Parlement européen
2014-2019

TEXTES ADOPTÉS

P8_TA(2017)0366

Lutte contre la cybercriminalité

Résolution du Parlement européen du 3 octobre 2017 sur la lutte contre la cybercriminalité (2017/2068(INI))

Le Parlement européen,

– vu les articles 2, 3 et 6 du traité sur l'Union européenne (traité UE),

– vu les articles 16, 67, 70, 72, 73, 75, 82, 83, 84, 85, 87 et 88 du traité sur le fonctionnement de l'Union européenne (traité FUE),

– vu les articles 1, 7, 8, 11, 16, 17, 21, 24, 41, 47, 48, 49, 50 et 52 de la charte des droits fondamentaux de l'Union européenne,

– vu la convention des Nations unies relative aux droits de l'enfant du 20 novembre 1989,

– vu le protocole facultatif à la convention relative aux droits de l'enfant, concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants, du 25 mai 2000,

– vu la déclaration de Stockholm et le programme d'action adoptés lors du premier Congrès mondial contre l'exploitation sexuelle des enfants à des fins commerciales, l'engagement mondial de Yokohama adopté lors du deuxième Congrès mondial contre l'exploitation sexuelle des enfants à des fins commerciales, l'engagement et le plan d'action de Budapest, adoptés à l'issue de la conférence préparatoire du deuxième Congrès mondial contre l'exploitation sexuelle des enfants à des fins commerciales,

– vu la convention du Conseil de l'Europe du 25 octobre 2007 sur la protection des enfants contre l'exploitation et les abus sexuels,

– vu sa résolution du 20 novembre 2012 sur la protection des enfants dans le monde numérique[1],

– vu sa résolution du 11 mars 2015 sur la lutte contre la pédopornographie sur l'internet[2],

– vu la décision-cadre 2001/413/JAI du Conseil du 28 mai 2001 concernant la lutte contre

1 JO C 419 du 16.12.2015, p. 33.
2 JO C 316 du 30.8.2016, p. 109.

la fraude et la contrefaçon des moyens de paiement autres que les espèces[1],

– vu la convention de Budapest sur la cybercriminalité du 23 novembre 2001[2] et son protocole additionnel,

– vu le règlement (CE) nº 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information[3],

– vu la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection[4],

– vu la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques[5],

– vu la directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil[6],

– vu la communication conjointe du 7 février 2013 au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, de la Commission et de la vice-présidente de la Commission et haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, intitulée «Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé» (JOIN(2013)0001),

– vu la directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil[7],

– vu la directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale[8],

– vu l'arrêt de la Cour de justice de l'Union européenne du 8 avril 2014[9] invalidant la directive sur la conservation des données,

– vu sa résolution du 12 septembre 2013 sur la stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé[10],

– vu la communication de la Commission du 6 mai 2015, intitulée «Stratégie pour un

---

1 JO L 149 du 2.6.2001, p. 1.
2 Conseil de l'Europe, Série des traités européens nº 185, 23.11.2001.
3 JO L 77 du 13.3.2004, p. 1.
4 JO L 345 du 23.12.2008, p. 75.
5 JO L 201 du 31.7.2002, p. 37.
6 JO L 335 du 17.12.2011, p. 1.
7 JO L 218 du 14.8.2013, p. 8.
8 JO L 130 du 1.5.2014, p. 1.
9 ECLI:EU:C:2014:238.
10 JO C 93 du 9.3.2016, p. 112.

marché unique numérique en Europe» (COM(2015)0192),

– vu la communication de la Commission du 28 avril 2015 intitulée «Le programme européen en matière de sécurité» (COM(2015)0185) et les rapports de suivi portant sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective,

– vu le rapport de la conférence sur les règles de compétence dans le cyberespace, qui s'est tenue à Amsterdam les 7 et 8 mars 2016,

– vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)[1],

– vu la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil[2],

– vu le règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol)[3],

– vu la décision de la Commission du 5 juillet 2016 relative à la signature d'un accord contractuel concernant un partenariat public-privé pour la recherche et l'innovation industrielles dans le domaine de la cybersécurité entre l'Union européenne, représentée par la Commission, et l'organisation partenaire (C(2016)4400),

– vu la communication conjointe au Parlement européen et au Conseil du 6 avril 2016 de la vice-présidente de la Commission et haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, intitulée «Cadre commun en matière de lutte contre les menaces hybrides: une réponse de l'Union européenne» (JOIN(2016)0018),

– vu la communication de la Commission intitulée «Stratégie européenne pour un Internet mieux adapté aux enfants» (COM(2012)0196) et le rapport de la Commission du 6 juin 2016 intitulé «Évaluation finale du programme pluriannuel de l'Union visant à protéger les enfants lors de l'utilisation de l'internet et d'autres technologies de communication (Internet plus sûr)» (COM(2016)0364),

– vu la déclaration commune d'Europol et de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) du 20 mai 2016 sur des pratiques d'enquêtes criminelles légales qui respectent les exigences du XXI^{e} siècle en matière de protection des données,

– vu les conclusions du Conseil du 9 juin 2016 concernant le réseau judiciaire européen

---

1 JO L 119 du 4.5.2016, p. 1.
2 JO L 119 du 4.5.2016, p. 89.
3 JO L 135 du 24.5.2016, p. 53

en matière de cybercriminalité,

– vu la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union[1],

– vu l'avis émis par l'ENISA en décembre 2016 sur le chiffrement intitulé «Un chiffrement fort sauvegarde notre identité numérique»,

– vu le rapport final du groupe sur les preuves dans le nuage (Cloud Evidence Group) T-CY du Conseil de l'Europe intitulé «Accès de la justice pénale aux preuves électroniques dans le cloud: Recommandations pour examen par le T-CY», du 16 septembre 2016,

– vu les travaux de la force d'action anticybercriminalité européenne (J-CAT),

– vu l'évaluation de la menace que représente la grande criminalité organisée (SOCTA) du 28 février 2017 et l'évaluation de la menace que représente la criminalité organisée sur l'internet (IOCTA) du 28 septembre 2016, réalisées par Europol,

– vu l'arrêt de la CJUE dans l'affaire C-203/15 (arrêt TELE2) du 21 décembre 2016[2],

– vu la directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil[3],

– vu l'article 52 de son règlement intérieur,

– vu le rapport de la commission des libertés civiles, de la justice et des affaires intérieures et l'avis de la commission du marché intérieur et de la protection des consommateurs (A8-0272/2017),

A. considérant que la cybercriminalité cause des dommages économiques et sociaux de plus en plus importants, ayant une incidence sur les droits fondamentaux des particuliers, posant une menace à l'encontre de l'état de droit dans le cyberespace et mettant en danger la stabilité de nos sociétés démocratiques;

B. considérant que la cybercriminalité est un problème d'ampleur croissante dans les États membres;

C. considérant que l'IOCTA de 2016 indique que la cybercriminalité augmente en intensité, en complexité et en ampleur, que la cybercriminalité déclarée dépasse la criminalité traditionnelle dans certains pays de l'Union européenne, qu'elle s'étend à d'autres domaines de la criminalité, tels que la traite des êtres humains, que l'utilisation des outils de chiffrement et d'anonymisation à des fins criminelles se développe et que les attaques à l'aide de rançongiciels sont plus nombreuses que les menaces posées par

---

1 JO L 194 du 19.7.2016, p. 1.

2 Arrêt de la Cour de justice de l'Union européenne du 21 décembre 2016, *Tele2 Sverige AB* contre *Post- och telestyrelsen* et *Secretary of State for the Home Department* contre *Tom Watson e.a.*, C-203/15, ECLI:EU:C:2016:970.

