Conseil de
l'Union européenne

Bruxelles, le 16 décembre 2020
(OR. en)

14133/20

Dossier interinstitutionnel:
2020/0305(NLE)

CYBER 280	**RECH 529**
JAI 1118	**COMPET 642**
JAIEX 121	**IND 273**
EJUSTICE 107	**COTER 115**
COSI 254	**ENFOPOL 350**
DATAPROTECT 154	**COPS 485**
COPEN 387	**MI 578**
TELECOM 269	**IXIM 139**
PROCIV 99	**POLMIL 201**
CSC 367	**HYBRID 48**
CIS 65	**CSCI 96**
RELEX 1019	**POLGEN 234**

NOTE DE TRANSMISSION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	16 décembre 2020
Destinataire:	Monsieur Jeppe TRANHOLM-MIKKELSEN, secrétaire général du Conseil de l'Union européenne
N° doc. Cion:	JOIN(2020) 18 final
Objet:	COMMUNICATION CONJOINTE AU PARLEMENT EUROPÉEN ET AU CONSEIL – La stratégie de cybersécurité de l'UE pour la décennie numérique

Les délégations trouveront ci-joint le document JOIN(2020) 18 final.

p.j.: JOIN(2020) 18 final

COMMISSION
EUROPÉENNE

LE HAUT REPRÉSENTANT DE
L'UNION POUR LES AFFAIRES
ÉTRANGÈRES ET LA
POLITIQUE DE SÉCURITÉ

Bruxelles, le 16.12.2020
JOIN(2020) 18 final

COMMUNICATION CONJOINTE AU PARLEMENT EUROPÉEN ET AU CONSEIL

La stratégie de cybersécurité de l'UE pour la décennie numérique

COMMUNICATION CONJOINTE AU PARLEMENT EUROPÉEN ET AU CONSEIL

La stratégie de cybersécurité de l'UE pour la décennie numérique

I. INTRODUCTION: UNE TRANSFORMATION NUMÉRIQUE CYBERSÉCURISÉE DANS UN ENVIRONNEMENT DE MENACE COMPLEXE

La cybersécurité fait partie intégrante de la sécurité des Européens. Qu'ils aient recours à des appareils, réseaux électriques, banques, aéronefs, administrations publiques ou hôpitaux connectés, les citoyens doivent pouvoir avoir l'assurance qu'ils seront protégés contre les cybermenaces. L'économie, la démocratie et la société de l'UE dépendent plus que jamais d'outils numériques et d'une connectivité sûrs et fiables. La cybersécurité est donc essentielle pour construire une Europe résiliente, verte et numérique.

Les transports, l'énergie et la santé, les télécommunications, la finance, la sécurité, les processus démocratiques, l'espace et la défense dépendent fortement de réseaux et de systèmes d'information de plus en plus interconnectés. Les interdépendances intersectorielles sont très fortes car les réseaux et les systèmes d'information sont eux-mêmes tributaires, pour fonctionner, d'un approvisionnement régulier en électricité. Le nombre d'appareils connectés dépasse déjà le nombre d'habitants de notre planète et devrait atteindre 25 milliards d'ici à 2025[1]: un quart de ces appareils se trouveront en Europe. La numérisation des formes de travail a été accélérée par la pandémie de COVID-19, au cours de laquelle 40 % des travailleurs de l'UE sont passés au télétravail, ce qui aura probablement des effets permanents sur leur vie quotidienne[2]. Ce phénomène accroît les vulnérabilités aux cyberattaques[3]. Les objets connectés sont souvent expédiés au consommateur avec des vulnérabilités connues, ce qui accroît encore leur surface d'exposition aux actes de cybermalveillance[4]. Le paysage industriel de l'UE est de plus en plus numérisé et connecté; cela signifie également que les cyberattaques peuvent avoir un impact bien plus important que jamais sur les industries et les écosystèmes.

Le panorama de la menace se double de tensions géopolitiques pesant sur l'internet mondial et ouvert et sur le contrôle des technologies tout au long de la chaîne

[1] Estimation de l'association professionnelle du secteur des télécommunications GSMA; https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf). L'International Data Corporation prévoit 42,6 milliards de machines, capteurs et caméras connectés; https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[2] Selon une enquête réalisée en juin 2020, 47 % des chefs d'entreprise ont déclaré avoir l'intention de permettre à leurs salariés de travailler à distance à temps plein même s'il devenait possible de retourner sur son lieu de travail; 82 % d'entre eux avaient l'intention de permettre le travail à distance au moins pour une certaine période; https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time.

[3] https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

[4] L'un des logiciels malveillants les plus préjudiciables à ce jour, connu sous le nom de «Mirai», a créé des réseaux zombies de plus de 600 000 appareils qui ont perturbé plusieurs grands sites web en Europe et aux États-Unis.

d'approvisionnement[5]. Ces tensions se reflètent dans l'augmentation du nombre d'États-nations érigeant des frontières numériques. Les restrictions imposées à l'internet et à son utilisation menacent le cyberespace mondial et ouvert, ainsi que l'état de droit, les droits fondamentaux, la liberté et la démocratie, qui sont les valeurs fondamentales de l'UE. Le cyberespace est de plus en plus exploité à des fins politiques et idéologiques, et la polarisation accrue au niveau international entrave le multilatéralisme effectif. Les menaces hybrides combinent des campagnes de désinformation avec des cyberattaques contre les infrastructures, les processus économiques et les institutions démocratiques, avec pour effets possibles de causer des dommages physiques, de permettre un accès illicite aux données à caractère personnel, de faciliter le vol de secrets industriels ou d'État, de semer la méfiance et d'affaiblir la cohésion sociale. Ces activités fragilisent la sécurité et la stabilité internationales et mettent en péril les avantages que le cyberespace apporte au développement économique, social et politique.

Le ciblage malveillant des infrastructures critiques constitue un risque majeur à l'échelle mondiale[6]. L'internet a une architecture décentralisée, sans structure centrale et avec une gouvernance multipartite. Il est parvenu à maintenir la croissance exponentielle des volumes de trafic tout en étant une cible constante pour les tentatives malveillantes de perturbation[7]. Parallèlement, le système est de plus en plus tributaire des fonctions essentielles de l'internet ouvert et mondial, telles que le système de noms de domaine (DNS), et des services internet essentiels pour les communications et l'hébergement, les applications et les données. Ces services sont de plus en plus concentrés entre les mains de quelques entreprises privées[8]. L'économie et la société européennes sont ainsi exposées aux perturbations géopolitiques ou techniques qui touchent le cœur de l'internet ou une ou plusieurs de ces entreprises. L'augmentation de l'utilisation de l'internet et l'évolution des modèles dues à la pandémie ont mis davantage en lumière la fragilité des chaînes d'approvisionnement qui dépendent de cette infrastructure numérique.

Les préoccupations en matière de sécurité dissuadent sérieusement d'utiliser les services en ligne[9]. Environ deux cinquièmes des utilisateurs de l'UE ont rencontré des problèmes liés à la sécurité et trois cinquièmes se sentent incapables de se protéger contre la

[5] Dont les composants électroniques, l'analyse des données, l'informatique en nuage, les réseaux plus rapides et plus intelligents avec la 5G et au-delà, le cryptage, l'intelligence artificielle (IA) et les nouveaux paradigmes de calcul et de traitement de données fiables tels que la chaîne de blocs, l'informatique en nuage, le nuage-périphérie (cloud-to-edge) et l'informatique quantique.

[6] Forum économique mondial - Global Risks Report 2020.

[7] Selon l'Organisation de coopération et de développement économiques, la pandémie a entraîné une augmentation de 60 % du trafic internet ; https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/. L'Organe des régulateurs européens des communications électroniques et la Commission publient régulièrement des rapports sur l'état de la capacité internet pendant la période d'application des mesures de confinement liées au coronavirus. Selon un rapport de l'ENISA, le nombre total d'attaques par déni de service distribué a augmenté de 241 % au troisième trimestre de 2019 par rapport au troisième trimestre de 2018. Ces attaques gagnent en intensité; la plus virulente jamais enregistrée a été perpétrée en février 2020, atteignant un pic de trafic de 2,3 térabits par seconde. Lors de la panne «CenturyLink» intervenue en août 2020, un problème de routage au niveau du fournisseur américain de services internet a entraîné une baisse de 3,5 % du trafic internet mondial; https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service

[8] Internet Society, The Global Internet Report: Consolidation in the Internet Economy; https://www.internetsociety.org/blog/2019/02/is-the-internet-shrinking-the-global-internet-report-consolidation-in-the-internet-economy-explores-this-question/
https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

cybercriminalité[10]. Un tiers d'entre eux des utilisateurs a reçu des courriels frauduleux ou des appels téléphoniques demandant des informations personnelles au cours des trois dernières années, mais 83 % n'ont jamais signalé d'acte de cybercriminalité. Une entreprise sur huit a été touchée par des cyberattaques[11]. Plus de la moitié des ordinateurs personnels d'entreprises et de particuliers qui ont été infectés une fois par des logiciels malveillants sont réinfectés au cours de la même année[12]. Des centaines de millions d'enregistrements sont perdus chaque année à la suite de violations de données; le coût moyen d'une violation pour une seule entreprise est passé à plus de 3,5 millions d'EUR en 2018[13]. Les effets d'une cyberattaque peuvent rarement être isolés et peuvent déclencher des réactions en chaîne dans l'ensemble de l'économie et de la société, touchant des millions d'individus[14].

