COMMISSION
EUROPÉENNE

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

Bruxelles, le 7.2.2013
JOIN(2013) 1 final

COMMUNICATION CONJOINTE AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS

Stratégie de cybersécurité de l'Union européenne:

un cyberespace ouvert, sûr et sécurisé

COMMUNICATION CONJOINTE AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS

Stratégie de cybersécurité de l'Union européenne:

un cyberespace ouvert, sûr et sécurisé

1. INTRODUCTION

1.1. Contexte

Au cours des vingt dernières années, Internet et, plus généralement, le cyberespace ont bouleversé l'ensemble de la société. Notre quotidien, nos droits fondamentaux, notre vie sociale et notre économie dépendent désormais de technologies de l'information et des communications (TIC) fonctionnant sans discontinuité. L'émergence d'un cyberespace libre et ouvert a favorisé l'intégration politique et sociale à l'échelle planétaire. Ce cyberespace a fait tomber les barrières entre les pays, les communautés et les individus et a permis l'interaction et le partage des informations et des idées à travers le monde. Il a constitué un forum pour la liberté d'expression et l'exercice des droits fondamentaux et a donné aux peuples les moyens de lutter pour des sociétés démocratiques et plus justes – comme le Printemps arabe l'a montré de façon frappante.

Pour que le cyberespace reste libre et ouvert, les normes, principes et valeurs que l'UE défend hors ligne doivent aussi s'appliquer en ligne. Les droits fondamentaux, la démocratie et l'État de droit doivent donc être protégés dans le cyberespace. Notre liberté et notre prospérité dépendent de plus en plus d'un Internet solide et novateur, qui continuera à se développer si l'innovation du secteur privé et la société civile favorisent sa croissance, mais la liberté en ligne exige aussi sécurité et sûreté. Le cyberespace doit être protégé contre les incidents, actes de malveillance et abus, et les pouvoirs publics ont un rôle important à jouer pour ce qui est de garantir un cyberespace libre et sûr. Plusieurs tâches leur incombent: sauvegarder l'accès et l'ouverture, respecter et protéger les droits fondamentaux en ligne et préserver la fiabilité et l'interopérabilité d'Internet. Cependant, le secteur privé détient et exploite des parties importantes du cyberespace et, pour qu'une initiative soit couronnée de succès dans ce domaine, elle doit tenir compte du rôle moteur des entreprises.

Les TIC sont devenues le nerf de la croissance et une ressource critique dont dépendent tous les secteurs économiques. Elles étayent les systèmes complexes qui permettent à l'activité économique de s'exercer dans des secteurs clés comme la finance, la santé, l'énergie et les transports, tandis que nombre de modèles d'entreprise reposent sur la disponibilité ininterrompue d'Internet et le bon fonctionnement des systèmes informatiques.

En achevant le marché unique du numérique, l'Europe pourrait faire augmenter son PIB de presque 500 milliards d'euros par an[1], soit une moyenne de 1 000 euros par personne. L'essor des nouvelles technologies connectées, dont les paiements électroniques, l'informatique en nuage ou la communication de machine à machine[2], est étroitement lié à la confiance et à

[1] http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf

[2] Par exemple, plantes équipées de capteurs indiquant au système d'arrosage à quel moment elles ont besoin d'eau.

l'assurance du public. Malheureusement, une enquête Eurobaromètre de 2012[3] a montré que près d'un tiers des Européens ne sont pas confiants lorsqu'ils utilisent Internet pour effectuer des opérations bancaires ou des achats. Dans leur écrasante majorité, ils ont également déclaré que, pour des raisons de sécurité, ils évitaient de divulguer des informations personnelles en ligne. Dans l'UE, plus d'un internaute sur dix a déjà été victime de fraude en ligne.

Au cours des dernières années, on a constaté que le monde numérique, s'il procure d'énormes avantages, est aussi très vulnérable. Les incidents de cybersécurité[4], d'origine malveillante ou accidentelle, se multiplient à un rythme inquiétant et pourraient perturber la fourniture de services essentiels que nous tenons pour acquis comme l'eau, les soins de santé, l'électricité ou les services mobiles. Les menaces peuvent avoir des origines diverses, notamment des attaques criminelles, à caractère politique, terroristes ou commanditées par un État, ainsi que des catastrophes naturelles et erreurs involontaires.

L'économie de l'UE est déjà touchée par des actes de cybercriminalité[5] visant le secteur privé et les particuliers, les cybercriminels utilisant des méthodes toujours plus sophistiquées pour s'introduire dans les systèmes informatiques, dérober des données critiques ou rançonner les entreprises, mais le développement de l'espionnage économique et d'activités commanditées par les États dans le cyberespace fait peser un nouveau type de menaces sur les pouvoirs publics et les entreprises de l'UE.

Dans certains pays hors de l'UE, l'État peut aussi abuser du cyberespace à des fins de surveillance et de contrôle de sa propre population, situation à laquelle l'UE peut remédier en promouvant la liberté et en veillant au respect des droits fondamentaux en ligne.

Tout cela explique pourquoi les pouvoirs publics à travers le monde ont commencé à élaborer des stratégies de cybersécurité et à considérer le cyberespace comme une question internationale de plus en plus importante. Le moment est donc venu pour l'UE d'intensifier son action dans ce domaine. La présente proposition de stratégie de cybersécurité de l'Union européenne, soumise par la Commission et la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité (haute représentante), expose la vision de l'UE dans ce domaine, précise les rôles et les responsabilités et définit les actions requises, fondées sur une protection solide et une promotion efficace des droits individuels, pour que l'environnement en ligne de l'UE soit le plus sûr au monde.

1.2. Principes de cybersécurité

L'Internet sans frontière et multicouche est devenu l'un des moteurs les plus puissants du progrès mondial, sans surveillance ni réglementation de la part des pouvoirs publics. Le secteur privé doit certes continuer à un jouer rôle éminent dans la construction et la gestion au jour le jour d'Internet, mais le besoin d'exigences de transparence, de responsabilité et de

---

[3] Eurobaromètre spécial 390 sur la cybersécurité (2012).

[4] On entend généralement par cybersécurité les mesures de sauvegarde et les actions auxquelles il est possible de recourir pour protéger le cyberespace, dans les domaines civil et militaire, des menaces associées à ses réseaux interdépendants et à son infrastructure informatique ou susceptibles de leur porter atteinte. La cybersécurité vise à préserver la disponibilité et l'intégrité des réseaux et de l'infrastructure ainsi que la confidentialité des informations qui y sont contenues.

[5] On entend généralement par cybercriminalité un large éventail d'activités criminelles dont les ordinateurs et systèmes informatiques constituent soit l'arme soit la cible principale. La cybercriminalité recouvre les délits habituels (fraude, contrefaçon et usurpation d'identité p. ex.), les délits liés au contenu (distribution en ligne de matériel pédopornographique ou incitation à la haine raciale p. ex.) et les délits spécifiques aux ordinateurs et systèmes informatiques (attaque contre un système informatique, déni de service et logiciel malveillant p. ex.).

sécurité se fait de plus en plus sentir. Aussi la présente stratégie vise-t-elle à préciser les principes qui doivent inspirer une politique de cybersécurité dans l'UE et au niveau international.

Les valeurs essentielles de l'UE prévalent dans le monde virtuel autant que dans le monde réel.

Les lois et normes qui régissent d'autres domaines de notre vie quotidienne s'appliquent également dans le domaine du cyberespace.

Protection des droits fondamentaux, de la liberté d'expression, des données personnelles et de la vie privée

La cybersécurité ne peut être viable et efficace que si elle repose sur les libertés et droits fondamentaux consacrés par la Charte des droits fondamentaux de l'Union européenne et les valeurs essentielles de l'UE. Inversement, les droits individuels ne peuvent être garantis sans des réseaux et systèmes sûrs. Tout partage d'informations à des fins de cybersécurité, dès lors que des données à caractère personnel sont en jeu, doit être conforme au droit de l'UE en matière de protection des données et tenir dûment compte des droits des personnes dans ce domaine.

