Cette directive vise à mettre à jour les règles existantes dans ce domaine et à renforcer les capacités des services répressifs dans la lutte contre cette forme de criminalité.

Les capacités d'enquête cybercriminelle des services répressifs des États membres doivent également être améliorées, et les procureurs et le monde judiciaire doivent parfaire leur compréhension de la criminalité facilitée par les technologies de l'information et de la communication ainsi que les possibilités d'enquête. Eurojust et Europol contribuent à cet objectif et au renforcement de la coordination, en collaboration étroite avec les groupes consultatifs spécialisés du centre européen de lutte contre la cybercriminalité d'Europol, ainsi qu'avec le réseau des chefs des unités spécialisées en cybercriminalité et le réseau des procureurs spécialisés dans la cybercriminalité. La Commission consacrera 10,5 millions d'euros à la lutte contre la cybercriminalité, principalement au titre de l'**instrument de soutien à la police du Fonds pour la sécurité intérieure**. La formation est un élément important et le groupe européen de formation et d'enseignement sur la cybercriminalité (ECTEG) a élaboré plusieurs outils utiles en la matière. Il conviendrait à présent de les diffuser largement auprès des professionnels des services répressifs, avec le soutien de l'Agence de l'Union européenne pour la formation des services répressifs (CEPOL).

3.3 La coopération public-privé contre la cybercriminalité

L'efficacité des mécanismes répressifs traditionnels est remise en cause par les caractéristiques du monde numérique, qui se compose pour l'essentiel d'infrastructures privées et d'une multitude d'acteurs qui relèvent de juridictions différentes. Dès lors, la coopération avec le secteur privé, notamment les entreprises et la société civile, est indispensable pour que les pouvoirs publics puissent lutter efficacement contre la criminalité. Dans ce contexte, le secteur financier est également déterminant et la coopération avec ce

---

[71] Le démantèlement récent de deux marchés très importants du web sombre, AlphaBay et Hansa, constitue une exception notable: Https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation (en anglais uniquement).

[72] Europol joue déjà un rôle majeur dans ce domaine. Voir, à titre d'exemple récent: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation (en anglais uniquement).

[73] Les produits de la fraude sont une source de revenus importante pour la criminalité organisée et constituent par conséquent un catalyseur pour d'autres activités criminelles telles que le terrorisme, le trafic de drogues et la traite des êtres humains.

[74] COM(2017) 489.

dernier devrait être renforcée. Par exemple, il conviendrait de conforter le rôle des cellules de renseignement financier[75] (CRF) dans la lutte contre la cybercriminalité.

*Certains États membres ont déjà pris des mesures marquantes. Aux Pays-Bas, les établissements financiers et les services répressifs travaillent main dans la main pour traquer la fraude en ligne et les cybercriminels au sein d'une équipe spéciale de lutte contre la criminalité électronique (*Electronic Crime Task Force*). Le centre de compétence allemand contre la cybercriminalité (*German Competence Centre against Cyber Crime*) fournit la plateforme opérationnelle qui permet à ses membres d'échanger des informations en collaboration étroite avec l'Office fédéral de police criminelle et d'élaborer des mesures visant à garantir la protection contre la cybercriminalité. Seize États membres[76] ont créé des centres d'excellence de lutte contre la cybercriminalité, afin de faciliter la coopération entre les autorités répressives, le milieu universitaire et les partenaires privés pour élaborer et échanger de bonnes pratiques, et pour renforcer la formation et les capacités.*
*La Commission soutient la mise en place de partenariats et de mécanismes de coopération public-privé à travers des projets ciblés tels que le réseau d'experts en cybersécurité et centre de lutte contre la fraude en ligne (*Online Fraud Cyber Centre and Experts Network*, OF2CEN)[77], et la mise en œuvre du modèle et de la norme de partage des informations afin d'analyser et d'atténuer les risques des crimes électroniques et la fraude en ligne.*

Dans la lutte contre la cybercriminalité, les entreprises privées doivent être en mesure de partager les informations sur les incidents concrets avec les services répressifs, y compris les données à caractère personnel, dans le respect intégral des règles en matière de protection des données. La réforme de la protection des données de l'UE, qui entrera en vigueur en mai 2018, définit un ensemble de règles communes fixant les conditions dans lesquelles les autorités répressives et les entités privées peuvent coopérer. La Commission européenne collaborera avec le comité européen de la protection des données et les parties prenantes concernées afin de recenser les bonnes pratiques dans ce domaine et, le cas échéant, de formuler des orientations.