Les enquêtes comportent une composante numérique pour pratiquement tous les types de criminalité. En 2019, un triplement du nombre d'incidents en glissement annuel a été constaté. On estime à 700 millions le nombre de nouveaux échantillons de logiciels malveillants, le moyen le plus fréquent de faciliter une cyberattaque[15]. Le coût annuel de la cybercriminalité pour l'économie mondiale en 2020 est estimé à 5,5 milliards d'EUR, soit le double de 2015[16]. Il s'agit du plus grand transfert de richesse économique de l'histoire, avant le commerce mondial de drogue. Un incident majeur, l'attaque perpétrée à l'aide du logiciel rançonneur Wannacry en 2017, a généré un coût pour l'économie mondiale estimé à plus de 6,5 milliards d'EUR[17].

Les services numériques et le secteur financier figurent parmi les cibles les plus fréquentes des cyberattaques, avec le secteur public et l'industrie manufacturière, mais les entreprises et les citoyens restent mal préparés en matière de cybermenaces et peu sensibles aux questions de cybersécurité[18] et les travailleurs manquent sérieusement de compétences en matière de cybersécurité[19]. Il y a eu près de 450 incidents de cybersécurité en 2019, qui ont touché des infrastructures critiques européennes telles que la finance et

---

[10] Indice relatif à l'économie et à la société numériques 2020; https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020;
https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

[11] Communiqué de presse d'Eurostat, «ICT security measures taken by vast majority of enterprises in the EU», 6/2020 - 13 janvier 2020. «Cyberattacks on critical infrastructure have become the new normal across sectors such as energy, healthcare and transportation» (Les cyberattaques contre des infrastructures critiques sont devenues la nouvelle norme dans des secteurs tels que l'énergie, les soins de santé et les transports); Forum économique mondial, Rapport sur les risques mondiaux 2020.

[12] Source: Comparitech.

[13] Rapport annuel sur le coût d'une violation des données, 2020 Ponemon Institute, et sur la base d'une analyse quantitative de 524 violations récentes dans 17 zones géographiques et 17 secteurs; https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

[14] Rapport du Centre commun de recherche (JRC), «Cybersecurity, our digital anchor»; https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/cybersecurity-our-digital-anchor

[15] Source: AV-TEST, https://www.av-test.org/en/statistics/malware/

[16] JRC, Cybersecurity – Our Digital Anchor.

[17] Source: Cyence.

[18] Les entreprises, en particulier les PME, restent également peu sensibilisées au vol électronique de secrets d'affaires; PwC, Study on the scale and impact of industrial espionage and theft of trade secrets through cyber (en anglais): Dissemination report on measures to tackle and prevent cyber-theft of trade secrets, 2018.

[19] Voir le rapport 2020 de l'ENISA concernant le panorama des menaces. Voir également le rapport d'enquête 2020 de Verizon sur la violation de données; https://enterprise.verizon.com/resources/reports/dbir/

l'énergie[20]. Les organisations de soins de santé et les professionnels de la santé ont été particulièrement touchés pendant la pandémie. La technologie devenant indissociable du monde physique, les cyberattaques mettent en danger la vie et le bien-être des plus vulnérables[21]. Plus de deux tiers des entreprises, en particulier les PME, sont considérées comme des «novices» en matière de cybersécurité et les entreprises européennes sont considérées comme moins bien préparées que les entreprises d'Asie et d'Amérique[22]. Selon les estimations, 291 000 postes de professionnels de la cybersécurité restent à pourvoir en Europe. Le recrutement et la formation d'experts en cybersécurité sont un processus dont la lenteur expose les organisations à des risques accrus en matière de cybersécurité[23].

L'UE ne dispose pas d'une connaissance collective de la situation en matière de cybermenaces. Cela s'explique par le fait que les autorités nationales ne collectent et ne partagent pas systématiquement les informations - telles que celles disponibles dans le secteur privé - qui pourraient aider à évaluer l'état de la cybersécurité dans l'UE. Seule une partie des incidents est signalée par les États membres et le partage d'informations n'est ni systématique ni exhaustif[24]; les cyberattaques peuvent n'être qu'une facette d'attaques malveillantes concertées contre les sociétés européennes. Il n'existe actuellement qu'une assistance opérationnelle mutuelle limitée entre les États membres et aucun mécanisme opérationnel n'est en place entre les États membres et les institutions, agences et organes de l'UE pour faire face à d'éventuels incidents de cybersécurité ou crises transfrontières de grande ampleur[25].

L'amélioration de la cybersécurité est donc essentielle pour que les citoyens aient confiance dans l'innovation, la connectivité et l'automatisation, y recourent et en tirent parti, ainsi que pour la protection des droits et libertés fondamentaux, notamment le droit au respect de la vie privée et à la protection des données à caractère personnel, et de la liberté d'expression et d'information. La cybersécurité est indispensable à la connectivité des réseaux et à l'internet ouvert et mondial, qui doit soutenir la transformation de l'économie et de la société dans les années 2020. Elle contribue à l'amélioration et à l'augmentation des emplois, au renforcement de la flexibilité des lieux de travail et de l'efficience et de la durabilité des transports et de l'agriculture, ainsi qu'à un accès plus aisé et plus équitable aux services de santé. Elle est également essentielle pour la transition vers une énergie plus propre dans le cadre du pacte vert pour l'Europe[26] au moyen de réseaux transfrontaliers et de compteurs intelligents, ainsi que de mesures visant à éviter les doubles emplois inutiles dans le stockage de données. Enfin, elle revêt une importance cruciale pour la sécurité et la stabilité internationales ainsi que pour le développement des économies, des démocraties et des sociétés à l'échelle mondiale. Les gouvernements, les entreprises et les particuliers doivent donc utiliser les outils numériques de manière responsable et soucieuse

---

[20] https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f

[21] Des logiciels rançonneurs ont été utilisés pour cibler les hôpitaux et les dossiers de santé, par exemple en Roumanie (juin 2020), à Düsseldorf (septembre 2020) et à Vastaamo (octobre 2020).

[22] PwC, The Global State of Information Security 2018; ESI Thoughtlab, The Cybersecurity Imperative, 2019.

[23] Agence de l'UE pour la cybersécurité, Cybersecurity Skills Development in the EU: The certification of cybersecurity degrees and ENISA's Higher Education Database, décembre 2019.

[24] Les États membres sont tenus de fournir au groupe de coopération un rapport annuel de synthèse sur les notifications reçues au titre de l'article 10, paragraphe 3, de la directive sur la sécurité des réseaux et des systèmes d'information [directive (UE) 2016/1148].

[25] Les instructions permanentes régissant l'assistance mutuelle entre les membres du réseau des CSIRT sont en place.

[26] Le pacte vert pour l'Europe, COM(2019) 640 final.

de la sécurité. La sensibilisation à la cybersécurité et l'hygiène doivent soutenir la transformation numérique des activités quotidiennes.

La nouvelle stratégie de cybersécurité de l'UE pour la décennie numérique constitue un élément clé de la stratégie «Façonner l'avenir numérique de l'Europe»[27], du plan de relance pour l'Europe de la Commission[28], de la stratégie pour l'union de la sécurité 2020-2025[29], de la stratégie globale pour la politique étrangère et de sécurité de l'UE[30] et du programme stratégique 2019-2024 du Conseil européen[31]. Elle expose la manière dont l'UE protégera ses citoyens, ses entreprises et ses institutions contre les cybermenaces, fera progresser la coopération internationale et jouera un rôle moteur dans l'action visant à assurer un internet mondial ouvert.

II. PENSER À L'ÉCHELLE MONDIALE, AGIR AU NIVEAU EUROPÉEN

La présente stratégie vise à garantir un internet ouvert et mondial doté de solides garde-fous pour faire face aux risques pour la sécurité et les libertés et droits fondamentaux des citoyens en Europe. À la suite des progrès accomplis dans le cadre des stratégies précédentes, elle contient des propositions concrètes de déploiement de **trois instruments principaux – instruments réglementaires, d'investissement et d'action –** couvrant **trois domaines d'action de l'UE: (1) la résilience, la souveraineté et le leadership technologiques, (2) le renforcement des capacités opérationnelles pour prévenir, décourager et réagir, et (3) favoriser un cyberespace mondial et ouvert.** L'UE est déterminée à soutenir cette stratégie au moyen d'**investissements d'un niveau inédit - qui pourrait atteindre quatre fois les niveaux précédents - dans la transition numérique de l'UE au cours des sept prochaines années**, dans le cadre des nouvelles politiques technologiques et industrielles et du programme de relance[32].