3 JO L 88 du 31.3.2017, p. 6.

les logiciels malveillants classiques tels que des chevaux de Troie;

D. considérant que le nombre d'attaques visant les serveurs de la Commission a augmenté de 20 % en 2016 par rapport à 2015;

E. considérant que la vulnérabilité des ordinateurs face aux attaques est due au développement particulier des technologies de l'information ces dernières années, à la vitesse à laquelle le commerce se développe en ligne et à l'absence d'intervention des pouvoirs publics;

F. considérant qu'il existe un marché noir qui ne cesse de croître de l'extorsion informatique, de l'utilisation de réseaux zombies loués, du piratage et du vol de biens numériques;

G. considérant que les logiciels malveillants, tels que les chevaux de Troie bancaires, constituent toujours l'élément central des attaques informatiques, mais que les attaques visant à détruire des infrastructures critiques, des structures économiques et à déstabiliser les sociétés, comme lors de l'attaque du rançongiciel «Wannacry» en mai 2017, sont également de plus en plus nombreuses et ont de plus en plus de conséquences, et constituent donc une menace croissante pour la sécurité, la défense et d'autres secteurs importants; que la majorité des demandes internationales de données par des autorités répressives sont relatives à la fraude et la criminalité financière, suivies des formes violentes et graves de criminalité;

H. considérant que, tout en apportant de nombreux avantages, l'interconnexion toujours croissante des personnes, des lieux et des choses augmente le risque de cybercriminalité; que les dispositifs connectés à l'internet des objets, comme les réseaux intelligents, les réfrigérateurs connectés, les voitures, et les instruments ou les outils médicaux, sont souvent moins bien protégés que les dispositifs traditionnels connectés à l'internet et constituent donc une cible idéale pour les cybercriminels, notamment parce que le régime des mises à jour de sécurité des dispositifs connectés est souvent lacunaire voire inexistant; que les dispositifs de l'internet des objets piratés qui contrôlent ou sont capables de contrôler des actionneurs physiques peuvent représenter une menace réelle pour la vie d'êtres humains;

I. considérant qu'un cadre juridique efficace pour la protection des données est indispensable pour instaurer la confiance dans le monde en ligne et permettre tant aux consommateurs qu'aux entreprises de tirer pleinement profit des avantages du marché unique numérique et de lutter contre la cybercriminalité;

J. considérant que les entreprises ne peuvent relever seules le défi qui consiste à rendre le monde connecté plus sûr et que les gouvernements devraient renforcer la cybersécurité au moyen de règlements et de mesures incitatives favorisant un comportement plus sûr des utilisateurs;

K. considérant que les lignes entre la cybercriminalité, le cyberespionnage, la guerre informatique, le cybersabotage et le cyberterrorisme sont de plus en plus floues; que la cybercriminalité peut cibler des individus, des entités publiques ou bien privées et couvrir un large éventail d'infractions, y compris les atteintes à la vie privée, les abus sexuels commis contre des enfants en ligne, l'incitation publique à la violence ou à la haine, le sabotage, l'espionnage, la criminalité financière et la fraude, comme la fraude

aux paiements, le vol et l'usurpation d'identité, ainsi que l'atteinte illégale à l'intégrité de systèmes;

L. considérant que, dans son rapport 2017 sur les risques mondiaux, le Forum économique mondial classe un incident de falsification et de vol de données de grande ampleur parmi les cinq risques mondiaux les plus susceptibles de se produire;

M. considérant qu'un nombre considérable d'actes de cybercriminalité ne font l'objet d'aucune poursuite et demeurent impunis; qu'une sous-déclaration importante, de longues périodes de détection permettant aux cybercriminels de développer des entrées/sorties multiples ou des portes dérobées, un accès peu aisé aux preuves électroniques, des difficultés à se les procurer et à faire valoir leur recevabilité en justice, ainsi que la complexité des procédures et des problèmes de compétence liés à la nature transfrontalière de la cybercriminalité restent monnaie courante;

N. considérant que le Conseil, dans ses conclusions de juin 2016, a souligné que, vu la nature transfrontalière de la cybercriminalité et les menaces communes en matière de cybersécurité auxquelles l'Union européenne est confrontée, il est essentiel de renforcer la coopération et l'échange d'informations entre les autorités policières et judiciaires et les experts en cybercriminalité pour mener des enquêtes efficaces dans le cyberespace et obtenir des preuves électroniques;

O. considérant que l'invalidation de la directive sur la conservation des données par la Cour de justice de l'Union européenne (ci-après «la Cour») dans son arrêt du 8 avril 2014, de même que l'interdiction d'une conservation généralisée, indifférenciée et non ciblée des données, confirmée par l'arrêt TELE2 de la Cour du 21 décembre 2016, imposent des limites strictes au traitement des données de télécommunications en masse ainsi qu'à l'accès des autorités compétentes à ces données;

P. considérant que l'arrêt Maximillian Schrems de la Cour[1] souligne que la surveillance de masse constitue une violation des droits fondamentaux;

Q. considérant que la lutte contre la cybercriminalité doit respecter les mêmes garanties procédurales et substantielles et les mêmes droits fondamentaux que la lutte contre toute autre domaine criminel, notamment en matière de protection des données et de liberté d'expression;

R. considérant que les enfants utilisent l'internet de plus en plus tôt et qu'ils sont particulièrement vulnérables face au risque d'être victimes du pédopiégeage et d'autres formes d'exploitation sexuelle en ligne (harcèlement en ligne, abus sexuels, coercition et extorsion sexuelles), du détournement de leurs données personnelles, ainsi que de campagnes dangereuses visant à promouvoir différentes formes d'autodestruction, comme dans l'affaire «blue whale», et qu'ils nécessitent donc une protection spéciale; considérant qu'en ligne, les délinquants peuvent trouver et piéger plus rapidement leurs victimes en se servant des messageries instantanés, des courriels, des jeux en ligne et des sites de réseaux sociaux, et que les réseaux peer-to-peer (P2P) cachés restent les plateformes centrales sur lesquelles les pédophiles accèdent aux contenus pédopornographiques, transmettent, stockent et partagent ces contenus, et trouvent de