Accès pour tous

Vu la place que le monde numérique a prise dans la société, n'avoir qu'un accès limité ou aucun accès à Internet et ne pas pouvoir maîtriser les outils informatiques constituent des handicaps. Chacun doit donc pouvoir accéder à Internet et à une libre circulation des informations, de même que l'intégrité et la sécurité d'Internet doivent être garanties pour offrir à tous un accès sûr.

Gouvernance participative, démocratique et efficace

Le monde numérique n'est pas contrôlé par une entité unique. Il existe actuellement plusieurs parties prenantes, dont de nombreuses entités commerciales et non gouvernementales, qui interviennent dans la gestion au jour le jour des ressources, protocoles et normes Internet et dans le développement futur d'Internet. L'UE réaffirme l'importance de toutes les parties prenantes dans le modèle actuel de gouvernance Internet et soutient cette approche de gouvernance participative[6].

Une responsabilité partagée pour assurer la sécurité

La dépendance croissante vis-à-vis des TIC dans tous les domaines de la vie a entraîné des problèmes de vulnérabilité qui doivent être définis correctement, analysés en profondeur et résolus ou atténués. Tous les acteurs concernés, qu'il s'agisse des pouvoirs publics, du secteur privé ou des particuliers, doivent accepter cette responsabilité partagée, prendre des mesures pour se protéger et, si nécessaire, apporter une réponse coordonnée pour renforcer la cybersécurité.

[6] Voir aussi COM(2009) 277, communication de la Commission au Parlement Européen et au Conseil sur «La gouvernance de l'internet: les prochaines étapes».

2. PRIORITES ET ACTIONS STRATEGIQUES

L'UE doit préserver un environnement en ligne offrant le degré de liberté et de sécurité le plus élevé possible dans l'intérêt de tous. Tout en reconnaissant que c'est aux États membres qu'il incombe en premier lieu de traiter les problèmes de sécurité dans le cyberespace, la présente stratégie propose des actions spécifiques qui peuvent permettre à l'UE d'améliorer ses performances globales. Ce sont des actions à court terme et à long terme, qui exigent divers outils stratégiques[7] et impliquent différents types d'acteurs, qu'il s'agisse des institutions de l'UE, des États membres ou des entreprises.

La vision de l'UE exposée dans la présente stratégie s'articule autour de cinq priorités stratégiques qui répondent aux problèmes signalés ci-dessus:

- parvenir à la cyber-résilience;
- faire reculer considérablement la cybercriminalité;
- développer une politique et des moyens de cyberdéfense liée à la politique de sécurité et de défense commune (PSDC);
- développer les ressources industrielles et technologiques en matière de cybersécurité;
- instaurer une politique internationale de l'Union européenne cohérente en matière de cyberespace et promouvoir les valeurs essentielles de l'UE.

2.1. Parvenir à la cyber-résilience

Pour promouvoir la cyber-résilience dans l'UE, les pouvoirs publics comme le secteur privé doivent développer leurs moyens et coopérer efficacement. Sur la base des résultats positifs obtenus grâce aux activités menées jusqu'à maintenant[8], une nouvelle action de l'UE peut notamment permettre de faire face aux cyber-risques et menaces de dimension transnationale et contribuer à une intervention coordonnée en cas d'urgence. Cela favorisera grandement le bon fonctionnement du marché intérieur et accroîtra la sécurité intérieure de l'UE.

Sans un effort substantiel pour développer les moyens, ressources et processus dans les secteurs public et privé en vue de prévenir, détecter et gérer les incidents de cybersécurité, l'Europe restera vulnérable. C'est pourquoi la Commission a élaboré une politique de sécurité des réseaux et de l'information (SRI)[9]. L'**Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)** a été instituée en 2004[10] et un nouveau règlement visant à la renforcer et à moderniser son mandat est en cours de négociation entre le Conseil et le Parlement[11]. En outre, la directive «cadre» sur les communications électroniques[12] exige des fournisseurs de communications électroniques qu'ils gèrent de manière appropriée les

---

7 Les actions relatives au partage d'informations, dès lors que des données à caractère personnel sont en jeu, doivent être conformes au droit de l'UE en matière de protection des données.

8 Voir références dans la présente communication ainsi que dans le document de travail des services de la Commission (analyse d'impact) accompagnant la proposition de directive sur la sécurité des réseaux et de l'information, soumise par la Commission, en particulier les points 4.1.4 et 5.2 et les annexes 2, 6 et 8.

9 La Commission a adopté, en 2001, une communication sur la «Sécurité des réseaux et de l'information: proposition pour une approche politique européenne» [COM(2001) 298] et, en 2006, «Une stratégie pour une société de l'information sûre» [COM(2006) 251]. Depuis 2009, la Commission a également adopté un plan d'action et une communication sur la protection des infrastructures d'information critiques (PIIC) [COM(2009) 149 approuvé par la résolution du Conseil 2009/C 321/01, et COM(2011) 163 approuvé par les conclusions du Conseil 10299/11].

10 Règlement (CE) n° 460/2004.

11 COM(2010) 521. Les actions proposées au titre de la présente stratégie n'impliquent pas de modifier le mandat actuel ou futur de l'ENISA.

12 Articles 13 *bis* et 13 *ter* de la directive 2002/21/CE.

risques pour leurs réseaux et signalent les atteintes significatives à la sécurité. De plus, la législation de l'UE sur la protection des données[13] exige des responsables du traitement des données qu'ils prévoient des exigences de protection et des mesures de sauvegarde des données, y compris des mesures relatives à la sécurité, et, dans le domaine des services de communications électroniques accessibles au public, qu'ils notifient aux autorités nationales compétentes les incidents impliquant une violation de données à caractère personnel.

Malgré les progrès permis par les engagements volontaires, il y a toujours des insuffisances dans l'UE, notamment en ce qui concerne les moyens disponibles au niveau national, la coordination en cas d'incidents transnationaux ainsi que la participation et la préparation du secteur privé. La présente stratégie est accompagnée par une proposition **législative** visant en particulier à:

- instaurer des exigences minimales communes de SRI au niveau national qui obligeraient les États membres à désigner des autorités nationales compétentes en la matière, à constituer une équipe d'intervention en cas d'urgence informatique (CERT) performante et à adopter une stratégie nationale et un plan national de coopération pour la SRI. La mise en place de moyens et la coordination concernent aussi les institutions de l'UE et une CERT responsable de la sécurité des systèmes informatiques des institutions, agences et organes de l'UE (CERT-UE) a été instituée à titre permanent en 2012;
- instaurer des mécanismes de prévention, de détection, d'atténuation et d'intervention coordonnées permettant aux autorités nationales compétentes en matière de SRI de partager des informations et de se porter mutuellement assistance. Il sera demandé à ces autorités nationales compétentes d'assurer une coopération appropriée à l'échelle de l'UE, notamment à l'aide d'un plan de coopération de l'Union en la matière, permettant d'intervenir en cas de cyberincident de dimension transnationale. Cette coopération bénéficiera aussi des progrès accomplis dans le cadre du Forum européen des États membres (EFMS)[14] qui a organisé des discussions et des échanges fructueux sur la politique publique de SRI et qui pourra être intégré au mécanisme de coopération une fois celui-ci mis en place;
- améliorer la préparation et renforcer l'engagement du secteur privé. Comme la grande majorité des réseaux et systèmes informatiques sont détenus et exploités par le secteur privé, il est essentiel de mieux collaborer avec celui-ci pour promouvoir la cybersécurité. Les acteurs privés doivent développer, au niveau technique, leurs propres moyens de cyber-résilience et partager les meilleures pratiques. Les outils mis au point par les entreprises pour intervenir en cas d'incident, en déterminer les causes et mener des enquêtes criminalistiques doivent aussi bénéficier au secteur public.