La cybersécurité doit être intégrée dans tous ces investissements numériques, en particulier les technologies clés telles que l'intelligence artificielle (IA), le cryptage et l'informatique quantique, au moyen d'incitations, d'obligations et de critères de référence. Cela peut stimuler la croissance du secteur européen de la cybersécurité et apporter la sécurité nécessaire pour faciliter l'abandon progressif des systèmes antérieurs. Le Fonds européen de la défense (FED) soutiendra les solutions européennes de cyberdéfense dans le cadre de la base industrielle et technologique de défense européenne. La cybersécurité est incluse dans les instruments de financement extérieur destinés à soutenir nos partenaires, notamment l'instrument de voisinage, de coopération au développement et de coopération internationale. La prévention de l'utilisation abusive des technologies, la protection des infrastructures critiques et les mesures visant à garantir également l'intégrité des chaînes

[27] Façonner l'avenir numérique de l'Europe, COM (2020) 67 final.
[28] L'heure de l'Europe: réparer les dommages et préparer l'avenir pour la prochaine génération, COM(2020) 98 final.
[29] La stratégie de l'UE pour l'union de la sécurité 2020-2025, COM (2020) 605 final.
[30] https://eeas.europa.eu/topics/eu-global-strategy_fr
[31] https://www.consilium.europa.eu/fr/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/
[32] Les investissements dans l'ensemble de la chaîne d'approvisionnement en technologies numériques, qui contribuent à la transition numérique ou à relever les défis qui en découlent, devraient représenter au moins 20 % (soit 134,5 milliards d'EUR) de la facilité pour la reprise et la résilience d'un montant de 672,5 milliards d'EUR de subventions et de prêts. Le financement de l'UE au titre du cadre financier pluriannuel 2021-2027 envisagé en faveur de la cybersécurité dans le cadre du programme pour une Europe numérique, et en faveur de la recherche en matière de cybersécurité dans le cadre d'Horizon Europe, avec un accent particulier sur le soutien aux PME, pourrait s'élever à 2 milliards d'EUR au total, à quoi il convient d'ajouter les investissements des États membres et de l'industrie.

d'approvisionnement permettent également à l'UE d'adhérer aux normes, règles et principes des Nations unies en matière de comportement responsable des États[33].

1. RÉSILIENCE, SOUVERAINETÉ TECHNOLOGIQUE ET LEADERSHIP

Les infrastructures critiques et les services essentiels de l'UE sont de plus en plus interdépendants et numérisés. Tous les objets connectés à l'internet dans l'UE, qu'il s'agisse de voitures automatisées, de systèmes de commande industriels ou d'appareils ménagers, ainsi que l'ensemble des chaînes d'approvisionnement qui mettent ces objets à disposition, doivent être sûrs dès le stade de la conception, résilients face aux cyber-incidents et corrigés rapidement lorsque des vulnérabilités sont décelées. Cet aspect est essentiel pour donner aux secteurs privé et public de l'UE la possibilité de choisir parmi les infrastructures et les services les plus sûrs. La décennie à venir sera l'occasion pour l'UE de jouer un rôle de premier plan dans la mise au point de technologies sûres dans l'ensemble de la chaîne d'approvisionnement. Garantir la résilience et renforcer les capacités industrielles et technologiques en matière de cybersécurité devraient nécessiter la mobilisation de tous les instruments réglementaires, d'investissement et de politique requis. La cybersécurité par la conception de procédés, d'opérations et de dispositifs industriels peut atténuer les risques, réduire potentiellement les coûts supportés par les entreprises ainsi que par la société dans son ensemble, et accroître ainsi la résilience.

1.1 Des infrastructures résilientes et des services critiques

Les **règles de l'UE relatives à la sécurité des réseaux et des systèmes d'information (SRI)** sont au cœur du marché unique de la cybersécurité. La Commission propose de réformer ces règles dans le cadre d'une directive SRI révisée afin d'accroître le niveau de **cyber-résilience de tous les secteurs concernés, publics et privés, qui remplissent une fonction importante pour l'économie et la société[34]**. Cette révision est nécessaire pour réduire les incohérences dans l'ensemble du marché intérieur en harmonisant le champ d'application, les exigences en matière de sécurité et de notification des incidents, la surveillance et le contrôle de l'application des règles au niveau national et les capacités des autorités compétentes.

Une directive SRI révisée servira de base à des règles plus spécifiques qui s'avèrent également nécessaires pour les secteurs d'importance stratégique, notamment l'énergie, les transports et la santé. Afin de garantir une approche cohérente telle qu'annoncée dans le cadre de la stratégie pour l'union de la sécurité 2020-2025, la directive réformée est proposée parallèlement à un réexamen des dispositions législatives concernant la résilience des infrastructures critiques[35]. Des technologies énergétiques intégrant des éléments numériques et la sécurité des chaînes d'approvisionnement associées sont importantes pour la continuité des services essentiels et pour le contrôle stratégique des infrastructures énergétiques critiques. La Commission proposera dès lors des mesures, parmi lesquelles un «code de réseau» fixant des règles en matière de cybersécurité des flux transfrontaliers d'électricité, en vue de leur adoption d'ici la fin de 2022. Le secteur financier doit également renforcer la résilience opérationnelle numérique et développer une capacité de résister à tous les types de

[33] https://undocs.org/fr/A/70/174
[34] [*insert reference to NIS proposal*]
[35] [insert reference to *proposal* for a directive on resilience of critical entities]

perturbations et de menaces liées aux TIC, comme l'a proposé la Commission[36]. Dans le domaine des transports, la Commission a ajouté des dispositions en matière de cybersécurité[37] à la législation de l'UE relative à la sûreté aérienne et poursuivra ses efforts pour renforcer la cyber-résilience dans tous les modes de transport. Le renforcement de la cyber-résilience des **processus et institutions démocratiques** est un élément central du plan d'action pour la démocratie européenne visant à préserver et à promouvoir des élections libres, ainsi que le discours démocratique et le pluralisme dans les médias[38]. Enfin, en ce qui concerne la sécurité des infrastructures et des services dans le cadre du futur programme spatial, la Commission poursuivra l'approfondissement de la stratégie Galileo en matière de cybersécurité pour la prochaine génération de services du système mondial de navigation par satellite et d'autres nouveaux éléments du programme spatial[39].

1.2 Construire un cyberbouclier européen

Avec l'expansion de la connectivité et la sophistication croissante des cyber-attaques, les centres d'échange et d'analyse d'informations, ou «ISAC», jouent un rôle précieux, y compris au niveau sectoriel, en permettant l'échange d'informations sur les cybermenaces entre un grand nombre de parties prenantes[40]. En outre, les réseaux et les systèmes informatiques nécessitent une surveillance et un suivi constants pour détecter les intrusions et les anomalies en temps réel. Un grand nombre d'entreprises privées, d'organismes publics et d'autorités nationales ont donc mis en place des centres de réponse aux incidents de sécurité informatique (CSIRT) et des centres des opérations de sécurité («Security Operations Centres» ou «SOC»).

Les centres des opérations de sécurité sont essentiels pour collecter les fichiers-journaux[41] et isoler les événements suspects survenant sur les réseaux de communication qu'ils surveillent. Ils y parviennent en identifiant des signaux et des schémas et en extrayant des connaissances sur les menaces à partir des grandes quantités de données qui doivent être évaluées. Ils ont contribué à la détection des activités d'exécutables malveillants et aidé ainsi à contenir des cyber-attaques. Le travail demandé dans ces centres est très exigeant et s'effectue à un rythme rapide, raison pour laquelle l'IA, et plus particulièrement les techniques d'apprentissage automatique, peuvent apporter un soutien précieux aux professionnels[42].

---

[36] Proposition de règlement sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014 et (UE) n° 909/2014 (COM/2020/595 final).

[37] Règlement d'exécution (UE) 2019/1583 de la Commission.

[38] Communication relative au plan d'action pour la démocratie européenne, COM(2020) 790. Dans le cadre du plan d'action, le Réseau européen de coopération en matière d'élections, constitué des réseaux électoraux des États membres, soutiendra le déploiement d'équipes communes d'experts pour lutter contre les menaces – y compris les cybermenaces – qui pèsent sur les processus électoraux; https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_fr

[39] Sont inclus l'initiative de communications gouvernementales par satellite (Govsatcom) et le système de surveillance des débris spatiaux (SST).

[40] https://www.enisa.europa.eu/media/enisa-en-francais/

[41] De manière à permettre aux services répressifs et judiciaires de les utiliser comme éléments de preuve.

[42] Source: étude de Ponemon Institute Research, «Improving the Effectiveness of the SOC, 2019»; pour les études concernant le recours à l'IA dans les SOC, voir par exemple: Khraisat, A., Gondal, I., Vamplew, P. *et al.* «Survey of intrusion detection systems: techniques, datasets and challenges», *Cybersecur* 2**,** 20 (2019).

La Commission propose de constituer un **réseau de centre des opérations de sécurité à l'échelle de l'UE**[43], et de soutenir l'amélioration des centres existants ainsi que la création de nouveaux centres. Elle soutiendra également la formation et le développement des compétences du personnel gérant ces centres. Sur la base d'une analyse des besoins menée avec les parties prenantes concernées et avec le soutien de l'Agence de l'Union européenne pour la cybersécurité (ENISA), elle pourrait engager plus de 300 millions d'euros pour soutenir la coopération public-privé et la coopération transfrontière dans la création de réseaux nationaux et sectoriels, incluant également des PME, en se fondant sur des dispositions appropriées en matière de gouvernance, de partage de données et de sécurité.