[1] ECLI:EU:C:2015:650.

nouvelles victimes sans être repérés;

S. considérant que la hausse de la coercition et de l'extorsion sexuelles demeure insuffisamment étudiée et signalée, principalement en raison de la nature du crime, qui entraîne un sentiment de honte et de culpabilité chez les victimes;

T. considérant que les abus à l'encontre d'enfants à distance retransmis en direct sont signalés comme une menace grandissante; que les abus à l'encontre d'enfants à distance retransmis en direct entretiennent des liens évidents avec la distribution commerciale de contenus pédopornographiques;

U. considérant qu'une étude récente de l'Agence nationale de lutte contre la criminalité au Royaume-Uni a démontré que les personnes plus jeunes qui se livrent à des activités de piratage sont moins motivées par l'argent et attaquent souvent des réseaux informatiques pour impressionner leurs amis ou protester contre un système politique;

V. considérant que la sensibilisation aux risques posés par la cybercriminalité a augmenté, mais que les mesures de précaution prises par les utilisateurs individuels, les institutions publiques et les entreprises demeurent tout à fait insuffisantes, essentiellement en raison d'un manque de connaissances et de ressources;

W. considérant que la lutte contre la cybercriminalité et contre les activités en ligne illégales ne devrait pas masquer les aspects positifs d'un cyberespace gratuit et ouvert, qui offre de nouvelles possibilités en matière de partage des connaissances et de promotion de l'intégration politique et sociale à travers le monde;

Considérations générales

1. souligne que la forte augmentation des rançongiciels, des réseaux zombies et des actions non autorisées qui perturbent les systèmes informatiques a une incidence sur la sécurité des personnes, la disponibilité et l'intégrité de leurs données à caractère personnel, ainsi que sur la protection de la vie privée et des libertés fondamentales, et l'intégrité des infrastructures critiques dont, entre autres, les structures d'approvisionnement en énergie et en électricité et les structures financières telles que la Bourse; rappelle, à cet égard, que la lutte contre la cybercriminalité est une priorité reconnue dans le cadre du programme européen en matière de sécurité du 28 avril 2015;

2. souligne la nécessité de clarifier les définitions communes de la cybercriminalité, de la guerre informatique, de la cybersécurité, du harcèlement en ligne et des attaques informatiques pour s'assurer que les institutions de l'Union et les États membres partagent des définitions juridiques communes;

3. souligne que la lutte contre la cybercriminalité devrait viser avant tout la protection et le renforcement des infrastructures critiques et autres dispositifs en réseau, et pas uniquement la mise en œuvre de mesures répressives;

4. rappelle l'importance des mesures juridiques prises au niveau européen afin d'harmoniser la définition des infractions liées aux attaques contre les systèmes d'information ainsi qu'aux abus sexuels contre des enfants et à leur exploitation sexuelle en ligne, et d'obliger les États membres à mettre en place un système d'enregistrement, de production et de communication de statistiques sur ces infractions, afin de lutter plus efficacement contre ces formes de criminalité;

5. prie instamment les États membres qui ne l'ont pas encore fait de transposer rapidement et correctement la directive 2011/93/UE relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie; invite donc la Commission à surveiller strictement et à garantir sa mise en œuvre pleine et effective, ainsi qu'à communiquer ses conclusions en temps utile au Parlement et à la commission compétente, tout en remplaçant en même temps la décision-cadre 2004/68/JAI du Conseil; souligne qu'Eurojust et Europol doivent recevoir les ressources appropriées pour améliorer l'identification des victimes, combattre les réseaux organisés d'agresseurs sexuels et accélérer la détection, l'analyse et le signalement de contenus pédopornographiques tant en ligne que hors ligne;

6. déplore le fait que 80 % des entreprises en Europe ont connu au moins un incident de cybersécurité et que les attaques informatiques à l'encontre d'entreprises passent souvent inaperçues ou ne sont pas déclarées; rappelle que, selon plusieurs études, le coût annuel des attaques informatiques pour l'économie mondiale est non négligeable; estime que l'obligation de révéler les failles de sécurité et de partager des informations sur les risques, introduite par le règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) et par la directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (directive sur la sécurité des réseaux et des systèmes d'information, ou directive SRI), contribuera à remédier à ce problème en apportant un soutien aux entreprises, notamment aux petites et moyennes entreprises (PME);

7. souligne que l'évolution constante du paysage des cybermenaces pose pour toutes les parties prenantes de graves problèmes juridiques et technologiques; estime que les nouvelles technologies ne devraient pas être vues comme une menace et indique que les progrès technologiques en matière de chiffrement amélioreront la sécurité globale de nos systèmes d'information, notamment en permettant aux utilisateurs finaux de mieux protéger leurs données et leurs communications; souligne toutefois que des lacunes considérables persistent en matière de sécurisation des communications et que les technologies telles que le routage en oignon et les réseaux cachés peuvent être employées par des utilisateurs malintentionnés, y compris des terroristes et des pédophiles, des pirates informatiques parrainés par des pays étrangers non amis ou des organisations religieuses ou politiques extrémistes à des fins criminelles, en particulier pour dissimuler leurs activités criminelles ou leur identité, ce qui entraîne de sérieuses complications dans les enquêtes;

8. est très préoccupé par la récente attaque mondiale par rançongiciel qui aurait touché des dizaines de milliers d'ordinateurs dans près de 100 pays et dans de nombreuses organisations, y compris le Service national de santé (NHS) du Royaume-Uni, victime la plus connue de cette attaque massive par logiciel malveillant; salue, dans ce contexte, le travail crucial de l'initiative No More Ransom (NMR) qui met à disposition des victimes de rançongiciels partout dans le monde plus de 40 outils de déchiffrement gratuits leur permettant de décrypter les dispositifs touchés;

9. souligne que les réseaux cachés et le routage en oignon garantissent par ailleurs, dans certains pays, un espace libre et à l'abri de toute détection par les autorités publiques répressives pour les journalistes, les militants politiques et les défenseurs des droits de l'homme;

10. constate que le recours, par les réseaux criminels et terroristes, à des outils et des services de cybercriminalité demeure limité; souligne, toutefois, que cette situation pourrait changer à la lumière des liens de plus en plus étroits entre terrorisme et criminalité organisée, ainsi que de la disponibilité considérable d'armes à feu et de précurseurs d'explosifs sur les réseaux cachés;