Toutefois, les acteurs privés ne sont pas encore réellement motivés pour fournir des données fiables sur la survenue ou les conséquences d'incidents de SRI, adopter une culture de gestion des risques ou investir dans des solutions de sécurité. La législation proposée vise donc à faire en sorte que les acteurs dans un certain nombre de domaines importants (à savoir l'énergie, les transports, la banque, les bourses de valeurs et les facilitateurs de services Internet clés ainsi que les administrations publiques) évaluent les risques qu'ils courent en termes de cybersécurité, assurent la fiabilité et la résilience des réseaux et systèmes informatiques par une gestion appropriée des risques et partagent les informations recensées avec les autorités

[13] Article 17 de la directive 95/46/CE et article 4 de la directive 2002/58/CE.

[14] Le Forum européen des États membres a été établi par le COM(2009) 149 en tant que plateforme destinée à favoriser les discussions entre les pouvoirs publics des États membres à propos des bonnes pratiques politiques concernant la sécurité et la résilience des infrastructures d'information critiques.

nationales compétentes en matière de SRI. L'adoption d'une culture de la cybersécurité pourrait accroître les débouchés commerciaux et la compétitivité dans le secteur privé et faire de la cybersécurité un argument de vente.

Ces entités devraient signaler aux autorités nationales compétentes en matière de SRI les incidents ayant un impact significatif sur la continuité des services essentiels et la fourniture des biens dépendant de réseaux et systèmes informatiques.

Les autorités nationales compétentes en matière de SRI devraient collaborer et échanger des informations avec d'autres organes réglementaires et, en particulier, avec les autorités chargées de la protection des données personnelles. Les autorités compétentes en matière de SRI devraient à leur tour signaler aux autorités de maintien de l'ordre les incidents pouvant constituer une infraction pénale grave. Les autorités nationales compétentes devraient aussi publier régulièrement, sur un site Web spécialisé, des informations non classifiées sur les procédures d'alerte rapide en cours concernant les risques et incidents et les interventions coordonnées. Les obligations légales ne doivent pas dispenser ni empêcher de développer une coopération informelle volontaire, y compris entre secteur public et secteur privé, pour relever les niveaux de sécurité et échanger des informations et de bonnes pratiques. Le Partenariat public-privé européen pour la résilience (EP3R)[15] constitue, en particulier, une plateforme viable et valable au niveau de l'UE et doit être développé.

Au titre du Mécanisme pour l'interconnexion en Europe (MIE)[16], un soutien financier serait apporté à des infrastructures clés, faisant le lien entre les moyens des États membres en matière de SRI et facilitant ainsi la coopération dans l'UE.

Enfin, les exercices de simulation de cyberincident au niveau de l'UE sont essentiels pour tester la coopération entre les États membres et le secteur privé. Le premier exercice, auquel participaient les États membres, a été effectué en 2010 («Cyber Europe 2010») et un deuxième exercice, impliquant aussi le secteur privé, a eu lieu en octobre 2012 («Cyber Europe 2012»). Un exercice de simulation UE–États-Unis a été effectué en novembre 2011 («Cyber Atlantic 2011») et d'autres exercices sont prévus dans les années à venir, y compris avec des partenaires internationaux.

La Commission entend:

- poursuivre, par l'intermédiaire du Centre commun de recherche et en étroite collaboration avec les autorités des États membres ainsi que les propriétaires et exploitants d'infrastructures critiques, ses activités consistant à recenser les faiblesses en matière de SRI de ces infrastructures en Europe et à promouvoir la mise au point de systèmes résilients;
- lancer, au début de 2013, un projet pilote financé par l'UE[17] consacré à la **lutte contre les réseaux zombies et les logiciels malveillants** afin de fournir un cadre

[15] Le Partenariat public-privé européen pour la résilience a été établi par le COM(2009) 149. Cette plateforme a entamé des travaux et encouragé la coopération entre le secteur public et le secteur privé afin de définir les principaux actifs, ressources, fonctions et exigences de base en matière de résilience ainsi que les besoins et mécanismes de coopération permettant d'intervenir en cas de perturbation majeure des communications électroniques.

[16] https://ec.europa.eu/digital-agenda/en/connecting-europe-facility. Ligne budgétaire 09.03.02 – Réseaux de télécommunications (favoriser l'interconnexion et l'interopérabilité des services publics nationaux en ligne ainsi que l'accès à ces réseaux).

de coordination et de coopération entre les États membres, des organismes du secteur privé tels que les fournisseurs de services Internet et des partenaires internationaux.

La Commission invite l'ENISA à:

- aider les États membres à développer de solides **moyens de cyber-résilience au niveau national**, notamment par l'acquisition de compétences sur la sécurité et la résilience des systèmes de commande de processus, des transports et de l'infrastructure énergétique;
- étudier, en 2013, la faisabilité d'équipe(s) d'intervention en cas d'incident de sécurité informatique concernant des systèmes de commande de processus (ICS-CSIRT) pour l'UE;
- continuer à aider les États membres et les institutions de l'UE à effectuer régulièrement des **exercices paneuropéens de simulation de cyberincident** qui constitueront aussi la base opérationnelle de la participation de l'UE à des exercices internationaux.

La Commission invite le Parlement européen et le Conseil à:

- adopter rapidement la proposition de directive sur un **niveau élevé de sécurité commun des réseaux et de l'information** dans l'Union, concernant les moyens et la préparation au niveau national, la coopération au niveau de l'UE, l'adoption de méthodes de gestion des risques et le partage des informations sur la SRI.

La Commission invite les entreprises à:

- prendre l'initiative d'**investir** dans un niveau élevé de cybersécurité, élaborer de bonnes pratiques et développer le partage d'informations au niveau sectoriel et avec les pouvoirs publics en vue d'assurer une protection solide et efficace des biens et des personnes, notamment par des partenariats public-privé comme l'EP3R et *Trust in Digital Life* (TDL)[18].

Sensibiliser

Assurer la cybersécurité est une responsabilité partagée. L'utilisateur final joue un rôle crucial dans la sécurité des réseaux et systèmes informatiques: il doit être informé des dangers qu'il court dans l'environnement en ligne et être habilité à prendre des mesures simples pour s'en prémunir.

Plusieurs initiatives ont été prises au cours des dernières années et doivent être poursuivies. L'ENISA a notamment contribué à la sensibilisation en publiant des rapports, en organisant des ateliers d'experts et en développant des partenariats public-privé. Europol, Eurojust et les autorités nationales de protection des données sont également actifs en la matière. En octobre 2012, l'ENISA a, avec quelques États membres, organisé le «Mois européen de la cybersécurité». La sensibilisation est l'un des domaines dans lequel le groupe de travail UE–États-Unis sur la cybersécurité et la cybercriminalité[19] progresse et elle s'avère également

[17] CIP-ICT PSP-2012-6, 325188. Il est doté d'un budget global de 15 millions d'euros, que l'UE prend en charge à hauteur de 7,7 millions d'euros.

[18] http://www.trustindigitallife.eu/

[19] Ce groupe de travail, institué au sommet UE–États-Unis de novembre 2010 (MEMO/10/597), est chargé d'élaborer des approches collaboratives sur un large éventail de questions de cybersécurité et de cybercriminalité.

essentielle dans le contexte du programme pour un Internet plus sûr[20] (axé sur la sécurité des enfants en ligne).

La Commission invite l'ENISA à:

- proposer une feuille de route concernant un «permis de conduire» en matière de sécurité des réseaux et de l'information, sous la forme d'un programme de certification volontaire visant à développer les compétences et qualifications des professionnels de l'informatique (administrateurs de sites Web p. ex.).

La Commission entend:

- organiser en 2014, avec l'aide de l'ENISA, un **championnat** de cybersécurité au cours duquel des étudiants s'affronteront en proposant des solutions de SRI.