Les États membres sont encouragés à investir conjointement dans ce projet. Les centres seraient alors en mesure de partager et de corréler plus efficacement les signaux détectés et de créer des renseignements de qualité sur les menaces à partager avec les ISAC et les autorités nationales, permettant ainsi une meilleure connaissance de la situation. L'objectif serait de relier par phases autant de centres que possible dans toute l'UE afin de créer des connaissances collectives et de partager des bonnes pratiques. Un soutien sera mis à la disposition de ces centres afin d'améliorer la détection et l'analyse des incidents et les vitesses de réaction à ceux-ci grâce à des capacités d'IA et d'apprentissage automatique de pointe, et sera complété par une infrastructure de calcul à haute performance développée dans l'UE par l'entreprise commune pour le calcul à haute performance européen[44].

Grâce à une collaboration et à une coopération durables, ce réseau fournira des alertes en temps utile sur les incidents de cybersécurité aux autorités et à toutes les parties prenantes intéressées, y compris à l'unité conjointe de cybersécurité (voir section 2.1). **Il servira de véritable bouclier de cybersécurité pour l'UE**, en offrant un maillage solide de tours de surveillance capable de détecter les menaces potentielles avant qu'elles ne puissent causer des dommages de grande ampleur.

1.3 Une infrastructure de communication ultrasécurisée

Les communications gouvernementales par satellite de l'Union européenne[45], qui constituent un volet du programme spatial, fourniront des capacités de communication spatiale sûres et économiquement efficientes pour garantir les missions et opérations critiques en matière de sécurité qui sont gérées par l'UE et ses États membres, y compris les acteurs nationaux de la sécurité et les organes et agences des institutions de l'UE.

Les États membres se sont engagés à œuvrer avec la Commission au déploiement d'une infrastructure de communication quantique (ICQ) sûre pour l'Europe[46]. L'ICQ offrira aux pouvoirs publics un tout nouveau moyen de transmettre des informations confidentielles grâce à une forme de cryptage ultrasécurisée offrant une protection contre les cyberattaques et sera construite avec des technologies européennes. Elle se composera de deux éléments

[43]Des dispositions plus détaillées concernant la gouvernance, les principes de fonctionnement et le financement de ces centres, ainsi que la manière dont ils compléteront les structures existantes telles que les pôles d'innovation numérique, seront élaborées.
[44]https://ec.europa.eu/digital-single-market/en/eurohpc-joint-undertaking
[45]Govsatcom est un élément du programme spatial de l'Union.
[46]La déclaration EuroQCI a été signée par une majorité d'États membres, tandis que le développement et le déploiement de l'infrastructure devraient avoir lieu au cours de la période 2021-2027 avec des fonds d'Horizon Europe et du programme pour une Europe numérique, ainsi que de l'Agence spatiale européenne, sous réserve des dispositifs de gouvernance appropriés; https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network

principaux: des réseaux terrestres de communication en fibre existants qui relient des sites stratégiques au niveau national et transfrontière; et des satellites spatiaux liés couvrant l'ensemble de l'UE, y compris ses territoires d'outre-mer[47]. Cette initiative visant à mettre au point et à déployer de nouvelles formes de cryptage plus sûres et à concevoir de nouveaux moyens de protéger les moyens de communication et les ressources de données critiques peut contribuer à préserver la sécurité des informations sensibles et, partant, des infrastructures critiques.

Dans cette perspective et au-delà, la Commission étudiera la possibilité de déployer un système de connectivité multiorbitale sécurisé. S'appuyant sur Govsatcom et l'ICQ, il intégrerait des technologies de pointe (technologies quantiques, 5G, IA, traitement des données à la périphérie) respectant le cadre le plus restrictif en matière de cybersécurité afin de garantir des services sécurisés dès la conception tels qu'une connectivité fiable, sûre et économiquement efficiente et une communication cryptée pour les activités critiques des pouvoirs publics.

1.4 Sécuriser la prochaine génération de réseaux mobiles à large bande

Les citoyens et les entreprises de l'UE utilisant les applications sophistiquées et innovantes rendues possibles par la **5G et les futures générations de réseaux** devraient tirer parti des normes de sécurité les plus élevées. En collaboration avec la Commission et avec le soutien de l'ENISA, les États membres ont mis en place, avec la boîte à outils relative à la 5G[48] de janvier 2020, une approche globale, objective et fondée sur les risques de la cybersécurité de la 5G qui s'appuie sur une évaluation des plans d'atténuation possibles et l'identification des mesures les plus efficaces. En outre, l'UE renforce ses capacités dans le domaine de la 5G et au-delà afin d'éviter les dépendances et de favoriser une chaîne d'approvisionnement durable et diversifiée.

En décembre 2020, la Commission a publié un rapport relatif aux effets de la recommandation du 26 mars 2019 sur la cybersécurité des réseaux 5G[49]. Ce rapport a montré que des progrès considérables avaient été accomplis depuis l'adoption de la boîte à outils et que la plupart des États membres étaient en voie d'achever la mise en œuvre d'une partie importante de la boîte à outils dans un avenir proche, en dépit de certains écarts et de lacunes restantes déjà mis en évidence dans le rapport d'avancement publié en juillet 2020[50].

[47]Le développement d'une composante spatiale est nécessaire pour parvenir à des connexions point à point de longue distance (supérieures à 1000 km) que les infrastructures terrestres ne peuvent supporter. En exploitant les propriétés de la mécanique quantique, l'ICQ permettra dans un premier temps aux parties de partager de manière sécurisée des clés secrètes aléatoires servant au cryptage et au décryptage de messages. Elle inclura également le déploiement d'une infrastructure d'essai et de conformité, afin d'évaluer la conformité des dispositifs et systèmes européens de communication quantique avec l'infrastructure ICQ, ainsi que leur certification et leur validation avant qu'ils ne soient intégrés dans cette dernière. Elle sera conçue pour pouvoir prendre en charge des applications supplémentaires à mesure que celles-ci atteindront le niveau de maturité technologique requis. Le projet pilote OpenQKD (https://openqkd.eu/) actuel est le prédécesseur de cette infrastructure d'essai et de conformité.

[48]Communication intitulée «Sécurité du déploiement de la 5G dans l'UE – Mise en œuvre de la boîte à outils de l'UE», COM(2020) 50.

[49]Rapport de la Commission relatif aux effets de la recommandation de la Commission du 26 mars 2019 sur la cybersécurité des réseaux 5G, 15 décembre 2020.

[50]Rapport du 24 juillet 2020 du groupe de coopération SRI sur la mise en œuvre de la boîte à outils.

En octobre 2020, le Conseil européen a invité l'UE et les États membres à «tirer pleinement parti de la boîte à outils de l'UE pour la cybersécurité de la 5G» et à «appliquer les restrictions pertinentes aux fournisseurs à haut risque d'actifs essentiels, définis comme critiques et sensibles dans les évaluations coordonnées des risques au niveau de l'UE, sur la base de critères objectifs communs»[51].

À l'avenir, l'UE et ses États membres devraient veiller à ce que les risques recensés aient été atténués de manière adéquate et coordonnée, notamment à l'aune de l'objectif visant à réduire au minimum l'exposition aux fournisseurs à haut risque et à éviter la dépendance à l'égard de ces fournisseurs au niveau national et de l'Union, et à ce que toute nouvelle évolution significative ou tout nouveau risque significatif soit pris en compte. Les États membres sont invités à tirer pleinement parti de la boîte à outils dans le cadre de leurs investissements dans les capacités numériques et la connectivité.

Sur la base du rapport relatif aux effets de la recommandation de 2019, la Commission encourage les États membres à accélérer les travaux visant à achever la mise en œuvre des principales mesures de la boîte à outils d'ici au deuxième trimestre de 2021. Elle invite également les États membres à continuer à suivre ensemble les progrès accomplis et à poursuivre l'harmonisation des approches suivies. Au niveau de l'UE, ce processus sera soutenu par trois grands objectifs: assurer une plus grande convergence des approches en matière d'atténuation des risques dans l'ensemble de l'UE, soutenir l'échange continu de connaissances et le renforcement des capacités, et promouvoir la résilience de la chaîne d'approvisionnement et d'autres objectifs de sécurité stratégique de l'UE. Des actions concrètes liées à ces objectifs clés sont exposées dans l'appendice spécifique de la présente communication.

La Commission continuera de travailler en étroite collaboration avec les États membres pour mettre en œuvre ces objectifs et actions avec le soutien de l'ENISA (voir annexe).

L'approche de la boîte à outils de l'UE relative à la 5G a par ailleurs suscité un intérêt dans les pays tiers qui mettent au point actuellement leur approche de sécurisation de leurs réseaux de communication. Les services de la Commission, conjointement avec le Service européen pour l'action extérieure et le réseau des délégations de l'UE, se tiennent prêts à fournir aux autorités du monde entier, si nécessaire, des informations complémentaires sur leur approche globale, objective et fondée sur les risques.