3.4 Renforcer la réaction politique

Le **cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance**[78] (la «boîte à outils cyberdiplomatique»), adopté récemment, définit les mesures relevant de la politique étrangère et de sécurité commune, et notamment les mesures restrictives, qui peuvent être utilisées pour renforcer la réaction de l'UE aux activités qui portent atteinte à ses intérêts politiques, sécuritaires et économiques. Ce cadre constitue une étape importante dans le renforcement des capacités de signalement et de réaction au niveau de l'UE et des États membres. Il renforcera notre capacité à imputer les activités informatiques malveillantes à leurs auteurs, afin d'influencer le comportement des agresseurs potentiels, tout en tenant compte de la nécessité de veiller à apporter des réponses

[75] Les cellules de renseignement financier servent de centres nationaux pour la réception et l'analyse des déclarations de transactions suspectes ainsi que des autres informations relatives au blanchiment de capitaux, aux infractions sous-jacentes associées et au financement du terrorisme. Elles diffusent également les résultats de cette analyse.

[76] L'Allemagne, l'Autriche, la Belgique, la Bulgarie, Chypre, l'Espagne, l'Estonie, la France, la Grèce, l'Irlande, la Lituanie, la Pologne, la République tchèque, la Roumanie, le Royaume-Uni et la Slovénie.

[77] L'initiative OF2CEN vise à permettre le partage systématique à l'échelle de l'UE des informations relatives aux fraudes sur l'internet entre les banques et les services répressifs, afin d'empêcher les paiements aux fraudeurs et aux passeurs d'argent, et de favoriser les enquêtes sur les auteurs d'infractions et leur poursuite. Elle est cofinancée par l'UE (instrument de soutien à la police du Fonds pour la sécurité intérieure).

[78] http://www.consilium.europa.eu/fr/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/.

proportionnées. L'imputation d'une activité malveillante à un acteur étatique ou non étatique reste une décision politique souveraine fondée sur des renseignements provenant de toutes sources. Les travaux de mise en œuvre du cadre sont en cours avec les États membres. Ils devraient avancer conjointement avec le plan d'action («*Blueprint*») pour répondre aux incidents informatiques à grande échelle[79]. L'appréciation de la situation nécessaire à l'utilisation de mesures au titre du cadre devrait être fusionnée, analysée et partagée par le SITCEN[80], en étroite collaboration avec les États membres et les institutions de l'UE.

3.5 Renforcer la dissuasion en matière de cybersécurité grâce aux capacités de défense des États membres

Les États membres mettent déjà en place des capacités de cyberdéfense. Vu l'interpénétration des domaines de la cyberdéfense et de la cybersécurité et le caractère à double usage (civil et militaire) des cyberoutils et des cybertechnologies, et compte tenu de la grande diversité des approches des États membres, l'UE est en outre bien placée pour favoriser les synergies entre les efforts militaires et civils[81].

Les États membres dont les capacités de cybersécurité sont les plus avancées et qui seraient désireux de les réunir avec d'autres pourraient envisager, avec le soutien du Haut Représentant, de la Commission et de l'Agence européenne de défense, d'intégrer la cybersécurité dans une «coopération structurée permanente» (CSP). Un tel projet pourrait s'inspirer des travaux exposés ci-dessus, afin d'encourager les capacités industrielles et l'autonomie stratégique de l'Union européenne. L'UE peut également favoriser l'interopérabilité, y compris en facilitant le renforcement des capacités, la coordination de la formation et de l'éducation, et les efforts de standardisation des biens et des technologies à double usage.

Il convient également d'exploiter pleinement le cadre commun existant pour répondre aux menaces hybrides, qui impliquent souvent des cyberattaques, notamment la cellule de fusion de l'UE contre les menaces hybrides et le centre européen de lutte contre les menaces hybrides, établi récemment à Helsinki, dont la mission est d'encourager le dialogue stratégique et de mener des travaux de recherche et d'analyse.

L'UE donnera une nouvelle impulsion au cadre stratégique de cyberdéfense de 2014[82], en tant qu'outil pour poursuivre l'intégration de la cybersécurité et de la défense dans la politique de sécurité et de défense commune (PSDC). La cyber-résilience des missions et des opérations de la PSDC elles-mêmes est essentielle: des procédures normalisées et des capacités techniques seront mises en place, qui pourront soutenir le déploiement de missions et d'opérations civiles comme militaires, ainsi que leurs structures respectives de capacités de planification et de conduite et les prestataires de services informatiques du SEAE. Afin de faire progresser la coopération entre les États membres et de mieux orienter les efforts de l'UE dans ce domaine, l'Agence européenne de défense et le SEAE, en coopération avec les services de la Commission, favoriseront la participation au niveau stratégique des décideurs politiques des différents États membres en matière de cyberdéfense. L'UE soutiendra également la mise en place de solutions européennes en matière de cybersécurité dans le cadre de ses efforts en faveur d'une base industrielle et technologique de défense européenne, ce qui

---

79 C(2017) 6100.

80 JOIN(2016) 018 final.

81 L'UE considère le cyberespace comme un nouveau domaine d'opérations, après les domaines terrestre, aérien et maritime. Les efforts déployés dans le domaine de la cyberdéfense s'étendent également à la protection et à la résilience des moyens spatiaux et des infrastructures correspondantes au sol.