La Commission invite les États Membres[21] à:

- organiser tous les ans à partir de 2013, avec l'aide de l'ENISA et la participation du secteur privé, un **mois de la cybersécurité** afin de sensibiliser les utilisateurs finaux. À partir de 2014, un mois de la cybersécurité sera organisé en même temps dans l'UE et aux États-Unis;
- **intensifier les efforts consacrés à l'éducation et la formation à la SRI au niveau national** en prévoyant une formation à la SRI en milieu scolaire d'ici à 2014, une formation à la SRI, au développement de logiciels sûrs et à la protection des données personnelles dans le cursus des étudiants en informatique et une formation de base à la SRI pour le personnel des administrations publiques.

La Commission invite les entreprises à:

- **sensibiliser** à la cybersécurité **à tous les niveaux**, dans leurs pratiques internes comme dans leurs relations avec la clientèle. En particulier, les entreprises doivent réfléchir à la façon de rendre les PDG et conseils d'administration plus responsables de la cybersécurité.

2.2. Faire reculer considérablement la cybercriminalité

Plus nous passons de temps dans le monde numérique, plus nous offrons de possibilités aux cybercriminels. Aussi la cybercriminalité, qui fait chaque jour plus d'un million de victimes dans le monde, est-elle la forme de criminalité qui augmente le plus rapidement. Par ailleurs, les cybercriminels et leurs réseaux sont de plus en plus sophistiqués et nous devons disposer des outils et moyens opérationnels appropriés pour nous y opposer. La cybercriminalité est une activité à forte rentabilité et faible risque et les cybercriminels profitent souvent de l'anonymat des sites Web. La cybercriminalité ignore les frontières et, compte tenu de la portée mondiale d'Internet, les responsables du maintien de l'ordre doivent adopter une approche transnationale coordonnée et collaborative pour faire face à cette menace croissante.

Une législation solide et efficace

[20] Le programme pour un Internet plus sûr permet de financer un réseau d'ONG actives dans le domaine de la protection de l'enfance en ligne, un réseau d'organes de maintien de l'ordre qui échangent des informations et de bonnes pratiques concernant l'exploitation délictueuse d'Internet aux fins de diffusion de matériel pédopornographique, et un réseau de chercheurs qui recueillent des informations sur l'utilisation des technologies en ligne par les enfants et sur les risques et conséquences que cela entraîne pour eux.

[21] Avec la participation des autorités nationales concernées, dont les autorités compétentes en matière de SRI et les autorités chargées de la protection des données.

L'UE et les États membres doivent se doter d'une législation solide et efficace pour combattre la cybercriminalité. La convention du Conseil de l'Europe sur la cybercriminalité, également appelée convention de Budapest, est un traité international contraignant qui fournit un cadre approprié à l'adoption d'une législation nationale.

L'UE a déjà adopté une législation en matière de cybercriminalité, dont une directive relative à la lutte contre l'exploitation sexuelle des enfants en ligne et la pédopornographie[22]. Elle va aussi approuver bientôt une directive sur les attaques visant les systèmes informatiques, en particulier à l'aide de réseaux zombies.

La Commission entend:

- assurer une transposition et une mise en œuvre rapides des directives relatives à la cybercriminalité;
- enjoindre aux États membres qui n'ont pas encore ratifié la **convention du Conseil de l'Europe sur la cybercriminalité** de le faire et d'appliquer ses dispositions le plus rapidement possible.

Des moyens opérationnels accrus pour combattre la cybercriminalité

Le mode opératoire des cybercriminels évolue très rapidement et les services de maintien de l'ordre ne peuvent pas combattre la cybercriminalité avec des outils dépassés. Actuellement, tous les États membres de l'UE ne disposent pas des moyens opérationnels nécessaires pour lutter efficacement contre la cybercriminalité et tous doivent mettre en place de véritables unités anticybercriminalité nationales.

La Commission entend:

- par ses programmes de financement[23], aider les États membres à **recenser leurs insuffisances et renforcer leurs moyens** d'enquête et de lutte contre la cybercriminalité. La Commission soutiendra aussi les organes dont la tâche est de faire le lien entre les chercheurs/universitaires, les professionnels du maintien de l'ordre et le secteur privé, à l'instar des travaux menés par les centres d'excellence de lutte contre la cybercriminalité, financés par la Commission, déjà créés dans certains États membres;
- avec les États membres et le soutien du CCR, coordonner les efforts afin de recenser les meilleures pratiques et techniques disponibles pour lutter contre la cybercriminalité (p. ex. en ce qui concerne la mise au point et l'utilisation d'outils criminalistiques ou l'analyse des menaces);
- collaborer étroitement avec le **Centre européen de lutte contre la cybercriminalité (EC3)** récemment créé **au sein d'Europol et avec Eurojust** pour aligner ces approches politiques sur les meilleures pratiques du point de vue opérationnel.

Une meilleure coordination au niveau de l'UE

[22] Directive 2011/93/UE remplaçant la décision-cadre 2004/68/JAI du Conseil.

[23] En 2013, au titre du programme spécifique «Prévenir et combattre la criminalité» (ISEC) et, après 2013, au titre du Fonds pour la sécurité intérieure (nouvel instrument du CFP).

L'UE peut compléter les travaux des États membres en promouvant une approche coordonnée et collaborative et en réunissant les autorités de maintien de l'ordre et judiciaires ainsi que les parties prenantes publiques et privées de l'UE et d'ailleurs.

La Commission entend:

- soutenir le **Centre européen de lutte contre la cybercriminalité** (EC3) récemment créé comme point focal européen en la matière. L'EC3 fournira des analyses et des informations, contribuera aux enquêtes, apportera des moyens criminalistiques de haut niveau, facilitera la coopération, créera des filières de partage des informations entre les autorités compétentes dans les États membres, le secteur privé et d'autres parties prenantes, et endossera progressivement le rôle de porte-parole des professionnels du maintien de l'ordre[24];
- soutenir les efforts en vue d'étendre la responsabilité des bureaux d'enregistrement des noms de domaine et de garantir l'exactitude des informations sur les propriétaires de site Web, notamment selon les recommandations en matière de maintien de l'ordre à l'intention de l'ICANN (*Internet Corporation for Assigned Names and Numbers*) et conformément au droit de l'Union, y compris aux règles sur la protection des données;
- s'appuyer sur la nouvelle législation pour continuer à intensifier les efforts de l'UE en vue de lutter contre les abus sexuels sur mineur en ligne. La Commission a adopté une Stratégie européenne pour un Internet mieux adapté aux enfants[25] et, avec des États membres de l'UE et des pays tiers, a lancé une **Alliance mondiale contre les abus sexuels commis contre des enfants via Internet**[26]. L'Alliance est le vecteur d'autres actions émanant des États membres et soutenues par la Commission et l'EC3.

La Commission invite Europol (EC3) à:

- axer principalement son soutien analytique et opérationnel aux enquêtes cybercriminelles des États membres sur le démantèlement et la désorganisation des réseaux dans les domaines des abus sexuels sur mineur, des paiements frauduleux, des réseaux zombies et de l'intrusion;
- produire régulièrement des rapports stratégiques et opérationnels sur les tendances et menaces émergentes afin d'établir les priorités et de cibler les enquêtes des équipes cybercriminelles dans les États membres.

La Commission invite le Collège européen de police (CEPOL), en coopération avec Europol, à:

- coordonner la conception et la planification de modules de formation censés fournir aux professionnels du maintien de l'ordre les connaissances et compétences nécessaires pour lutter efficacement contre la cybercriminalité.

La Commission invite Eurojust à:

[24] Le 28 mars 2012, la Commission européenne a adopté une communication intitulée «Combattre la criminalité à l'ère numérique: établissement d'un Centre européen de lutte contre la cybercriminalité».

[25] COM(2012) 196 final.

[26] Conclusions du Conseil sur une alliance mondiale contre les abus sexuels commis contre des enfants via Internet (déclaration conjointe UE–États-Unis) des 7 et 8 juin 2012 et déclaration sur le lancement d'une alliance mondiale contre les abus sexuels commis contre des enfants via Internet (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm).