1.5 Un internet d'objets sécurisés

Chaque objet connecté présente des vulnérabilités qui peuvent être exploitées avec des ramifications potentiellement importantes. Les règles du marché intérieur comprennent des mesures de protection contre les produits et services non sûrs. La Commission s'emploie déjà à garantir des **solutions de sécurité et une certification transparentes dans le cadre du règlement sur la cybersécurité** et à encourager la sécurité des produits et services sans compromettre leur performance[52]. Elle adoptera son premier programme de travail glissant de

[51]EUCO 13/20, Réunion extraordinaire du Conseil (1er et 2 octobre 2020) – Conclusions.

[52]Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification des technologies de l'information et des communications en matière de cybersécurité et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité). Le règlement sur la cybersécurité promeut la certification des TIC au niveau de l'UE, au moyen d'un cadre européen de certification de cybersécurité pour la création de schémas européens volontaires de certification de cybersécurité dont le but est de garantir un niveau adéquat de cybersécurité pour les produits

l'Union au cours du premier trimestre de 2021 (à mettre à jour au moins une fois tous les trois ans) afin de permettre à l'industrie, aux autorités nationales et aux organismes de normalisation de se préparer à l'avance aux futurs schémas européens de certification de cybersécurité[53]. À mesure que l'expansion de l'internet des objets se poursuit, il convient de renforcer les règles applicables, tant pour garantir la résilience globale que pour renforcer la cybersécurité.

La Commission envisagera une approche globale, comprenant d'éventuelles **nouvelles règles horizontales visant à améliorer la cybersécurité de tous les produits connectés et services associés mis sur le marché intérieur**[54]. De telles règles pourraient prévoir un **nouveau devoir de diligence pour les fabricants d'appareils connectés**, afin qu'ils remédient aux vulnérabilités des logiciels, notamment en poursuivant les mises à jour de logiciels et de sécurité, ainsi qu'en garantissant la suppression de données à caractère personnel et d'autres données sensibles à la fin de la vie des appareils. Ces règles renforceraient l'initiative pour le droit à la réparation des logiciels obsolètes présentée dans le cadre du plan d'action pour l'économie circulaire et compléteraient les mesures en vigueur couvrant des types de produits spécifiques, telles que des exigences contraignantes à proposer pour l'accès au marché de certains produits sans fil (au moyen d'un acte délégué relevant de la directive sur les équipements radioélectriques[55]), et l'objectif visant à mettre en œuvre les règles de cybersécurité applicables aux véhicules à moteur pour tous les nouveaux types de véhicules à partir de juillet 2022[56]. Elles s'appuieraient en outre sur la proposition de révision des règles relatives à la sécurité générale des produits, qui ne traitent pas directement des aspects liés à la cybersécurité[57].

1.6 Une plus grande sécurité mondiale de l'internet

Un ensemble de protocoles de base et d'infrastructures de soutien garantit la fonctionnalité et l'intégrité de l'internet dans le monde entier[58]. Cet ensemble comprend le DNS (Domain Name System, système de noms de domaine) et son système hiérarchique et délégué de zones, commençant, en haut de la hiérarchie, par la zone racine et les treize serveurs racines du DNS[59] dont dépend le World Wide Web. La Commission a l'intention d'élaborer **un plan**

TIC, services TIC et processus TIC dans l'Union, ainsi que de réduire la fragmentation du marché intérieur en ce qui concerne les schémas de certification de cybersécurité dans l'Union. Parallèlement, les entreprises spécialisées dans la «notation» de la cybersécurité sont généralement établies en dehors de l'UE, avec pour corollaire une transparence et une surveillance limitées; https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings

[53]Conformément à l'article 47, paragraphe 5, du règlement sur la cybersécurité.

[54]Les conclusions du Conseil plaident en faveur de mesures horizontales pour la cybersécurité des dispositifs connectés; 13629/20, 2 décembre 2020.

[55]Directive 2014/53/UE.

[56] En phase avec le règlement ONU adopté en juin 2020; http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf

[57]Révision des règles actuelles relatives à la sécurité générale des produits (directive 2001/95/CE); des règles adaptées concernant la responsabilité des producteurs devraient également être proposées dans le contexte numérique, dans le cadre réglementaire de l'UE en matière de responsabilité.

[58] «Le noyau public de l'internet ouvert, à savoir ses principaux protocoles et ses principales infrastructures, qui constituent un bien public mondial, joue un rôle essentiel dans la fonction de l'internet en général et soutient son fonctionnement normal. L'ENISA devrait soutenir la sécurité du noyau public de l'internet ouvert et la stabilité de son fonctionnement, y compris, sans s'y limiter, ses protocoles clés (notamment DNS, BGP et IPv6), le fonctionnement du système des noms de domaines (tel que le fonctionnement de tous les domaines de premier niveau) et le fonctionnement de la zone racine»; considérant 23 du règlement sur la cybersécurité.

[59] https://www.iana.org/domains/root/servers

d'urgence, soutenu par un financement de l'UE, destiné à faire face à des scénarios extrêmes portant atteinte à l'intégrité et à la disponibilité du système mondial de serveurs racines du DNS. Elle collaborera avec l'ENISA, les États membres, les opérateurs des deux serveurs racines du DNS de l'UE[60] et la communauté multipartite afin d'évaluer le rôle joué par ces opérateurs pour garantir que l'internet reste accessible à l'échelle mondiale en toutes circonstances.

Pour qu'un client accède à une ressource sous un nom de domaine donné sur l'internet, sa requête (généralement une adresse URL – Uniform Resource Locator) doit être traduite ou «résolue» en une adresse IP, par référence aux serveurs de noms de domaine (DNS). Toutefois, les citoyens et les organisations de l'UE s'appuient de plus en plus sur quelques services de résolution de noms de domaine publics gérés par des entités de pays tiers. Cette concentration de la résolution des noms de domaine entre les mains d'un petit nombre d'entreprises[61] rend le processus de résolution lui-même vulnérable en cas d'événements importants touchant un fournisseur important, et complique la tâche des autorités de l'UE si elles doivent répondre à d'éventuelles cyberattaques malveillantes et à d'éventuels incidents géopolitiques et techniques majeurs[62].

En vue de réduire les problèmes de sécurité liés à la concentration du marché, la Commission encouragera les parties prenantes, y compris les entreprises, fournisseurs de services internet et vendeurs de navigateurs de l'UE, à adopter une stratégie de diversification de la résolution de noms de domaine. Elle compte également contribuer à la sécurité de la connectivité internet en favorisant la mise sur pied d'un **service européen public de résolution de noms de domaine**. Cette initiative «DNS4EU» offrira un autre service, européen, pour accéder à l'internet mondial. DNS4EU sera transparent et conforme aux normes et règles les plus récentes en matière de sécurité, de protection des données et de vie privée dès la conception et par défaut, et fera partie de l'alliance industrielle européenne pour les données et l'informatique en nuage[63].

La Commission, en liaison avec les États membres et les entreprises du secteur, va également **accélérer l'adoption des normes clés de l'internet, notamment l'IPv6**[64], **et des normes et bonnes pratiques de sécurité internet bien établies en matière de DNS, de routage et de sécurité du courrier électronique**[65], sans exclure des mesures réglementaires telles qu'une clause européenne de limitation dans le temps pour l'IPv4 afin d'orienter le marché si les progrès réalisés en vue de leur adoption sont insuffisants. L'UE devrait agir (par exemple

[60] Les serveurs i.root gérés par Netnod en Suède et les serveurs k.root gérés par RIPE NCC aux Pays-Bas.
[61] Consolidation in the DNS resolver market – how much, how fast how dangerous? (), Evidence of decreasing Internet entropy – the lack of redundancy in DNS resolution by major websites and services ( )
[62] Il est également prouvé que les données DNS peuvent être utilisées à des fins de profilage, ce qui a une incidence sur le respect des droits à la vie privée et à la protection des données.
[63] Déclaration commune: Building the next generation cloud for businesses and the public sector in the EU (Construire l'informatique en nuage de la prochaine génération pour les entreprises et le secteur public dans l'UE); https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe
[64] Le déploiement de l'IPv6 est désormais plus avancé avec la forte baisse de l'offre et l'augmentation du coût des adresses IPv4. Ce déploiement est cependant inégal dans l'UE.
[65] Parmi ces normes figurent DNSSEC, HTTPS, DNS over HTTPS (DoH), DNS over TLS (DoT), SPF, DKIM, /DMARC, STARTTLS, DANE et les normes et bonnes pratiques en matière de routage comme l'initiative MANRS (Mutually Agreed Norms for Routing Security ou Normes convenues mutuellement pour la sécurité du routage).

dans le cadre de la stratégie UE-Afrique[66]) en faveur de la mise en œuvre de ces normes dans les pays partenaires afin de soutenir le développement de l'internet mondial et ouvert et de contrer les modèles d'internet fermés et fondés sur des contrôles. Enfin, la Commission examinera la nécessité d'un mécanisme permettant un suivi et une collecte plus systématiques de données agrégées sur le trafic internet et des conseils sur les perturbations potentielles[67].