11. condamne fermement toute atteinte à l'intégrité d'un système portée ou dirigée par un pays étranger ou par ses agents dans le but de perturber le processus démocratique d'un autre pays;

12. souligne que les demandes transfrontalières de saisie de domaine, de suppression de contenu et d'accès aux données des utilisateurs posent d'épineux problèmes qui imposent une réaction prompte dans la mesure où les enjeux sont de taille; insiste, dans ce contexte, sur le fait que les cadres internationaux en matière de droits de l'homme, qui s'appliquent en ligne et hors ligne, représentent un critère de référence important au niveau mondial;

13. invite les États membres à veiller à ce que les victimes d'attaques informatiques puissent bénéficier pleinement de tous les droits inscrits dans la directive 2012/29/UE, et à redoubler d'efforts en ce qui concerne l'identification des victimes et les services qui leur sont destinés, notamment en apportant un soutien continu au groupe de travail d'Europol sur l'identification des victimes; invite les États membres, en coopération avec Europol, à mettre en place de toute urgence des plateformes actives à ce sujet en vue de veiller à ce que tous les utilisateurs de l'internet sachent comment demander de l'aide lorsqu'ils sont la cible d'activités illégales en ligne; invite la Commission à publier une étude sur les répercussions de la cybercriminalité transfrontalière en se fondant sur la directive 2012/29/UE;

14. souligne que l'IOCTA 2014 d'Europol évoque le besoin d'instruments juridiques plus performants et plus efficaces en tenant compte des limites actuelles du processus du traité d'entraide judiciaire (TEJ), et préconise également davantage d'harmonisation de la législation à travers l'Union le cas échéant;

15. souligne que la cybercriminalité affecte gravement le fonctionnement du marché unique numérique en sapant la confiance dans les fournisseurs de services numériques, en compromettant les transactions transfrontalières et en portant gravement atteinte aux intérêts des consommateurs de services numériques;

16. insiste sur le fait que les stratégies et les mesures de cybersécurité ne peuvent être judicieuses et efficaces que si elles sont fondées sur les libertés et les droits fondamentaux, tels qu'ils sont consacrés dans la charte des droits fondamentaux de l'Union européenne, et sur les principes fondamentaux de l'Union;

17. souligne qu'il existe un grand besoin légitime de protection des communications entre particuliers ainsi qu'entre les particuliers et les organisations publiques et privées à des fins de prévention de la cybercriminalité; précise qu'une cryptographie solide peut contribuer à satisfaire ce besoin; insiste par ailleurs sur le fait que limiter l'utilisation ou réduire la puissance des outils cryptographiques fera apparaître des vulnérabilités pouvant être exploitées à des fins criminelles et érodera la confiance dans les services électroniques, ce qui aura des répercussions négatives sur la société civile comme sur les entreprises du secteur;

18. demande l'adoption d'un plan d'action pour la protection des droits des enfants en ligne et hors ligne dans le cyberespace, et rappelle que les autorités répressives doivent porter une attention particulière aux infractions commises contre des enfants dans leur lutte contre la cybercriminalité; souligne, à cet égard, la nécessité de renforcer la coopération judiciaire et policière entre les États membres, ainsi qu'avec Europol et son Centre européen de lutte contre la cybercriminalité (EC3), à des fins de prévention et de lutte contre la cybercriminalité et, en particulier, l'exploitation sexuelle des enfants en ligne;

19. exhorte la Commission et les États membres à mettre en place toutes les mesures juridiques nécessaires pour lutter contre le phénomène de la violence en ligne à l'égard des femmes et le harcèlement en ligne; demande, en particulier, à l'Union et aux États membres d'unir leurs forces en vue de créer un cadre pénal obligeant les sociétés de l'internet à supprimer les contenus dégradants, offensants et humiliants ou à en arrêter la propagation; demande également la mise en place d'un soutien psychologique pour les femmes victimes de violence en ligne et les jeunes filles victimes de harcèlement en ligne;

20. souligne qu'il convient que les contenus illicites en ligne soient supprimés immédiatement par toutes voies de droit; souligne le rôle des technologies de l'information et des communications, des fournisseurs de services internet et des fournisseurs d'hébergement internet dans la suppression rapide et efficace de contenu illicite en ligne à la demande de l'autorité répressive responsable;

Prévention

21. invite la Commission, dans le contexte de la révision de la stratégie de cybersécurité de l'Union européenne, à continuer à repérer les vulnérabilités en matière de sécurité des réseaux et de l'information dans les infrastructures critiques européennes, à favoriser le développement de systèmes résilients et à évaluer la situation en ce qui concerne la lutte contre la cybercriminalité dans l'Union et les États membres, afin de parvenir à une meilleure compréhension des tendances et de l'évolution de la situation en ce qui concerne les infractions dans le cyberespace;

22. souligne que la cyber-résilience est essentielle dans la prévention de la cybercriminalité et devrait donc se voir accorder la plus haute priorité; invite les États membres à adopter des politiques et des mesures proactives pour la défense des réseaux et des infrastructures critiques, et appelle de ses vœux une approche européenne globale en matière de lutte contre la cybercriminalité qui soit compatible avec les droits fondamentaux, la protection des données, la cybersécurité, la protection des consommateurs et le commerce électronique;

23. salue, à cet égard, l'investissement de fonds de l'Union dans des projets de recherche tels que le partenariat public-privé en matière de cybersécurité (PPP Cybersécurité), qui vise à développer la cyber-résilience européenne grâce à l'innovation et au renforcement des capacités; reconnaît en particulier les efforts déployés par le PPP Cybersécurité pour élaborer des réponses appropriées pour la gestion des «vulnérabilités jour zéro»;

24. souligne, à cet égard, l'importance des logiciels libres et ouverts; demande que davantage de fonds de l'Union soient mis spécifiquement à la disposition de la recherche en sécurité informatique fondée sur des logiciels libres et ouverts;

25. déplore la pénurie de professionnels de l'informatique spécialisés dans la cybersécurité; exhorte les États membres à investir dans l'éducation;

26. estime que la réglementation devrait jouer un rôle plus prépondérant dans la gestion des risques en matière de cybersécurité, en améliorant les normes de conception et de mise à jour des produits et des logiciels ainsi que les normes minimales relatives aux identifiants et aux mots de passe par défaut;

27. invite instamment les États membres à intensifier les échanges d'informations, par l'intermédiaire d'Eurojust, d'Europol et de l'ENISA, ainsi que le partage des meilleures pratiques via le réseau européen des CSIRT (centres de réponse aux incidents de sécurité informatique) et des CERT (centres de réponse aux urgences informatiques), en ce qui concerne les problèmes auxquels ils sont confrontés dans la lutte contre la cybercriminalité, ainsi que les solutions juridiques et techniques concrètes pour y remédier et accroître la cyber-résilience; invite la Commission, à cet égard, à promouvoir une coopération efficace et à faciliter l'échange d'informations en vue d'anticiper et de gérer les risques potentiels, tel que prévu dans la directive SRI;