- recenser les principaux obstacles à la coopération judiciaire dans le cadre d'enquêtes cybercriminelles et à la coordination entre États membres et avec les pays tiers, et soutenir les activités d'enquête et de poursuite en matière de cybercriminalité ainsi que les activités de formation dans ce domaine.

La Commission invite Eurojust et Europol (EC3) à:

- coopérer étroitement, en particulier par l'échange d'informations, afin d'être plus efficaces dans leur lutte contre la cybercriminalité, conformément à leur mandat et leurs compétences respectifs.

2.3. Développer une politique et des moyens de cyberdéfense s'inscrivant dans le cadre de la politique de sécurité et de défense commune (PSDC)

Les efforts de cybersécurité dans l'UE ont aussi une dimension de cyberdéfense. Pour accroître la résilience des systèmes de communication et d'information préservant les intérêts des États membres en matière de défense et de sécurité nationale, le développement des moyens de cyberdéfense doit être axé sur la détection, l'intervention et la récupération en cas de cybermenace sophistiquée.

Comme ces menaces sont multiformes, il faut développer des synergies entre les approches civile et militaire de la protection des cyberinfrastructures critiques. Ces efforts doivent être étayés par de la R&D et une coopération étroite entre les pouvoirs publics, le secteur privé et les universités dans l'UE. Afin d'éviter les doublons, l'Union étudiera les différentes possibilités de conjuguer les efforts de l'UE et de l'OTAN pour accroître la résilience des infrastructures critiques d'État, de défense ou d'information dont dépendent les membres des deux organisations.

La haute représentante se concentrera sur les activités clés suivantes et invitera les États membres et l'Agence européenne de défense (AED) à y prendre part:

- définir les exigences de cyberdéfense opérationnelle de l'UE et promouvoir le développement de moyens et technologies de cyberdéfense propres à l'Union sous tous ses aspects – doctrine, commandement, organisation, personnel, formation, technologies, infrastructure, logistique et interopérabilité;
- élaborer le cadre politique de cyberdéfense de l'UE pour protéger les réseaux dans le contexte de missions et d'opérations de PSDC, notamment par la gestion dynamique des risques, l'analyse approfondie des menaces et le partage des informations. Offrir aux militaires davantage de possibilités de se former et de s'exercer à la cyberdéfense dans le contexte européen et multinational, y compris par l'intégration d'éléments de cyberdéfense dans les programmes actuels d'exercices;
- promouvoir le dialogue et la coordination entre les acteurs civils et militaires dans l'UE en mettant particulièrement l'accent sur l'échange de bonnes pratiques, le partage d'informations et l'alerte rapide, l'intervention en cas d'incident, la gestion des risques, la sensibilisation et l'établissement de la cybersécurité comme priorité;
- maintenir un dialogue avec les partenaires internationaux, notamment l'OTAN, d'autres organisations internationales et les centres d'excellence multinationaux, pour faire en sorte de disposer de moyens de défense efficaces, de recenser les domaines de coopération et d'éviter les doubles emplois.

2.4. Développer les ressources industrielles et technologiques en matière de cybersécurité

L'Europe dispose de moyens de R&D de haut niveau mais nombre des principaux fournisseurs mondiaux de produits et services TIC innovants sont basés hors de l'UE. Aussi risque-t-elle de se retrouver dans une situation de dépendance excessive vis-à-vis non seulement de TIC produites ailleurs, mais aussi de solutions de sécurité élaborées hors de ses frontières. Il importe de faire en sorte que les composants matériels et logiciels produits dans l'UE et dans les pays tiers, qui sont utilisés pour les services et infrastructures critiques et, de plus en plus, dans les appareils mobiles, soient fiables et sûrs et garantissent la protection des données personnelles.

Promouvoir un marché unique des produits de cybersécurité

Assurer un niveau élevé de sécurité n'est possible que si tous les intervenants dans la chaîne de valeur (p. ex. fabricants d'équipement, développeurs de logiciels, prestataires de services de la société de l'information) font de la sécurité une priorité. Il semble[27] toutefois que nombre d'acteurs considèrent toujours la sécurité, tout au plus, comme une charge supplémentaire, d'où une demande de solutions de sécurité assez limitée. Il faut donc que des exigences appropriées de performance en matière de cybersécurité soient imposées d'un bout à l'autre de la chaîne de valeur des produits TIC utilisés en Europe et que le secteur privé soit incité à garantir un niveau élevé de cybersécurité. Par exemple, l'étiquetage indiquant des performances de cybersécurité adéquates permettra aux entreprises qui ont de bons résultats dans ce domaine d'en faire un argument de vente et un avantage concurrentiel. De même, les obligations énoncées dans la directive SRI proposée contribueraient grandement à accroître la compétitivité des entreprises dans les secteurs concernés.

Il faut également favoriser une demande commerciale de produits hautement sécurisés à l'échelle de l'Europe. Premièrement, la présente stratégie vise à accroître la coopération et la transparence concernant la sécurité dans les produits TIC. Elle préconise d'établir une plateforme, réunissant les parties intéressées des secteurs public et privé en Europe, afin de recenser les bonnes pratiques de cybersécurité au long de la chaîne de valeur et de créer les conditions commerciales favorables à l'élaboration et à l'adoption de solutions TIC sûres. L'une des priorités doit être de prendre des mesures incitant à assurer une gestion des risques appropriée et à adopter des normes et solutions de sécurité, et éventuellement d'instaurer des systèmes volontaires de certification à l'échelle de l'UE en s'inspirant des systèmes existant dans l'Union et ailleurs. La Commission œuvrera à promouvoir l'adoption d'approches cohérentes par les États membres pour éviter les disparités entraînant des désavantages d'ordre géographique pour les entreprises.

Deuxièmement, la Commission soutiendra l'élaboration de normes de sécurité et y contribuera par des systèmes volontaires de certification à l'échelle de l'UE dans le domaine de l'informatique en nuage, compte dûment tenu de la nécessité d'assurer la protection des données. Les travaux doivent porter sur la sécurité de la chaîne d'approvisionnement, en particulier dans les secteurs économiques critiques (systèmes de commande de processus, infrastructures énergétiques et de transports). Ces travaux doivent reposer sur les activités en cours des organismes européens de normalisation (CEN, CENELEC et ETSI)[28] et du Groupe

[27] Voir document de travail des services de la Commission (analyse d'impact) accompagnant la proposition de directive sur la sécurité des réseaux et de l'information, point 4.1.5.2.

[28] Notamment au titre de la norme de réseaux intelligents M/490 pour la première série de normes concernant un réseau intelligent et une architecture de référence.

de coordination en matière de cybersécurité (CSCG) ainsi que sur l'expertise de l'ENISA, de la Commission et d'autres acteurs concernés.

La Commission entend:

- lancer, en 2013, une **plateforme** public-privé **sur les solutions de SRI** afin d'élaborer des mesures favorisant l'adoption de solutions TIC sûres et l'application d'une exigence de bonnes performances de cybersécurité aux produits TIC utilisés en Europe;
- à partir des travaux de cette plateforme, proposer, en 2014, des recommandations pour assurer la cybersécurité au long de la chaîne de valeur;
- étudier comment les principaux fournisseurs de matériels et logiciels TIC pourraient informer les autorités nationales compétentes des faiblesses détectées qui pourraient avoir des conséquences importantes pour la sécurité.

La Commission invite l'ENISA à:

- élaborer, en coopération avec les autorités nationales compétentes, les parties intéressées, les organismes européens et internationaux de normalisation et le Centre commun de recherche de la Commission européenne, des **orientations et recommandations techniques pour l'adoption de normes et bonnes pratiques SRI** dans les secteurs public et privé.