82 www.consilium.europa.eu/en/workarea/downloadasset.aspx?id=40802190515.

inclut aussi la promotion de pôles régionaux d'excellence en matière de cybersécurité et de défense.

Les services de la Commission, en étroite coopération avec le SEAE, les États membres et les autres organes pertinents de l'UE, mettront en place d'ici à 2018 une **plateforme de formation et d'enseignement en matière de cyberdéfense** visant à combler le manque actuel de compétences dans le domaine de la cyberdéfense. Cette démarche complétera les travaux menés par l'Agence européenne de défense dans ce domaine en vue de résoudre le déficit actuel de compétences en matière de cybersécurité et de cyberdéfense.

Actions clés

- Une initiative de la Commission pour améliorer l'accès transfrontière aux preuves électroniques (début 2018).
- L'adoption rapide par le Parlement européen et par le Conseil de la proposition de directive concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces.
- L'introduction de clauses imposant le protocole IPv6 dans les marchés publics et le financement des projets et de la recherche de l'UE; la conclusion d'accords volontaires entre les États membres et les fournisseurs de service internet pour stimuler l'adoption du protocole IPv6.
- Une attention renouvelée et renforcée d'Europol à la cybercriminalistique et à la surveillance du darknet.
- La mise en œuvre du cadre pour une réponse diplomatique conjointe de l'UE aux actes de cybermalveillance.
- L'accroissement du soutien financier accordé à des projets nationaux et transnationaux destinés à améliorer la justice pénale dans le cyberespace.
- La mise en place en 2018 d'une plateforme de formation en lien avec la cybersécurité visant à remédier à l'actuel déficit de compétences en matière de cybersécurité et de cyberdéfense.

4. RENFORCER LA COOPÉRATION INTERNATIONALE EN MATIÈRE DE CYBERSÉCURITÉ

Guidée par les valeurs essentielles de l'UE et les droits fondamentaux tels que la liberté d'expression et le droit à la vie privée et à la protection des données à caractère personnel, ainsi que la promotion d'un cyberespace ouvert, libre et sûr, la politique internationale de l'UE en matière de cybersécurité est conçue pour relever le défi en constante évolution qui consiste à promouvoir la cyberstabilité mondiale et à contribuer à l'autonomie stratégique de l'Europe dans le cyberespace.

4.1 La cybersécurité dans les relations extérieures

Une étude montre que partout dans le monde, les citoyens considèrent que les cyberattaques menées depuis d'autres pays constituent l'une des principales menaces pour la sécurité nationale[83]. Compte tenu de la nature mondialisée de la menace, il est capital de nouer et d'entretenir des alliances et des partenariats solides avec les pays tiers pour la prévention et la dissuasion des cyberattaques, qui sont de plus en plus importants pour la stabilité et la sécurité internationales. L'UE accordera la priorité à la mise en place d'un cadre stratégique pour la

[83] *Spring 2017 Global Attitudes Survey*, Pew Research Center.

prévention des conflits et la stabilité dans le cyberespace dans ses engagements bilatéraux, régionaux, multipartites et multilatéraux.

L'UE soutient fermement la position selon laquelle le droit international, et en particulier la Charte des Nations unies, est applicable au cyberespace. En complément du droit international contraignant, l'UE approuve les normes, les règles et les principes volontaires non contraignants sur le comportement responsable des États, qui ont été formulés par le groupe d'experts gouvernementaux des Nations unies[84]; elle encourage également l'élaboration et la mise en œuvre de mesures régionales de renforcement de la confiance, tant au sein de l'Organisation pour la sécurité et la coopération en Europe que dans d'autres régions du monde.