28. est préoccupé par le fait qu'Europol a constaté que la majorité des attaques menées avec succès contre des particuliers sont imputables à un manque d'hygiène numérique et de sensibilisation des utilisateurs, ou au fait qu'une attention insuffisante est accordée aux mesures techniques de sécurité telles que la sécurité dès la conception; souligne que les utilisateurs sont les premières victimes du matériel et des logiciels mal protégés;

29. invite la Commission et les États membres à lancer une campagne de sensibilisation associant tous les acteurs et parties prenantes pertinents afin d'accroître l'autonomie des enfants et d'aider les parents, les personnes responsables des enfants et les acteurs éducatifs à comprendre et à gérer les risques en ligne ainsi qu'à protéger la sécurité des enfants en ligne, à appuyer les États membres dans la mise en place des programmes de prévention des abus sexuels en ligne, à promouvoir les campagnes de sensibilisation relatives aux comportements responsables sur les médias sociaux et à inciter les principaux moteurs de recherche et réseaux sociaux à adopter une démarche proactive à l'égard de la protection de la sécurité des enfants en ligne;

30. invite la Commission et les États membres à lancer des campagnes de sensibilisation, d'information et de prévention, ainsi qu'à promouvoir les bonnes pratiques afin de veiller à ce que tous les citoyens, en particulier les enfants et les autres utilisateurs vulnérables, mais aussi les administrations centrales et locales, les opérateurs d'importance vitale et les acteurs du secteur privé, notamment les PME, aient conscience des risques posés par la cybercriminalité, connaissent les mesures garantissant leur sécurité en ligne et sachent comment protéger leurs dispositifs; invite en outre la Commission et les États membres à promouvoir des mesures de sécurité concrètes, telles que le chiffrement ou d'autres technologies renforçant la sécurité et la protection de la vie privée et des outils d'anonymisation;

31. souligne que les campagnes de sensibilisation devraient être assorties de programmes éducatifs concernant l'«utilisation avisée» des instruments des technologies de l'information; encourage les États membres à inclure, dans les programmes scolaires de sciences informatiques, la cybersécurité ainsi que les risques et les conséquences de l'utilisation de données à caractère personnel en ligne; souligne à cet égard les efforts déployés dans le cadre de la stratégie européenne pour un internet mieux adapté aux

enfants (stratégie BIK 2012);

32. souligne la nécessité urgente, dans la lutte contre la cybercriminalité, de prévoir davantage d'efforts en matière d'éducation et de formation à la sécurité des réseaux et de l'information (SRI), en instaurant une formation sur la SRI, sur le développement de logiciels sécurisés et sur la protection des données à caractère personnel pour les étudiants en sciences informatiques, ainsi qu'une formation de base sur la SRI pour le personnel employé dans l'administration publique;

33. estime qu'une assurance contre le piratage informatique pourrait être l'un des outils encourageant les actions dans le domaine de la sécurité, de la part des entreprises responsables de l'architecture logicielle et des utilisateurs incités à faire bon usage des logiciels;

34. souligne que les entreprises devraient repérer les vulnérabilités et les risques au moyen d'évaluations régulières, protéger leurs produits et leurs services en remédiant immédiatement aux vulnérabilités, notamment grâce à des politiques de gestion des correctifs et des mises à jour en matière de protection des données, atténuer les incidences des attaques par rançongiciels en mettant en place des systèmes de secours fiables et signaler systématiquement les attaques informatiques;

35. prie instamment les États membres de créer des CERT auxquels les entreprises et les consommateurs pourront signaler les sites internet et les courriels malveillants, comme le prévoit la directive SRI, afin que les États membres soient régulièrement informés des incidents de sécurité et des mesures permettant de combattre et d'atténuer les risques pesant sur leurs propres systèmes; encourage les États membres à envisager la création d'une base de données pour recenser tous les types de cybercriminalité et surveiller l'évolution des phénomènes en question;

36. prie instamment les États membres d'investir dans une meilleure sécurisation de leurs infrastructures critiques et données connexes afin de faire face aux attaques informatiques;

Renforcement de la responsabilité des fournisseurs de services

37. estime que le renforcement de la coopération entre les autorités compétentes et les fournisseurs de services est un facteur clé pour accélérer et rationaliser l'entraide judiciaire et les procédures de reconnaissance mutuelle, dans les domaines de compétence prévus dans le cadre juridique européen; invite les fournisseurs de services de communications électroniques établis dans un pays tiers à désigner par écrit un représentant auprès de l'Union européenne;

38. rappelle qu'en ce qui concerne l'internet des objets, les producteurs constituent la source principale de l'amélioration des régimes de responsabilité, pour aboutir à des produits de meilleure qualité et à un environnement plus sûr au regard de l'accès externe ainsi qu'à une fonction d'actualisation documentée;

39. estime, compte tenu des tendances de l'innovation et de l'accessibilité croissante des dispositifs de l'internet des objets, qu'il convient d'apporter une attention particulière à la sécurité de tous les dispositifs, y compris les plus basiques; considère qu'il est dans l'intérêt des producteurs de matériel informatique et des développeurs de logiciels

innovants d'investir dans des solutions visant à prévenir la cybercriminalité et à échanger des informations sur les menaces en matière de cybersécurité; prie instamment la Commission et les États membres de promouvoir l'option de la sécurité dès la conception et exhorte les entreprises du secteur à incorporer des solutions de sécurité dès la conception dans tous les dispositifs en question; encourage dans ce contexte le secteur privé à mettre en œuvre des mesures volontaires élaborées à partir de la législation de l'Union en la matière, telle que la directive SRI, et conformes aux normes internationalement reconnues afin de renforcer la confiance dans la sécurité des logiciels et dispositifs, tels que le label de confiance de l'internet des objets;

40. encourage les fournisseurs de services à adhérer au code de conduite visant à combattre les discours de haine illégaux en ligne et invite la Commission et les entreprises participantes à poursuivre leur coopération dans ce domaine;

41. rappelle que la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur[1] (directive sur le commerce électronique) dispose que les intermédiaires ne sont pas tenus responsables des contenus qu'ils transmettent ou hébergent tant qu'ils jouent un rôle neutre et passif, mais qu'une réaction rapide est attendue de leur part en vue de supprimer ou d'empêcher l'accès à des informations illicites dès qu'ils ont connaissance de violations ou d'activités illégales;