La Commission invite les parties prenantes publiques et privées à:

- favoriser l'élaboration et l'adoption de **normes de sécurité** et techniques à l'initiative des entreprises, et l'adhésion aux principes de sécurité et de respect de la vie privée dès la conception par les fabricants de produits et fournisseurs de services TIC, y compris d'informatique en nuage. Les logiciels et matériels de nouvelle génération doivent comporter des fonctions de **sécurité plus solides, intégrées et conviviales**;
- élaborer des normes de performance des entreprises, à l'initiative de celles-ci, en matière de cybersécurité et améliorer l'information du public en mettant au point des **étiquettes de sécurité** ou des labels de qualité aidant le consommateur à s'y retrouver.

Développer les investissements dans la R&D et l'innovation

La R&D peut étayer une politique industrielle forte, promouvoir un secteur européen des TIC fiable, favoriser le marché intérieur et limiter la dépendance de l'Europe vis-à-vis des technologies étrangères. La R&D doit combler les lacunes technologiques concernant la sécurité des TIC, anticiper les problèmes de sécurité futurs, prendre en compte l'évolution constante des besoins de l'utilisateur et tirer avantage des technologies à double usage. Elle doit aussi continuer à soutenir le développement de la cryptographie. Tout cela doit être complété par des efforts pour transformer les résultats de la R&D en solutions commerciales en prenant les mesures incitatives nécessaires et en créant les conditions politiques appropriées.

L'UE doit tirer le meilleur parti du programme-cadre pour la recherche et l'innovation «Horizon 2020»[29] qui doit être lancé en 2014. La proposition de la Commission comporte des objectifs spécifiques à la fiabilité des TIC et à la lutte contre la cybercriminalité, qui sont conformes à la présente stratégie. Horizon 2020 permettra de soutenir la recherche concernant les TIC émergentes; de fournir des solutions pour systèmes, services et applications TIC sûrs de bout en bout; de prendre des mesures favorisant la mise en œuvre et l'adoption des solutions existantes; et d'aborder l'interopérabilité des réseaux et systèmes informatiques. Au niveau de l'UE, on s'attachera particulièrement à optimiser et mieux coordonner les divers programmes de financement (Horizon 2020, Fonds pour la sécurité intérieure, recherche de l'AED dont la coopération-cadre européenne).

La Commission entend:

- utiliser Horizon 2020 pour aborder divers aspects de la confidentialité et de la sécurité des TIC, depuis la R&D à l'innovation et au déploiement. Horizon 2020 permettra aussi de mettre au point des outils et instruments pour lutter contre les activités criminelles et terroristes visant le cyberespace;
- instaurer des mécanismes pour mieux coordonner les agendas de recherche des institutions de l'Union européenne et des États membres et inciter ces derniers à investir davantage dans la R&D.

La Commission invite les États Membres à:

- élaborer, d'ici à la fin de 2013, de bonnes pratiques en matière de recours au **pouvoir d'achat des administrations publiques** (par les marchés publics p. ex.) pour favoriser le développement et le déploiement de fonctions de sécurité dans les produits et services TIC;
- encourager la participation précoce des entreprises et universités à l'élaboration et à la coordination des solutions. Cela doit se faire en tirant le plus grand parti de la base industrielle de l'Europe et des innovations technologiques de la R&D associée, et doit être coordonné avec les agendas de recherche des organismes civils et militaires.

La Commission invite Europol et l'ENISA à:

- recenser les tendances et besoins émergents en fonction de l'évolution de la cybercriminalité et des types de cybersécurité de façon à mettre au point des outils et technologies numériques adaptés en matière de criminalistique.

La Commission invite les parties prenantes publiques et privées à:

- élaborer, en coopération avec le secteur de l'assurance, des **barèmes harmonisés de calcul des primes de risque**, qui permettraient aux entreprises ayant investi dans la sécurité de bénéficier de tarifs moins élevés.

[29] «Horizon 2020» est l'instrument financier de mise en œuvre de l'«Union pour l'innovation», initiative phare de la stratégie Europe 2020 visant à garantir la compétitivité de l'Europe à l'échelle mondiale. Courant de 2014 à 2020, le nouveau programme-cadre de l'UE pour la recherche et l'innovation contribuera aux efforts qui visent à créer de la croissance et de nouveaux emplois en Europe.

2.5. Instaurer une politique internationale de l'Union européenne cohérente en matière de cyberespace et promouvoir les valeurs essentielles de l'UE

Préserver un cyberespace ouvert, libre et sûr constitue un défi mondial que l'UE doit relever avec les partenaires et organisations internationaux concernés, le secteur privé et la société civile.

Dans le cadre de sa politique internationale en la matière, l'UE visera à promouvoir l'ouverture et la liberté d'Internet, à encourager les efforts pour élaborer des règles de conduite et à appliquer la législation internationale existante dans le cyberespace. L'UE œuvrera aussi à réduire la fracture numérique et participera activement aux efforts internationaux pour se doter de moyens de cybersécurité. L'engagement international de l'UE concernant ces questions sera guidé par les valeurs essentielles de l'Union que sont la dignité humaine, la liberté, la démocratie, l'égalité, l'État de droit et le respect des droits fondamentaux.

Intégrer les questions inhérentes au cyberespace dans les relations extérieures et la politique étrangère et de sécurité commune (PESC) de l'UE

La Commission, la haute représentante et les États membres doivent élaborer une politique internationale de l'UE cohérente en matière de cyberespace, qui visera à renforcer l'engagement et resserrer les liens avec les principaux partenaires et organisations internationaux, ainsi qu'avec la société civile et le secteur privé. Les consultations de l'UE avec ses partenaires internationaux sur les questions inhérentes au cyberespace doivent être pensées, coordonnées et mises en œuvre de façon à procurer une valeur ajoutée aux dialogues bilatéraux existant entre les États membres de l'UE et les pays tiers. L'UE mettra aussi l'accent sur le dialogue avec les pays tiers en accordant une attention particulière à ceux qui sont dans le même état d'esprit et partagent ses valeurs. Elle préconisera d'assurer un niveau élevé de protection des données, notamment en cas de transfert de données personnelles vers un pays tiers. Pour traiter les problèmes mondiaux que pose le cyberespace, l'UE s'efforcera de coopérer plus étroitement avec les organisations qui sont actives dans ce domaine comme le Conseil de l'Europe, l'OCDE, les Nations unies, l'OSCE, l'OTAN, l'UA, l'ANASE et l'OEA. Au niveau bilatéral, la coopération avec les États-Unis est particulièrement importante et sera encore développée, notamment dans le cadre du groupe de travail UE–États-Unis sur la cybersécurité et la cybercriminalité.

L'une des finalités essentielles de cette politique internationale de l'UE sera de promouvoir le cyberespace comme un espace de liberté et de droits fondamentaux. Élargir l'accès à Internet doit faire avancer les processus de démocratisation et promouvoir les réformes démocratiques dans le monde. L'accroissement de la connectivité mondiale ne doit pas s'accompagner de censure ni de surveillance de masse. L'UE doit promouvoir la responsabilité sociale des entreprises[30] et prendre des initiatives internationales pour améliorer la coordination au niveau mondial dans ce domaine.

La responsabilité de rendre le cyberspace plus sûr incombe à tous les acteurs de la société de l'information mondiale, du particulier jusqu'à l'État, et l'UE soutient les efforts en vue de définir des règles de conduite dans le cyberespace, que toutes les parties prenantes devraient observer. De même que, dans l'UE, un individu est censé remplir ses devoirs civiques, assumer ses responsabilités sociales et respecter les lois en ligne, l'État doit se conformer aux normes et législations existantes. Sur les questions de sécurité internationale, l'UE encourage

[30] «Responsabilité sociale des entreprises: une nouvelle stratégie de l'UE pour la période 2011-2014», COM(2011) 681 final.

l'élaboration de mesures de confiance en matière de cybersécurité afin d'accroître la transparence et limiter le risque de malentendu quant à l'attitude de l'État.