1.7 Une présence renforcée sur la chaîne d'approvisionnement en technologies

Grâce au soutien financier qu'elle prévoit d'apporter à la transformation numérique cybersécurisée au titre du cadre financier pluriannuel 2021-2027, l'UE dispose d'une occasion unique de mettre en commun ses actifs afin de promouvoir sa stratégie industrielle[68] et son rôle de chef de file dans le domaine des technologies numériques et de la cybersécurité tout au long de la chaîne d'approvisionnement numérique (y compris les données et l'informatique en nuage, les technologies de processeurs de nouvelle génération, la connectivité ultrasécurisée et les réseaux 6G), conformément à ses valeurs et priorités. L'intervention du secteur public devrait s'appuyer sur les outils fournis par le cadre réglementaire de l'UE en matière de marchés publics et les projets importants d'intérêt européen commun. Au-delà de cela, elle peut débloquer des investissements privés grâce à des partenariats public-privé (notamment en s'appuyant sur l'expérience du partenariat public-privé contractuel sur la cybersécurité et sa mise en œuvre par l'intermédiaire de l'Organisation européenne pour la cybersécurité), à du capital-risque à l'appui des PME ou à des alliances et stratégies industrielles en matière de capacités technologiques.

Une attention particulière sera également accordée à l'instrument d'appui technique[69] et à l'utilisation optimale des derniers outils de cybersécurité par les PME, en particulier celles qui ne relèvent pas du champ d'application de la directive SRI révisée, y compris au moyen d'activités spécifiques dans le cadre des pôles d'innovation numérique du programme pour une Europe numérique. L'objectif est de susciter un volume d'investissement similaire de la part des États membres, qui sera complété par les entreprises du secteur au titre d'un partenariat cogéré avec les États membres dans le cadre du **Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et du Réseau de centres nationaux de coordination (CCCN)**, tels que proposés. Le CCCN devrait jouer un rôle essentiel, avec la contribution du secteur et des milieux universitaires, dans le développement de la souveraineté technologique de l'UE en matière de cybersécurité, dans le renforcement des capacités de sécurisation des infrastructures sensibles telles que la 5G et dans la réduction de la dépendance vis d'autres parties du monde pour les technologies les plus cruciales.

La Commission entend soutenir, potentiellement avec le CCCN, la mise au point d'un programme spécifique de master en cybersécurité, et contribuer à l'élaboration d'une feuille de route européenne commune pour la recherche et l'innovation en matière de cybersécurité au-delà de 2020. Les investissements réalisés par l'intermédiaire du CCCN s'appuieraient également sur la coopération en matière de recherche et de développement menée par les

[66] Communication conjointe intitulée «Vers une stratégie globale avec l'Afrique», 9.3.2020, JOIN(2020) 4 final.
[67] Un tel «observatoire de l'internet» pourrait s'inscrire dans le cadre des activités du Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité; proposition de règlement établissant le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination, COM(2018) 630 final.
[68] Communication sur une nouvelle stratégie industrielle pour l'Europe, COM(2020) 102 final.
[69] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=COM:2020:0409:FIN.

réseaux de centres d'excellence en matière de cybersécurité, qui réunissent les meilleures équipes de recherche européennes et les entreprises du secteur pour concevoir et mettre en œuvre des programmes de recherche communs, conformément à la feuille de route de l'Organisation européenne pour la cybersécurité[70]. La Commission continuera de s'appuyer sur les travaux de recherche menés par l'ENISA et Europol et continuera également de soutenir, dans le cadre du programme Horizon Europe, les différents innovateurs internet qui développent des technologies de communication sécurisées et respectueuses de la vie privée fondées sur des logiciels et du matériel libres, comme c'est actuellement le cas de l'initiative «Internet de nouvelle génération».

1.8 Une main-d'œuvre européenne cyberqualifiée

Les efforts déployés par l'UE pour assurer le perfectionnement de la main-d'œuvre, pour développer, attirer et conserver les meilleurs talents en matière de cybersécurité et pour investir dans des activités de recherche et d'innovation de classe mondiale constituent un élément important de la protection contre les cybermenaces en général. Ce domaine offre un grand potentiel. Aussi convient-il d'accorder une attention particulière au développement, à l'attraction et à la conservation de talents plus diversifiés. La version révisée du plan d'action en matière d'éducation numérique permettra de sensibiliser à la cybersécurité parmi les personnes, en particulier les enfants et les jeunes, et les organisations, en particulier les PME[71]. Elle encouragera également la participation des femmes à l'enseignement des sciences, des technologies, de l'ingénierie et des mathématiques («STEM»), ainsi que le perfectionnement des emplois dans le domaine des TIC et la reconversion dans les compétences numériques. En outre, la Commission, de concert avec l'Office de l'Union européenne pour la propriété intellectuelle au sein d'Europol, l'ENISA, les États membres et le secteur privé, mettra au point des outils de sensibilisation et des orientations pour accroître la résilience des entreprises de l'UE **face au vol de propriété intellectuelle facilité par les TIC**[72].

L'éducation, y compris l'enseignement et la formation professionnels (EFP), la sensibilisation et les exercices devraient également permettre de renforcer les compétences en matière de cybersécurité et de cyberdéfense au niveau de l'UE. À cette fin, les acteurs concernés de l'UE tels que l'ENISA, l'Agence européenne de défense (AED) et le Collège européen de sécurité et de défense (CESD)[73] devraient rechercher des synergies entre leurs activités respectives.

Initiatives stratégiques

L'UE devrait veiller à:

- adopter la directive SRI révisée;
- adopter des mesures réglementaires pour un internet des objets sécurisés;
- atteindre, grâce à l'investissement du CCCN dans la cybersécurité (notamment par l'intermédiaire du programme pour une Europe numérique, d'Horizon Europe et de la

[70] https://ecs-org.eu/working-groups/wg6-sria-and-cyber-security-technologies
[71] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_fr
[72] https://ec.europa.eu/commission/presscorner/detail/fr/IP_20_2187
[73] Par l'intermédiaire de la plateforme de formation, d'entraînement, d'exercices et d'évaluation (ETEE) dans le domaine du cyber.

facilité pour la reprise), jusqu'à 4,5 milliards d'EUR d'investissements publics et privés sur la période 2021-2027;

- mettre en place un réseau européen de centres des opérations de sécurité reposant sur l'IA et une infrastructure de communication ultrasécurisée exploitant les technologies quantiques;
- favoriser l'adoption généralisée des technologies de cybersécurité grâce à un soutien spécifique aux PME dans le cadre des pôles d'innovation numérique;
- mettre au point un service de résolution de noms de domaine de l'UE en tant que solution de remplacement sûre et ouverte d'accès à l'internet pour les citoyens, les entreprises et les administrations publiques de l'UE; et
- achever la mise en œuvre de la «boîte à outils» de la 5G d'ici le deuxième trimestre de 2021 (voir annexe).

2. RENFORCEMENT DES CAPACITÉS OPÉRATIONNELLES DE PRÉVENTION, DE DISSUASION ET DE RÉACTION

Les incidents de cybersécurité, qu'ils soient accidentels ou qu'ils résultent d'une action délibérée de délinquants, d'acteurs étatiques ou d'autres acteurs non étatiques, peuvent causer des dommages considérables. Leur ampleur et leur complexité, qui impliquent souvent l'exploitation des services, du matériel et des logiciels de tiers pour compromettre un objectif final, rendent difficile la lutte contre l'environnement de menace collectif de l'UE sans partage d'informations et coopération systématiques et complets sur une réaction commune. L'UE cherche, **par la mise en œuvre intégrale des outils réglementaires, la mobilisation et la coopération**, à aider les États membres à défendre leurs citoyens, ainsi que leurs intérêts économiques et nationaux en matière de sécurité, dans le plein respect des libertés et droits fondamentaux et de l'état de droit. Plusieurs communautés, composées de réseaux, d'institutions, organes et agences de l'UE, ainsi que d'autorités des États membres, sont chargées de prévenir et de décourager les cybermenaces, d'en dissuader les auteurs potentiels et d'y réagir, en utilisant leurs instruments et initiatives respectifs[74]. Ces communautés comprennent: i) les autorités SRI, telles que les CSIRT, et la réaction aux catastrophes, ii) les autorités répressives et judiciaires, iii) la cyberdiplomatie et iv) la cyberdéfense.

2.1 Une unité conjointe de cybersécurité

Une unité conjointe de cybersécurité servirait de plateforme virtuelle et physique de coopération pour les différentes communautés de cybersécurité de l'UE, en mettant l'accent sur la coordination opérationnelle et technique contre les menaces et cyberincidents transfrontières majeurs**.**

[74] Y compris le soutien de l'Agence de l'Union européenne pour la cybersécurité (ENISA) à la coopération opérationnelle et à la gestion des crises; le réseau des CSIRT; le réseau CyCLONe (réseau des organisations de liaison en matière de crises de cybersécurité, devant devenir le réseau UE-CyCLONe comme proposé dans la directive SRI révisée); le groupe de coopération SRI; «rescEU»; le Centre européen de lutte contre la cybercriminalité et la Force d'action anticybercriminalité européenne d'Europol, ainsi que le protocole de réaction d'urgence des services répressifs; le Centre de situation et du renseignement de l'UE (INTCEN) et la boîte à outils cyberdiplomatique; la capacité unique d'analyse du renseignement (SIAC); les cyberprojets relevant de la coopération structurée permanente (CSP), notamment celui intitulé «Équipes d'intervention rapide en cas d'incident informatique et assistance mutuelle dans le domaine de la cybersécurité» (CRRT).