42. souligne la nécessité absolue de protéger les bases de données des services répressifs contre les incidents liés à la sécurité et l'accès illicite, puisqu'il s'agit là d'un sujet de préoccupation pour les citoyens; fait part de son inquiétude en ce qui concerne le champ d'action extraterritorial des services répressifs qui doivent accéder à des données dans le contexte d'enquêtes pénales, et souligne la nécessité de mettre en œuvre des règles strictes à cet égard;

43. estime que les questions liées aux contenus illicites en ligne doivent être traitées de manière diligente et efficace, notamment au moyen de procédures de retrait si le contenu n'est pas ou plus nécessaire aux fins de recherche, de détection et de poursuite; rappelle que les États membres peuvent, lorsque la suppression d'un contenu n'est pas possible, prendre des mesures nécessaires et proportionnées pour bloquer l'accès à ce contenu depuis le territoire de l'Union; souligne que de telles mesures doivent être conformes aux procédures législatives et judiciaires existantes, ainsi qu'à la charte, et doivent aussi être soumises à des garanties adéquates, y compris la possibilité d'un recours juridictionnel;

44. insiste sur le rôle que jouent les fournisseurs de services numériques de la société de l'information dans la suppression rapide et efficace de contenu illicite en ligne à la demande de l'autorité répressive responsable, et se félicite des progrès accomplis à cet égard, notamment avec la contribution au forum de l'Union sur l'internet; souligne la nécessité d'un renforcement de l'engagement et de la coopération des autorités compétentes et des fournisseurs de services de la société de l'information afin d'obtenir des entreprises du secteur des retraits rapides et efficaces, et d'éviter le blocage de contenus illicites au moyen de mesures gouvernementales; invite les États membres à engager la responsabilité juridique des plateformes qui ne respectent pas les obligations;

---

[1] JO L 178 du 17.7.2000, p. 1.

rappelle que les mesures de suppression de contenus illicites en ligne qui établissent des conditions d'utilisation ne sont permises que si les règles de procédure nationales prévoient la possibilité pour les utilisateurs de faire valoir leurs droits devant un tribunal une fois ces mesures connues;

45. souligne que, conformément à la résolution du Parlement du 19 janvier 2016 intitulée «Vers un acte sur le marché unique numérique»[1], la responsabilité limitée des intermédiaires constitue un aspect essentiel de la protection du caractère ouvert de l'internet, des droits fondamentaux, de la sécurité juridique et de l'innovation; se félicite de l'intention de la Commission de donner des orientations sur les procédures de signalement et de retrait, afin d'aider les plateformes en ligne à remplir leurs tâches et à respecter les règles en matière de responsabilité définies dans la directive sur le commerce électronique (directive 2000/31/CE), d'améliorer la sécurité juridique et de renforcer la confiance des utilisateurs; presse la Commission de présenter une propositions législative en la matière;

46. demande l'application du principe consistant à «suivre l'argent», comme exposé dans sa résolution du 9 juin 2015 sur la communication intitulée «Vers un consensus renouvelé sur la protection des droits de propriété intellectuelle: un plan d'action de l'UE»[2], sur la base du cadre réglementaire de la directive sur le commerce électronique et de la directive relative au respect des droits de propriété intellectuelle;

47. souligne l'importance capitale de la formation et du soutien psychologique spécifiques fournis en continu aux modérateurs de contenus, au sein des entités privées ou publiques, qui sont chargés de l'évaluation des contenus en ligne répréhensibles ou illicites, étant donné qu'ils devraient être considérés comme les premiers intervenants dans ce domaine;

48. invite les fournisseurs de services à prévoir des types de signalement clairs ainsi qu'une infrastructure administrative bien définie, capable d'assurer un suivi rapide et approprié des signalements;

49. invite les fournisseurs de services à œuvrer à l'intensification des activités de sensibilisation des risques en ligne, en particulier pour les enfants, par le développement d'outils interactifs et de matériels d'information;

Renforcement de la coopération policière et judiciaire

50. est préoccupé par le fait qu'un nombre considérable d'actes de cybercriminalité demeurent impunis; déplore que l'utilisation, par les fournisseurs de services internet, de technologies telles que les NAT CGN entrave gravement les enquêtes en rendant techniquement impossible l'identification précise de l'utilisateur d'une adresse IP et donc des auteurs de délits en ligne; insiste sur la nécessité de permettre aux autorités répressives d'avoir un accès licite aux informations pertinentes, dans les cas restreints où cet accès est nécessaire et proportionné pour des raisons de sécurité et de justice; souligne que les autorités judiciaires et répressives doivent être dotées de capacités suffisantes pour mener des enquêtes légitimes;

---

1 Textes adoptés de cette date, P8_TA(2016)0009.
2 JO C 407 du 4.11.2016, p. 25.

51. invite instamment les États membres à ne pas imposer aux fournisseurs de services de chiffrement d'obligations qui fragiliseraient ou compromettraient la sécurité de leur réseaux ou services, telles que la création ou la mise à disposition de «portes dérobées»; souligne que des solutions réalistes doivent être proposées, tant par voie législative que par l'évolution technologique continue, lorsqu'il est indispensable de trouver de telles solutions pour des raisons de sécurité et de justice; invite les États membres à coopérer, en concertation avec le pouvoir judiciaire et Eurojust, pour harmoniser les conditions de l'utilisation licite des outils d'enquête en ligne;

52. souligne que l'interception légale peut être une mesure très efficace pour combattre le piratage illicite, à condition qu'elle soit nécessaire, proportionnée, fondée sur une procédure judiciaire régulière et qu'elle respecte pleinement les droits fondamentaux, la législation de l'Union en matière de protection des données et la jurisprudence; invite tous les États membres à utiliser les possibilités d'interception légale visant des suspects, à établir des règles claires en ce qui concerne la procédure d'autorisation judiciaire préalable des activités d'interception légale, y compris les restrictions sur l'utilisation et la durée des outils de piratage légal, à mettre en place un mécanisme de surveillance, et à prévoir des voies de recours efficaces pour les personnes visées par les activités de piratage;

53. encourage les États membres à échanger avec le milieu de la sécurité des technologies de l'information et de la communication, et à l'encourager à participer plus activement au piratage dit «éthique» ainsi qu'au signalement de contenus illicites, tels que le matériel pédopornographique;

54. encourage Europol à mettre en place un système d'alerte anonyme depuis les réseaux cachés, qui permettra aux particuliers de signaler aux autorités les contenus illicites, tels que des représentations pédopornographiques, en utilisant des mesures de protection technologiques déjà mises en œuvre par de nombreux organes de presse qui se servent de tels systèmes pour faciliter l'échange de données sensibles avec les journalistes en garantissant un degré plus élevé d'anonymat et de sécurité qu'avec les courriels classiques;

55. insiste sur la nécessité de réduire au maximum les risques que posent, pour la vie privée des utilisateurs de l'internet, les fuites des exploits ou des outils utilisés par les services répressifs dans le cadre de leurs enquêtes légitimes;