Au niveau bilatéral, les cyberdialogues[85] seront renforcés et complétés par des efforts visant à faciliter la coopération avec les pays tiers afin de renforcer les principes de diligence raisonnable et de responsabilité des États dans le cyberespace. L'UE accordera la priorité aux questions de sécurité internationale dans le cyberespace dans ses engagements internationaux, tout en veillant à ce que la question de la cybersécurité ne devienne pas un prétexte au protectionnisme des marchés et à la limitation des libertés et des droits fondamentaux, y compris la liberté d'expression et l'accès à l'information. Une approche globale de la cybersécurité impose le respect des droits de l'homme, et l'UE continuera à défendre ses valeurs fondamentales à l'échelle mondiale, en s'appuyant sur les orientations de l'UE en matière de droits de l'homme relatives à la liberté en ligne[86]. À cet égard, l'UE souligne qu'il est important que toutes les parties prenantes participent à la gouvernance de l'internet.

La Commission a également présenté une proposition[87] de modernisation des contrôles à l'exportation de l'UE, en introduisant notamment des contrôles sur les exportations de technologies critiques de cybersurveillance qui pourraient entraîner des violations des droits de l'homme ou être utilisées pour nuire à la sécurité de l'UE. Elle renforcera également les dialogues avec les pays tiers pour promouvoir une convergence mondiale et un comportement responsable dans ce domaine.

4.2 Renforcement des capacités en matière de cybersécurité

La cyberstabilité mondiale repose sur la capacité locale et nationale de l'ensemble des pays à prévenir les cyberincidents et à y faire face, ainsi qu'à mener des enquêtes et à engager des poursuites dans les dossiers de cybercriminalité. En soutenant les efforts visant à instaurer une résilience nationale dans les pays tiers, on contribuera à améliorer le niveau de cybersécurité à l'échelle mondiale, ce qui aura des retombées positives pour l'Union. La lutte contre des cybermenaces en évolution rapide exigera selon toute logique de déployer des efforts en matière de formation, de stratégie et de législation, ainsi que de mettre en place, dans tous les pays, des équipes d'intervention en cas d'urgence informatique et des unités spécialisées en cybercriminalité opérant de façon efficace.

Depuis 2013, l'UE est à la pointe de l'action en faveur du renforcement des capacités en matière de cybersécurité au niveau international. Dans ce cadre, elle veille à établir systématiquement un lien entre ces efforts et son action dans le domaine de la coopération au développement. L'UE continuera à promouvoir un modèle de renforcement des capacités qui

---

[84] A/68/98 et A/70/174.

[85] En septembre 2017, l'UE a mené des cyberdialogues avec les États-Unis, la Chine, le Japon, la République de Corée et l'Inde.

[86] Orientations de l'UE en matière de droits de l'homme relatives à la liberté d'expression en ligne et hors ligne.

[87] COM(2016) 616.

soit fondé sur les droits et conforme à l'approche Digital4Development[88]. Les priorités en matière de renforcement des capacités seront les pays du voisinage européen et les pays en développement qui connaissent une évolution rapide à la fois de la connectivité et des menaces. Les efforts de l'Union dans ce domaine viendront compléter ceux qu'elle déploie dans le cadre de son programme de développement, à la lumière du programme de développement durable des Nations unies à l'horizon 2030 et de l'effort global consacré au renforcement des capacités institutionnelles.

Il convient, afin d'améliorer la capacité de l'UE à mobiliser son expertise collective au profit de ce renforcement des capacités, de mettre en place un réseau spécialisé de l'UE pour le renforcement des cybercapacités, regroupant le SEAE, les autorités des États membres compétentes en matière de cybersécurité, les agences de l'UE, les services de la Commission, les universités et la société civile. Des lignes directrices de l'UE sur le renforcement des capacités en matière de cybersécurité seront élaborées afin de contribuer à fournir de meilleures orientations politiques et à déterminer les priorités que l'UE devra respecter dans le cadre de ses efforts pour aider les pays tiers.

L'Union coopérera également avec les autres bailleurs de fonds actifs dans ce domaine pour éviter les doubles emplois et faciliter un renforcement plus ciblé des capacités dans les différentes régions.

4.3 Coopération UE-OTAN

Forte des progrès considérables déjà accomplis, l'UE approfondira sa coopération avec l'OTAN dans les domaines de la cybersécurité, de la lutte contre les menaces hybrides et de la défense, ainsi que le prévoit la déclaration commune du 8 juillet 2016[89]. Au nombre des priorités fixées figurent la promotion de l'interopérabilité grâce à des exigences et des normes cohérentes en matière de cyberdéfense, le renforcement de la coopération en matière de formation et d'exercices, ainsi que l'harmonisation des exigences de formation.