L'unité conjointe de cybersécurité constituerait une avancée importante vers l'achèvement du **cadre européen de gestion des crises en matière de cybersécurité**. Comme indiqué dans les orientations politiques de la présidente de la Commission[75], cette unité devrait permettre aux États membres et aux institutions, organes et agences de l'UE de tirer pleinement parti des structures, ressources et capacités existantes et promouvoir une approche axée sur le «**besoin de partager (*need-to-share*)**». L'unité conjointe de cybersécurité offrirait les moyens nécessaires pour consolider les progrès accomplis jusqu'à présent dans la mise en œuvre de la recommandation de 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs (présentant un «plan d'action» en la matière)[76]. Elle permettrait également de renforcer encore la coopération autour de l'architecture proposée dans le plan d'action et d'exploiter les progrès réalisés, notamment au sein du groupe de coopération SRI et du réseau CyCLONe.

Il pourrait ainsi être possible de combler les **deux principales lacunes** qui aggravent actuellement les vulnérabilités et sont à l'origine de manques d'efficacités dans la réaction aux menaces et incidents transfrontières qui portent atteinte à l'Union. Premièrement, les **communautés** civiles, diplomatiques, répressives et militaires en matière de cybersécurité ne disposent pas encore d'un espace commun pour favoriser une coopération structurée et faciliter la coopération opérationnelle et technique. Deuxièmement, les parties prenantes concernées par la cybersécurité n'ont pas encore été en mesure d'exploiter pleinement le **potentiel** de la coopération opérationnelle et de l'assistance mutuelle au sein des communautés et réseaux existants. Il faut notamment déplorer l'absence d'une plateforme permettant une coopération opérationnelle avec le secteur privé. L'unité conjointe de cybersécurité devrait améliorer et accélérer la coordination et permettre à l'UE de faire face aux incidents et crises de cybersécurité majeurs et d'y réagir.

L'unité conjointe de cybersécurité ne serait pas un organe autonome supplémentaire, pas plus qu'elle ne modifierait les compétences et prérogatives des autorités nationales de cybersécurité ou des participants de l'UE. Cette unité servirait plutôt de filet de sécurité pour permettre aux participants de s'appuyer mutuellement sur le soutien et l'expertise des uns et des autres, en particulier dans le cas où différentes cybercommunautés seraient amenées à collaborer étroitement. Dans le même temps, les événements récents montrent la nécessité pour l'UE d'accroître son niveau d'ambition et sa capacité à faire face au paysage composé par les cybermenaces et aux réalités en la matière. Dans le cadre de leur contribution à l'unité conjointe de cybersécurité, les acteurs de l'UE (Commission et agences et organes de l'UE) seront donc prêts à accroître sensiblement leurs ressources et capacités, de manière à renforcer leur état de préparation et leur résilience.

L'unité conjointe de cybersécurité permettrait d'atteindre trois objectifs principaux. Premièrement, elle garantirait l'**état de préparation** de l'ensemble des communautés de la cybersécurité; deuxièmement, grâce à la mise en commun d'informations, elle permettrait une **connaissance** de la situation qui serait partagée en continu; troisièmement, elle renforcerait la coordination en matière de **réaction** et de relance. Pour atteindre ces objectifs, l'unité conjointe de cybersécurité devrait s'appuyer sur des **composantes et finalités** clairement définies, comme la garantie d'un **partage d'informations rapide et sûr**,

[75]«Une Union plus ambitieuse - Mon programme pour l'Europe», Orientations politiques pour la prochaine Commission européenne (2019-2024), par Ursula von der Leyen, candidate à la présidence de la Commission européenne.

[76]Projet de recommandation C(2017) 6100 final du 13.9.2017 sur la réaction coordonnée aux incidents et crises de cybersécurité à grande échelle.

l'amélioration de la **coopération** entre participants, en prévoyant notamment une interaction entre États membres et entités compétentes de l'UE, la mise en place de **partenariats structurés avec une base industrielle de confiance**, et la facilitation d'une approche coordonnée de la **coopération avec des partenaires extérieurs**. Pour ce faire, sur la base d'une cartographie des capacités disponibles au niveau national et au niveau de l'UE, l'unité conjointe de cybersécurité pourrait faciliter l'élaboration d'un cadre de coopération.

Pour faire en sorte que l'unité conjointe de cybersécurité occupe une place centrale dans la coopération opérationnelle de l'UE en matière de cybersécurité, la Commission collaborera avec les États membres et les institutions, organes et organismes de l'UE concernés, notamment l'ENISA, CERT-EU et Europol, afin de promouvoir une **approche graduelle et inclusive**, dans le plein respect des compétences et mandats de toutes les parties prenantes. Conformément à cette approche, l'unité conjointe de cybersécurité pourrait contribuer à renforcer la coopération entre les éléments constitutifs d'une cybercommunauté spécifique, lorsque ceux-ci l'estiment nécessaire.

Quatre grandes étapes sont proposées pour la mise en place de l'unité conjointe de cybersécurité:

- *définir*, en recensant les capacités disponibles au niveau national et au niveau de l'UE;
- *préparer*, en établissant un cadre pour la coopération structurée et l'assistance ;
- *déployer*, en mettant en œuvre le cadre s'appuyant sur les ressources fournies par les participants, afin que l'unité conjointe de cybersécurité devienne opérationnelle;
- *étendre*, en renforçant la capacité de réaction coordonnée avec la contribution du secteur et des partenaires.

En s'inspirant des résultats de la consultation des États membres et des institutions, organes et organismes de l'UE[77], la Commission présentera d'ici à février 2021, avec la participation du haut représentant et dans le cadre des compétences de celui-ci, le processus, les étapes et un calendrier pour **définir, préparer, déployer et étendre l'unité conjointe de cybersécurité**.

2.2 Combattre la cybercriminalité

Notre dépendance à l'égard des outils en ligne a augmenté de manière exponentielle la surface d'attaque des cybercriminels et mené à une situation dans laquelle, pour pratiquement tous les types d'infractions, les enquêtes présentent une composante numérique. En outre, des pans essentiels de notre société sont menacés par les cyberacteurs et par ceux qui utilisent des outils informatiques pour planifier et exécuter des actes illicites. Il existe donc des liens étroits avec la politique globale de sécurité de l'UE, comme en témoignent les éléments touchant à la cybersécurité qui figurent dans sa stratégie de 2020 pour l'union de la sécurité et dans le programme de lutte antiterroriste de l'UE[78].

[77]Consultation des États membres (y compris durant l'exercice Blue OLEx 2020 rassemblant les responsables des autorités nationales de cybersécurité) et des institutions, organes et organismes de l'UE ayant eu lieu entre juillet et novembre 2020.
[78]Communication intitulée «Un programme de lutte contre le terrorisme pour l'UE: anticiper, prévenir, protéger et réagir», 9 décembre 2020, COM(2020) 795 final.

La lutte efficace contre la cybercriminalité est un facteur clé pour garantir la cybersécurité: la dissuasion ne peut être obtenue par la seule résilience, mais exige également d'identifier et de poursuivre les auteurs d'infractions. Il est donc essentiel de favoriser la coopération et les échanges entre les acteurs de la cybersécurité et les services répressifs. Au niveau de l'UE, Europol et l'ENISA ont par conséquent déjà mis en place une coopération étroite dans le cadre de laquelle les deux agences ont organisé des conférences et des ateliers en commun et fourni des rapports conjoints à la Commission, aux États membres et à d'autres parties prenantes au sujet des menaces et défis technologiques en matière de cybersécurité. La Commission continuera à soutenir cette approche intégrée afin de garantir une réponse cohérente et efficace, se fondant sur des informations permettant de dresser un tableau complet de la situation.

L'un des éléments importants de cette réponse est que les autorités nationales et de l'UE doivent étendre et améliorer la capacité des services répressifs à enquêter sur la cybercriminalité, en respectant pleinement les droits fondamentaux et en assurant l'équilibre nécessaire entre les différents droits et intérêts. L'UE devrait être en mesure de lutter contre la cybercriminalité grâce à la mise en œuvre pleine et entière d'une législation adaptée à sa finalité, en mettant en particulier l'accent sur la lutte contre la pédopornographie en ligne et sur les enquêtes numériques, y compris la criminalité sur le «dark net». Les services répressifs doivent disposer de tous les moyens nécessaires pour mener des enquêtes numériques. La Commission présentera donc un plan d'action visant à améliorer les capacités numériques des services répressifs, en leur fournissant les compétences et outils nécessaires. En outre, Europol continuera à développer son rôle de centre d'expertise pour soutenir les autorités répressives nationales dans la lutte contre la criminalité facilitée par internet et la criminalité cyberdépendante (c'est-à-dire les infractions ne pouvant être commises qu'au moyen de dispositifs et de systèmes informatiques), en contribuant à la définition de normes communes en matière de police scientifique (par l'intermédiaire du laboratoire et de la plateforme d'innovation d'Europol).Toutes ces activités exigent d'être adoptées d'une manière appropriée par les États membres, qui sont encouragés à utiliser les programmes nationaux du Fonds pour la sécurité intérieure et à proposer des projets en réponse aux appels à propositions dans le cadre de la facilité thématique.