56. souligne que les autorités judiciaires et répressives doivent être dotées de capacités et de ressources suffisantes pour leur permettre de lutter efficacement contre la cybercriminalité;

57. souligne que la multitude de juridictions nationales distinctes et définies territorialement crée des difficultés dans la détermination de la loi applicable dans des interactions transnationales et donne lieu à une insécurité juridique, empêchant ainsi la coopération par-delà les frontières, laquelle est nécessaire pour traiter efficacement la cybercriminalité;

58. souligne la nécessité de développer des éléments concrets pour une approche commune de l'Union européenne en matière de juridiction dans le cyberespace, telle qu'exprimée lors de la réunion informelle des ministres de la justice et des affaires intérieures du 26 janvier 2016;

59. insiste, à cet égard, sur la nécessité de développer des normes de procédure communes susceptibles d'établir les facteurs territoriaux déterminant les lois applicables dans le cyberespace et de définir des mesures d'enquête pouvant être utilisées indépendamment des frontières géographiques;

60. reconnaît qu'une telle approche européenne commune, qui doit respecter les droits fondamentaux et la vie privée, suscitera la confiance des parties prenantes, réduira les retards en matière de traitement des demandes transfrontalières, établira une interopérabilité entre les acteurs hétérogènes et permettra d'incorporer les règles de procédure nécessaires aux cadres opérationnels;

61. estime qu'à long terme, les normes de procédure communes en matière de compétence d'exécution dans le cyberespace devraient aussi être développées au niveau mondial; salue, à cet égard, les travaux du groupe sur les preuves dans le nuage du Conseil de l'Europe;

Preuves électroniques

62. souligne qu'une approche européenne commune en matière de justice pénale dans le cyberespace constitue une priorité, car elle améliorera le respect de l'état de droit dans le cyberespace et facilitera l'obtention de preuves électroniques dans le cadre de procédures pénales, tout en contribuant à ce que les affaires soient résolues beaucoup plus rapidement qu'actuellement;

63. insiste sur la nécessité de trouver des moyens de recueillir et d'obtenir des preuves électroniques plus rapidement, ainsi que sur l'importance que revêt la coopération étroite entre les autorités répressives – notamment par un recours accru aux équipes communes d'enquête –, les pays tiers et les fournisseurs de services actifs sur le territoire européen, conformément au règlement général sur la protection des données ((UE) 2016/679), à la directive (UE) 2016/680 (directive «police») et les accords actuels en matière d'entraide judiciaire; souligne qu'il est nécessaire de créer des points de contact uniques dans tous les États membres et d'optimiser l'utilisation des points de contact existants, étant donné que cela facilitera l'accès aux preuves électroniques ainsi que le partage d'informations, améliorera la coopération avec les fournisseurs de services et accélérera les procédures d'entraide judiciaire;

64. reconnaît que le cadre juridique actuellement fragmenté peut poser des difficultés aux fournisseurs de services qui s'efforcent de répondre favorablement aux demandes des services répressifs; invite la Commission à proposer un cadre juridique européen pour les preuves électroniques comprenant des règles harmonisées pour déterminer le statut des fournisseurs de services, national ou étranger, et obliger ces derniers à répondre aux demandes en provenance d'autres États membres fondées sur des procédures juridiques appropriées et conformément à la décision d'enquête européenne, tout en tenant compte du principe de proportionnalité afin d'éviter des conséquences négatives sur l'exercice de la liberté d'établissement et la libre prestation de services, et en donnant des garanties adéquates, en vue de créer une sécurité juridique et d'accroître la capacité des fournisseurs de services et des intermédiaires à répondre aux demandes des services répressifs;

65. souligne qu'il est nécessaire que le cadre pour les preuves électroniques contienne des garanties suffisantes concernant les droits et les libertés de toutes les parties concernées;

précise qu'un tel cadre doit comporter une exigence prévoyant d'adresser en premier lieu les demandes de preuves électroniques aux propriétaires des données ou aux responsables de leur traitement, afin de garantir le respect de leurs droits, mais aussi des droits de toute autre partie concernée par les données en question (par exemple, leur droit au respect du secret professionnel et à demander réparation dans le cas d'un accès aux données disproportionné ou illicite); souligne également la nécessité de veiller à ce que tout cadre juridique protège les prestataires et toutes les autres parties contre les demandes susceptibles de créer des conflits de lois ou de porter atteinte à la souveraineté d'autres États;

66. invite les États membres à mettre pleinement en œuvre la directive 2014/41/UE concernant la décision d'enquête européenne en matière pénale aux fins de recueillir et d'obtenir efficacement des preuves électroniques dans l'Union, ainsi qu'à prévoir des dispositions spécifiques relatives au cyberespace dans leurs codes pénaux nationaux afin de contribuer à la recevabilité des preuves électroniques devant les tribunaux et à permettre aux juges de disposer d'orientations plus claires en ce qui concerne la pénalisation de la cybercriminalité;

67. salue les travaux actuels de la Commission portant sur la création d'une plateforme de coopération, munie d'un canal de communication sécurisé et permettant l'échange de décisions d'enquête européenne par voie numérique, en ce qui concerne les preuves électroniques et les réponses entre autorités judiciaires de l'Union; invite la Commission, conjointement avec les États membres, Eurojust et les fournisseurs de services, à examiner et harmoniser les formulaires, les outils et les procédures de demande pour recueillir et obtenir des preuves électroniques, afin de faciliter l'authentification, de garantir la marche rapide des procédures et d'améliorer la transparence et la responsabilisation dans le processus permettant de recueillir et d'obtenir des preuves électroniques; invite l'Agence de l'Union européenne pour la formation des services répressifs (CEPOL) à élaborer des modules de formation sur l'utilisation efficace des cadres actuels utilisés pour recueillir et obtenir des preuves électroniques; souligne, dans ce contexte, que la simplification des politiques des fournisseurs de services contribuera à atténuer le caractère hétérogène des différentes méthodes, notamment concernant les procédures et les conditions pour accorder l'accès aux données demandées;

Renforcement des capacités au niveau européen

68. indique que les incidents récents ont clairement montré l'extrême vulnérabilité de l'Union européenne, et plus particulièrement des institutions de l'Union, des gouvernements et des parlements nationaux, des grandes entreprises européennes et des infrastructures et réseaux informatiques européens, aux attaques sophistiquées réalisées au moyen de logiciels complexes et malveillants; invite l'ENISA à évaluer de façon continue le niveau de menace et invite la Commission à investir dans les capacités informatiques ainsi que dans la défense et la résilience des infrastructures critiques des institutions de l'Union afin de réduire la vulnérabilité de l'Union face à de graves attaques informatiques provenant d'organisations criminelles d'envergure, ainsi qu'à des attaques financées par des États ou liées à groupes terroristes;