L'UE ne préconise pas de créer de nouveaux instruments juridiques internationaux concernant les questions inhérentes au cyberespace.

Les obligations juridiques consacrées par le Pacte international relatif aux droits civils et politiques, la Convention européenne des droits de l'homme et la Charte des droits fondamentaux de l'UE doivent être respectées en ligne également. L'UE se concentrera sur les moyens de faire en sorte que ces mesures soient aussi appliquées dans le cyberespace.

Pour lutter contre la cybercriminalité, la convention de Budapest est un instrument ouvert à l'adoption par les pays tiers. Elle fournit un modèle pour rédiger une législation nationale en matière de cybercriminalité et constitue une base de coopération internationale dans ce domaine.

Si des conflits armés gagnent le cyberespace, le droit humanitaire international et, si nécessaire, le droit international en matière de droits de l'homme s'appliqueront au cas d'espèce.

Mettre en place davantage de moyens de cybersécurité et des infrastructures informatiques résilientes dans les pays tiers

Le bon fonctionnement des infrastructures sous-jacentes qui fournissent et facilitent les services de communications sera favorisé par une coopération internationale accrue consistant notamment en l'échange de bonnes pratiques, le partage d'informations, les exercices d'alerte rapide et de gestion conjointe des incidents, etc. L'UE contribuera à la réalisation de cet objectif en intensifiant les efforts actuellement déployés au niveau international pour renforcer les réseaux de coopération entre les pouvoirs publics et le secteur privé en matière de protection des infrastructures d'information critiques (PIIC).

Toutes les régions du monde ne bénéficient pas des effets positifs d'Internet en raison d'un manque d'accès ouvert, sûr, interopérable et fiable. L'Union européenne continuera donc à soutenir les efforts des pays pour donner à la population un plus large accès à Internet, développer l'utilisation d'Internet, assurer son intégrité et sa sécurité et lutter efficacement contre la cybercriminalité.

En coopération avec les États membres, la Commission et la haute représentante entendent:

- œuvrer à une politique internationale de l'UE cohérente en matière de cyberespace afin d'approfondir la collaboration avec les principaux partenaires et organisations internationaux, d'intégrer les questions inhérentes au cyberespace à la PESC et d'améliorer la coordination de celles qui ont une dimension mondiale;
- soutenir l'élaboration de règles de conduite et de mesures de confiance en matière de cybersécurité, faciliter le dialogue sur la façon d'appliquer le droit international existant dans le cyberespace et promouvoir la convention de Budapest pour lutter contre la cybercriminalité;
- soutenir la défense et la protection des droits fondamentaux, y compris l'accès à l'information et la liberté d'expression, en s'attachant à: a) établir de

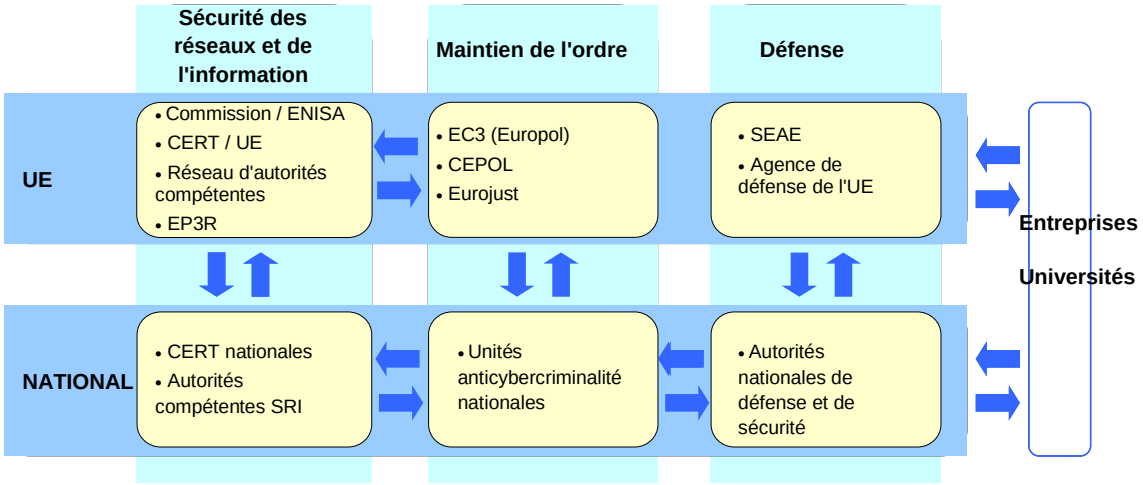
nouvelles orientations publiques sur la liberté d'expression en ligne et hors ligne; b) contrôler l'exportation des produits et services qui pourraient être utilisés à des fins de censure ou de surveillance de masse en ligne; c) mettre au point des mesures et des outils permettant d'élargir l'accès à Internet, d'accroître son ouverture et sa résilience pour échapper à la censure ou la surveillance de masse par les technologies des communications; d) habiliter les parties prenantes à utiliser les technologies des communications pour promouvoir les droits fondamentaux;

- s'employer, aux côtés des principaux partenaires et organisations internationaux, du secteur privé et de la société civile, à aider les pays tiers à se doter de moyens de portée mondiale afin d'améliorer l'accès à l'information et à un Internet ouvert, à prévenir et affronter les cybermenaces, y compris les événements accidentels, la cybercriminalité et le cyberterrorisme, et à renforcer la coordination entre les donateurs afin de canaliser les efforts dans ce sens;
- recourir à différents dispositifs d'aide de l'UE pour la mise en place de moyens de cybersécurité, y compris contribuer à la formation du personnel de maintien de l'ordre, judiciaire et technique pour faire face aux cybermenaces, ainsi qu'à la création des politiques, stratégies et institutions nationales pertinentes dans les pays tiers;
- accroître la coordination des politiques et le partage des informations à l'aide des réseaux internationaux de PIIC comme le réseau *Meridian*, ainsi que la coopération entre les autorités compétentes en matière de SRI et autres.

3. ROLES ET RESPONSABILITES

Dans la société et l'économie numériques interconnectées, les cyberincidents ne s'arrêtent pas aux frontières. Tous les acteurs, depuis les autorités compétentes en matière de SRI, les CERT et les services de maintien de l'ordre jusqu'aux entreprises, doivent assumer leurs responsabilités au niveau national et de l'UE et collaborer pour renforcer la cybersécurité. Comme cela peut exiger de recourir à différents cadres et compétences juridiques, il est essentiel pour l'UE de préciser les rôles et responsabilités des nombreux acteurs impliqués.

Étant donné la complexité de la question et la diversité des acteurs impliqués, la solution ne peut résider dans une supervision européenne centralisée. Les administrations nationales sont les mieux placées pour organiser la prévention et l'intervention en cas de cyberincident et de cyberattaque et pour établir des contacts et des réseaux avec le secteur privé et le grand public grâce aux canaux administratifs et cadres juridiques en place. En même temps, eu égard à la nature transnationale potentielle ou réelle des risques, une intervention au niveau national exigerait, dans bien des cas, une participation de l'UE pour être efficace. Pour traiter les problèmes de cybersécurité de façon exhaustive, les activités doivent couvrir trois domaines – SRI, maintien de l'ordre et défense – qui sont également régis par des cadres juridiques différents.



3.1. Coordination entre autorités compétentes en matière de SRI/CERT, maintien de l'ordre et défense

Niveau national

Les États membres devraient disposer, dès maintenant ou après mise en œuvre de la présente stratégie, de structures prenant en charge la cyber-résilience, la cybercriminalité et la cyberdéfense, et ils devraient atteindre le niveau requis de moyens pour traiter les cyberincidents. Toutefois, étant donné qu'un certain nombre d'entités peuvent avoir des responsabilités opérationnelles à différents niveaux de la cybersécurité et vu l'importance de la participation du secteur privé, la coordination au niveau national doit être optimisée entre les ministères. Les États membres devraient définir, dans leurs stratégies de cybersécurité, les rôles et responsabilités de leurs diverses entités nationales.