L'UE et l'OTAN favoriseront également la coopération en matière de recherche et d'innovation dans le domaine de la cyberdéfense et continueront à développer l'actuel arrangement technique pour le partage d'informations concernant la cybersécurité entre leurs organismes compétents respectifs[90]. Les efforts communs déployés récemment pour lutter contre les menaces hybrides, notamment la coopération entre la cellule de fusion de l'UE contre les menaces hybrides et la branche d'analyse des menaces hybrides de l'OTAN, devraient être davantage exploités pour renforcer la résilience et la réaction aux cybercrises. La poursuite de la coopération entre l'UE et l'OTAN sera encouragée au moyen d'exercices de cyberdéfense auxquels participeront le SEAE et d'autres entités de l'Union et leurs homologues de l'OTAN, dont le centre coopératif d'excellence pour la cyberdéfense de l'OTAN à Tallinn. Pour la première fois, l'OTAN et l'UE mèneront des exercices parallèles et coordonnés en réponse à un scénario hybride; l'OTAN dirigera les opérations en 2017, puis ce sera au tour de l'UE en 2018. Le prochain rapport sur la coopération UE-OTAN, qui sera soumis au Conseil de chacune des deux entités en décembre 2017, sera l'occasion d'examiner les possibilités de développer encore la coopération, notamment en mettant en place des moyens de communication communs, sûrs et fiables entre tous les organes et institutions concernés, y compris l'ENISA.

Actions clés

[88] SWD(2017) 157.
[89] http://www.consilium.europa.eu/fr/press/press-releases/2016/07/08-eu-nato-joint-declaration/.
[90] CERT-UE et Capacité OTAN de réaction aux incidents informatiques (NCIRC).

- Promouvoir le cadre stratégique de prévention des conflits et la stabilité dans le cyberespace;
- Développer un nouveau réseau pour le renforcement des capacités afin d'améliorer la capacité des pays tiers à faire face aux cybermenaces et élaborer des lignes directrices de l'UE sur le renforcement des capacités en matière de cybersécurité qui permettront à l'UE de mieux définir les domaines sur lesquels ses efforts devront porter en priorité;
- Approfondir la coopération entre l'UE et l'OTAN, notamment par la participation à des exercices parallèles et coordonnés et le renforcement de l'interopérabilité des normes en matière de cybersécurité.

5. CONCLUSION

La préparation de l'UE aux cyberattaques est essentielle tant pour le marché unique numérique que pour l'union de la sécurité et de la défense. Il est indispensable de renforcer la cybersécurité en Europe et de faire face aux menaces pesant sur les cibles civiles comme sur les cibles militaires.

Le sommet numérique qui se tiendra prochainement (le 29 septembre 2017) sous l'égide de la présidence estonienne sera l'occasion pour les États membres d'afficher leur détermination commune à placer la cybersécurité au cœur de l'Union en tant que société numérique. Dans le cadre de cette détermination commune, la Commission appelle les États membres à formuler des engagements sur la manière dont ils entendent agir dans les domaines relevant de leur responsabilité au premier chef. Ils devraient notamment s'attacher à renforcer la cybersécurité par les moyens suivants:

- garantir la mise en œuvre intégrale et effective de la directive SRI sur la cybersécurité pour le 9 mai 2018 et mettre à la disposition des autorités publiques chargées de la cybersécurité les ressources nécessaires au bon accomplissement de leurs tâches;
- appliquer les mêmes règles aux administrations publiques, compte tenu du rôle qu'elles jouent au sein de la société et de l'économie dans son ensemble;
- dispenser dans les administrations publiques des formations ayant trait à la cybersécurité;
- faire figurer en bonne place la sensibilisation à la cybersécurité dans les campagnes d'information et intégrer la cybersécurité dans les cursus universitaires et les programmes de formation professionnelle;
- tirer parti des initiatives relevant de la «coopération structurée permanente» (PESCO) et du Fonds européen de la défense pour soutenir l'élaboration de projets en matière de cyberdéfense.

La présente communication conjointe a exposé l'ampleur du défi et l'éventail des mesures que l'Union peut prendre. Nous avons besoin d'une Europe résiliente et capable de protéger efficacement ses citoyens en anticipant les incidents de cybersécurité potentiels, en intégrant une protection renforcée dans ses structures et dans les comportements, en surmontant rapidement les cyberattaques et en exerçant un effet dissuasif sur les responsables. La présente communication propose des mesures ciblées visant à renforcer de manière coordonnée les structures et les capacités de l'UE en matière de cybersécurité, avec la pleine coopération des États membres et des différentes structures concernées de l'UE, tout en respectant leurs compétences et leurs responsabilités. Sa mise en œuvre démontrera clairement que l'UE et ses États membres vont collaborer afin de mettre en place un niveau de cybersécurité permettant de relever les défis toujours plus grands auxquels l'Europe est actuellement confrontée.