69. salue la contribution importante du Centre européen de lutte contre la cybercriminalité (EC3) d'Europol et d'Eurojust, ainsi que de l'ENISA, à la lutte contre la cybercriminalité;

70. invite Europol à soutenir les autorités répressives nationales dans la mise en place de voies de transmission sûres et adéquates;

71. déplore l'absence de normes européennes en matière de formation et de certification; constate que les tendances futures en matière de cybercriminalité rendent indispensable un niveau d'expertise accru des professionnels; se félicite de la voie déjà ouverte par les initiatives telles que le groupe européen de formation et d'enseignement sur la cybercriminalité (ECTEG), le projet de formation des formateurs et les activités de formation encadrées par le cycle politique de l'Union européenne, en vue de remédier au manque d'expertise au niveau de l'Union;

72. demande à la CEPOL et au Réseau européen de formation judiciaire d'étendre leur offre de formations consacrées à des thèmes touchant à la cybercriminalité aux instances chargées de faire respecter la loi et aux autorités judiciaires à travers l'Union;

73. souligne que le nombre d'actes de cybercriminalité signalés à Eurojust a augmenté de 30 %; demande l'allocation de fonds suffisants et, si nécessaire, la création de postes supplémentaires afin de permettre à Eurojust de faire face à sa charge de travail croissante en matière de cybercriminalité, ainsi que de développer et de renforcer son soutien aux procureurs nationaux spécialisés dans la cybercriminalité dans les affaires transfrontalières, notamment par l'intermédiaire du réseau judiciaire européen en matière de cybercriminalité, récemment créé;

74. demande que le mandat de l'ENISA soit révisé et que les agences nationales chargées de la cybersécurité soient renforcées; appelle de ses vœux le renforcement de l'ENISA, en ce qui concerne sa mission, son personnel et ses ressources; souligne que le nouveau mandat devrait également inclure des liens renforcés avec Europol et les acteurs du secteur, afin de permettre à l'agence de mieux épauler les autorités compétentes dans la lutte contre la cybercriminalité;

75. demande à l'Agence des droits fondamentaux de l'Union européenne (FRA) d'élaborer un guide pratique et détaillé visant à fournir des orientations aux États membres en ce qui concerne la supervision et les contrôles approfondis;

Amélioration de la coopération avec les pays tiers

76. insiste sur l'importance d'une coopération étroite avec les pays tiers dans le cadre de la lutte contre la cybercriminalité, y compris au moyen de l'échange des meilleures pratiques, d'enquêtes communes, du renforcement des capacités et de l'entraide judiciaire;

77. invite les États membres ne l'ayant pas encore fait à ratifier et à mettre pleinement en œuvre la convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001 (convention de Budapest) ainsi que ses protocoles additionnels et, en coopération avec la Commission, à la promouvoir auprès des enceintes internationales compétentes;

78. souligne sa vive préoccupation quant aux travaux en cours au sein du comité de la convention sur la cybercriminalité du Conseil de l'Europe concernant l'interprétation de l'article 32 de la convention de Budapest qui porte sur l'accès transfrontière à des données informatiques stockées («preuves dans le nuage»), et s'oppose à toute adoption

d’un protocole additionnel ou d’orientations visant à élargir le champ d’application de cette disposition au-delà du régime établi par la convention, qui constitue déjà une exception d’importance majeure au principe de territorialité, car de telles mesures pourraient permettre aux services répressifs d’accéder à distance et sans entrave à des serveurs et à des ordinateurs situés dans d’autres juridictions sans avoir recours à l’entraide judiciaire ou à d’autres instruments de coopération judiciaire mis en place en vue de garantir les droits fondamentaux des personnes, dont la protection des données et le respect de la légalité, et notamment, en particulier, la convention 108 du Conseil de l’Europe;

79. déplore l’absence d’une législation internationale contraignante en matière de cybercriminalité et exhorte les États membres et les institutions européennes à œuvrer à l’élaboration d’une convention en la matière;

80. invite la Commission à proposer des options d’initiatives pour améliorer l’efficacité et promouvoir l’utilisation des traités d’entraide judiciaire (TEJ) en vue de mettre fin à l’appropriation de la compétence extraterritoriale par des pays tiers;

81. invite les États membres à garantir une capacité suffisante de traitement des demandes d’entraide judiciaire relatives aux enquêtes dans le cyberespace, ainsi qu’à élaborer des programmes de formation pertinents destinés au personnel chargé de traiter de telles demandes;

82. souligne que les accords de coopération stratégique et opérationnelle entre Europol et les pays tiers facilitent les échanges d’informations et la coopération pratique;

83. prend acte du fait que le plus grand nombre de demandes émanant des services répressifs sont transmises aux États-Unis et au Canada; est préoccupé par le fait que le taux de divulgation des grands fournisseurs de services américains en réponse aux demandes formulées par les autorités de justice pénale européennes soit inférieur à 60 % et rappelle que, selon le chapitre V du règlement général sur la protection des données, les TEJ et d’autres accords internationaux constituent le mécanisme privilégié pour permettre l’accès aux données personnelles détenues hors de l’Union;

84. invite la Commission à présenter des mesures concrètes pour protéger les droits fondamentaux des suspects ou des prévenus lorsqu’un échange d’informations entre les services répressifs européens et les pays tiers a lieu, notamment en ce qui concerne les garanties quant à l’obtention rapide, sur la base d’une décision judiciaire, d’éléments de preuve pertinents, des données des abonnés ou des métadonnées détaillées et des données relatives au contenu (si elles ne sont pas cryptées) de services répressifs et/ou de fournisseurs de services en vue d’améliorer l’entraide judiciaire;

85. invite la Commission, conjointement avec les États membres, les organismes européens associés et, lorsque cela est nécessaire, les pays tiers, à étudier de nouveaux moyens de recueillir et d’obtenir efficacement les preuves électroniques hébergées dans des pays tiers, dans le plein respect des droits fondamentaux et de la législation européenne en matière de protection des données, en accélérant et en simplifiant l’utilisation des procédures d’entraide judiciaire et, le cas échéant, de la reconnaissance mutuelle;

86. souligne l’importance du centre de l’OTAN de réaction aux incidents de sécurité informatique;

87. invite tous les États membres à participer au forum mondial sur la cyberexpertise (GFCE) afin de simplifier la constitution de partenariats en vue de développer les capacités;

88. soutient l'aide au renforcement des capacités fournie par l'Union européenne aux pays du voisinage oriental, étant donné que de nombreuses attaques informatiques proviennent de ces pays;

°

° °

89. charge son Président de transmettre la présente résolution au Conseil et à la Commission.