Le partage d'informations entre entités nationales et avec le secteur privé doit être encouragé pour permettre aux États membres et aux entreprises d'avoir une vision globale des différentes menaces et de mieux appréhender les tendances et techniques nouvelles utilisées tant pour lancer des cyberattaques que pour y réagir plus rapidement. En établissant des plans nationaux de coopération en matière de SRI à activer en cas de cyberincident, les États membres devraient pouvoir attribuer clairement les rôles et responsabilités et optimiser leurs mesures d'intervention.

Niveau de l'UE

Comme au niveau national, il y a au niveau de l'UE plusieurs acteurs prenant en charge la cybersécurité. En particulier, l'ENISA, Europol/EC3 et l'AED sont trois agences actives dans les domaines respectifs de la SRI, du maintien de l'ordre et de la défense. Ces agences ont des conseils d'administration où les États membres sont représentés et constituent des plateformes de coordination au niveau de l'UE.

La coordination et la collaboration seront encouragées, au sein de l'ENISA, d'Europol/EC3 et de l'AED, dans plusieurs domaines qui les concernent au même titre, notamment l'analyse des tendances, la gestion des risques, la formation et le partage des meilleures pratiques. Elles devraient collaborer tout en préservant leurs spécificités. Avec la CERT-UE, la Commission et les États membres, ces agences devraient aussi contribuer à la constitution d'un groupe d'experts techniques et politiques de confiance dans ce domaine.

Les canaux informels de coordination et de collaboration seront complétés par des relations plus structurées. Le personnel militaire de l'UE et l'équipe responsable du projet de cyberdéfense de l'AED peuvent servir de vecteur de coordination en matière de défense. Le comité de direction du programme d'Europol/EC3 réunira entre autres Eurojust, le CEPOL, les États membres[31], l'ENISA et la Commission et permettra de partager leur savoir-faire respectif et d'assurer que les actions de l'EC3 sont menées en partenariat, eu égard à l'expertise additionnelle et aux mandats de toutes les parties prenantes. Le nouveau mandat de l'ENISA doit lui permettre de resserrer les liens avec Europol et de développer les relations avec les parties prenantes industrielles. Surtout, la proposition législative de la Commission sur la SRI instaurerait un cadre de coopération par l'intermédiaire d'un réseau d'autorités nationales compétentes en la matière et le partage des informations entre ces dernières et les autorités de maintien de l'ordre.

Niveau international

La Commission et la haute représentante assurent, avec les États membres, la coordination de l'action internationale dans le domaine de la cybersécurité. Ce faisant, la Commission et la haute représentante s'emploieront à défendre les valeurs essentielles de l'UE et à promouvoir une utilisation pacifique, ouverte et transparente des cybertechnologies. La Commission, la haute représentante et les États membres maintiennent un dialogue politique avec leurs partenaires internationaux et des organisations internationales comme le Conseil de l'Europe, l'OCDE, l'OSCE, l'OTAN et les Nations unies.

3.2. Soutien de l'UE en cas de cyberincident ou cyberattaque majeurs

Les cyberincidents ou cyberattaques majeurs sont susceptibles d'avoir un impact sur les pouvoirs publics, les entreprises et les particuliers dans l'UE. Une fois mise en œuvre la présente stratégie et, en particulier, la directive SRI proposée, la prévention, la détection et l'intervention en cas de cyberincident devraient être plus efficaces et les États membres et la Commission devraient se tenir mieux informés des cyberincidents ou cyberattaques majeurs. Cependant, les mécanismes d'intervention différeront en fonction de la nature, de l'ampleur et des incidences transnationales de l'incident.

Si l'incident a un impact sérieux sur la continuité des activités, la directive SRI propose que soient déclenchés les plans de coopération en matière de SRI, nationaux ou de l'Union selon la nature nationale ou transnationale de l'incident. Dans ce contexte, le réseau d'autorités compétentes en matière de SRI servirait au partage des informations et au soutien. Cela permettrait de préserver et/ou de restaurer les réseaux et services touchés.

Si l'incident semble relever d'un délit, Europol/EC3 devraient être informés afin que, avec les autorités de maintien de l'ordre des pays concernés, ils puissent ouvrir une enquête, préserver les éléments de preuve, identifier les auteurs et enfin veiller à ce que ces derniers soient poursuivis.

Si l'incident semble relever du cyberespionnage ou s'apparenter à une attaque commanditée par un État ou a des conséquences pour la sécurité nationale, les autorités nationales de sécurité et de défense alerteront leurs homologues afin qu'ils sachent qu'ils font l'objet d'une attaque et qu'ils puissent se défendre. Les mécanismes d'alerte rapide seront alors activés et, si nécessaire, les procédures de gestion des crises ou autres seront déclenchées. Un

[31] Par l'intermédiaire de leurs représentants au sein de la *task force* de l'UE sur la cybercriminalité, qui se compose des chefs des unités anticybercriminalité des États membres.

cyberincident ou une cyberattaque particulièrement sérieux pourraient constituer un motif suffisant pour qu'un État membre invoque la clause de solidarité de l'UE (article 222 du traité sur le fonctionnement de l'Union européenne).

Si l'incident semble avoir compromis des données à caractère personnel, les autorités nationales de protection des données ou les autorités réglementaires nationales conformément à la directive 2002/58/CE devraient être impliquées.

Enfin, la gestion des cyberincidents et cyberattaques sera facilitée par les réseaux de contact et le soutien des partenaires internationaux, celui-ci pouvant consister en des solutions techniques, des enquêtes criminelles ou l'activation de mécanismes de gestion des crises et d'intervention.

4. CONCLUSION ET SUIVI

La présente stratégie de cybersécurité de l'Union européenne, proposée par la Commission et la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, expose la vision de l'UE et définit les actions requises, fondées sur une protection et une promotion efficaces des droits individuels, pour que l'environnement en ligne de l'UE soit le plus sûr au monde[32].

Cette vision ne peut se concrétiser que par un véritable partenariat entre les nombreux intervenants, garantissant que les responsabilités soient prises pour relever les défis qui se profilent.

La Commission et la haute représentante invitent donc le Conseil et le Parlement européen à approuver la stratégie et à contribuer à la réalisation des actions décrites. Un soutien et un engagement résolus sont également exigés du secteur privé et de la société civile, lesquels sont des acteurs clés pour relever notre niveau de sécurité et préserver les droits individuels.

C'est maintenant qu'il faut agir. Aussi la Commission et la haute représentante sont-elles déterminées à collaborer avec tous les acteurs pour assurer la sécurité nécessaire à l'Europe. Pour faire en sorte que la stratégie soit mise en œuvre rapidement et évaluée en fonction des éventuelles évolutions, elles réuniront toutes les parties prenantes dans le cadre d'une conférence à haut niveau et mesureront les progrès accomplis en 12 mois.

[32] Le financement de la stratégie sera assuré dans la limite des montants prévus pour chacun des domaines politiques concernés (MIE, Horizon 2020, Fonds pour la sécurité intérieure, PESC et coopération extérieure, notamment l'instrument de stabilité) comme indiqué dans la proposition de la Commission concernant le cadre financier pluriannuel 2014-2020 (sous réserve de l'approbation par l'autorité budgétaire et des montants définitifs du CFP adopté pour 2014-2020). En ce qui concerne la nécessité d'assurer la compatibilité globale avec le nombre de postes disponibles pour les agences décentralisées et le sous-plafond pour les agences décentralisées à chaque rubrique de dépenses dans le prochain CFP, les agences (CEPOL, AED, ENISA, Eurojust et Europol/EC3) auxquelles il est demandé d'exercer de nouvelles tâches, en vertu de la présente communication, seront encouragées à le faire dans la mesure où la capacité réelle de l'agence à absorber des ressources supplémentaires aura été établie et où toutes les possibilités de redéploiement auront été recensées.