La Commission utilisera tous les moyens adéquats, y compris les procédures d'infraction, pour faire en sorte que la directive de 2013 relative aux attaques contre les systèmes d'information[79] soit pleinement transposée et mise en œuvre, y compris la fourniture de statistiques par les États membres. Il sera ainsi possible de mieux prévenir l'utilisation abusive des noms de domaine, y compris, le cas échéant, pour la diffusion de contenus illicites, et de s'efforcer d'assurer la disponibilité de données d'enregistrement précises en poursuivant le dialogue avec la Société pour l'attribution des noms de domaines et des numéros sur Internet (ICANN) et d'autres parties prenantes du système de gouvernance de l'internet, notamment par l'intermédiaire du groupe de travail sur la sécurité publique du comité consultatif gouvernemental de l'ICANN. La proposition figurant dans la directive SRI révisée prévoit dès lors la tenue à jour de bases de données précises et complètes de noms de domaine et de données d'enregistrement, ou «données WHOIS», et la fourniture d'un accès licite à ces données, en tant qu'éléments essentiels pour garantir la sécurité, la stabilité et la résilience du système de noms de domaines (DNS).

[79]Directive 2013/40/UE relative aux attaques contre les systèmes d'information.

La Commission continuera également d'œuvrer à la mise en place de canaux appropriés et à la clarification des règles aux fins d'obtenir un accès transfrontière aux preuves électroniques pour les enquêtes pénales (nécessaires dans 85 % des enquêtes, 65 % du total des demandes étant adressées à des fournisseurs établis dans une autre juridiction), en facilitant l'adoption et la mise en œuvre ultérieure du «train de mesures sur les preuves électroniques» et des mesures pratiques[80]. L'adoption rapide, par le Parlement européen et le Conseil, des propositions relatives aux preuves électroniques est indispensable pour que les professionnels disposent d'un outil efficace. Les preuves électroniques doivent être lisibles, de sorte que la Commission poursuivra ses travaux sur le soutien à la capacité des services répressifs dans le domaine des enquêtes numériques, y compris le traitement du cryptage dans le cadre d'enquêtes pénales, tout en préservant pleinement la fonction de celui-ci en matière de protection des droits fondamentaux et de la cybersécurité.

2.3 Boîte à outils cyberdiplomatique de l'UE

L'UE utilise sa **boîte à outils cyberdiplomatique**[81] pour empêcher les actes de cybermalveillance, les décourager, les prévenir et y faire face. Après l'introduction, en mai 2019, du cadre juridique permettant d'imposer des mesures restrictives ciblées contre les cyberattaques[82], l'UE a imposé, en juillet 2020, des sanctions à six personnes et trois entités responsables de cyberattaques visant l'UE et ses États membres, ou ayant participé à de telles attaques, dans le cadre de ce régime[83]. Deux autres personnes et un organisme ont été inscrits sur la liste en octobre 2020[84]. Les actes de cybermalveillance, y compris ceux dont les effets ne se font sentir que lentement, devraient être combattus au moyen d'une réponse diplomatique conjointe efficace et globale de l'UE, en utilisant l'ensemble des mesures disponibles au niveau de l'UE.

Une réponse diplomatique commune rapide et efficace de l'UE requiert une solide connaissance partagée de la situation et la capacité de préparer rapidement une position commune de l'UE. Le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité encouragera et facilitera la mise en place, au sein du Centre de situation et de renseignement de l'UE (INTCEN), d'un **groupe de travail des États membres de l'UE en**

[80]COM(2018) 225 et 226; C(2020) 2779 final. En particulier, le projet SIRIUS a récemment bénéficié d'un financement supplémentaire au titre de l'instrument de partenariat afin d'améliorer les canaux permettant d'obtenir un accès transfrontière licite aux preuves électroniques pour les enquêtes pénales (nécessaires dans 85 % des enquêtes portant sur des infractions graves, 65 % du total des demandes étant adressées à des fournisseurs établis dans une autre juridiction), et de définir des règles compatibles au niveau international.

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

[82]Décision (PESC) 2019/797 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres (JO L 129I du 17.5.2019, p. 13); et règlement (UE) 2019/796 du Conseil
du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres (JO L 129I du 17.5.2019, p. 1).

[83]Décision (PESC) 2020/1127 du Conseil du 30 juillet 2020 modifiant la décision (PESC) 2019/797 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres (ST/9564/2020/INIT) (JO L 246 du 30.7.2020, p. 12); et règlement d'exécution (UE) 2020/1125 du Conseil du 30 juillet 2020 mettant en œuvre le règlement (UE) 2019/796 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres (ST/9564/2020/INIT) (JO L 246 du 30.7.2020, p. 4).

[84] Décision (PESC) 2020/1537 du Conseil du 22 octobre 2020 modifiant la décision (PESC) 2019/797 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres (JO L 351I du 22.10.2020, p. 5); et règlement d'exécution (UE) 2020/1536 du Conseil du 22 octobre 2020 mettant en œuvre le règlement (UE) 2019/796 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres (JO L 351I du 22.10.2020, p. 1).

matière de cyber-renseignement, chargé de faire progresser la coopération stratégique en matière de renseignement sur les cybermenaces et les actes de cybermalveillance. Ces travaux continueront de soutenir la connaissance de la situation et la prise de décision au niveau de l'UE en ce qui concerne une réponse diplomatique conjointe. Le groupe de travail doit coopérer avec les structures existantes[85], y compris, le cas échéant, celles qui couvrent la menace plus large d'interférences hybrides et étrangères, afin de recueillir des informations et d'évaluer le niveau de connaissance de la situation.

Afin de renforcer sa capacité à empêcher les comportements malveillants dans le cyberespace, à les décourager, à les prévenir et à y faire face, le haut représentant, avec la participation de la Commission conformément à ses compétences, présentera une proposition visant à ce que l'UE définisse d'une manière plus précise sa **position en matière de cyberdissuasion**. S'appuyant sur les travaux menés à ce jour au titre de la boîte à outils cyberdiplomatique, cette position devrait contribuer à un comportement et à une coopération responsables des États dans le cyberespace, et devrait donner une direction particulière à la lutte contre les cyberattaques ayant les effets les plus importants, notamment celles qui portent atteinte à nos infrastructures critiques ainsi qu'à nos institutions et processus démocratiques[86], et les attaques dirigées contre les chaînes d'approvisionnement de même que les vols de propriété intellectuelle facilités par les TIC. Cette position devrait indiquer comment l'UE et les États membres pourraient tirer parti de leurs outils de communication politique, économique, diplomatique, juridique et stratégique contre les actes de cybermalveillance, et aborder la manière dont l'UE et les États membres pourraient améliorer leur capacité à imputer la responsabilité d'actes de cybermalveillance. En outre, en collaboration avec le Conseil et la Commission, le haut représentant a pour objectif d'examiner des **mesures supplémentaires au titre de la boîte à outils cyberdiplomatique**, y compris la possibilité d'autres options en matière de mesures restrictives, ainsi qu'en envisageant le **vote à la majorité qualifiée pour les inscriptions sur la liste dans le cadre du régime de sanctions horizontales pour contrer les cyberattaques**. De surcroît, l'UE devrait déployer des efforts supplémentaires pour **renforcer la coopération avec les partenaires internationaux**, y compris l'OTAN, afin de faire progresser la compréhension commune du paysage de la menace, de développer des mécanismes de coopération et de définir des réponses diplomatiques coopératives.

Le haut représentant, avec la participation de la Commission, proposera également une mise à jour des **lignes directrices relatives à la mise en œuvre de la boîte à outils cyberdiplomatique[87]**, notamment en vue d'accroître l'efficacité du processus décisionnel, et continue d'organiser régulièrement des exercices ainsi que des évaluations portant sur la boîte à outils cyberdiplomatique. De plus, l'UE devrait **intégrer davantage la boîte à outils cyberdiplomatique dans les mécanismes de gestion de crise de l'UE** et rechercher des synergies avec les efforts déployés pour lutter contre les menaces hybrides, la désinformation et l'ingérence étrangère au titre du cadre commun en matière de lutte contre les menaces hybrides[88] et du plan d'action pour la démocratie européenne. Dans ce contexte, l'UE devrait

[85]Comme la capacité unique d'analyse du renseignement de l'UE (SIAC) et, le cas échéant, les projets pertinents mis en place dans le cadre de la coopération structurée permanente (CSP), ainsi que le système d'alerte rapide (RAS) de 2018 qui a été créé pour soutenir l'approche globale de l'UE en matière de lutte contre la désinformation.

[86]Notamment en recherchant des synergies avec les initiatives au titre du plan d'action pour la démocratie européenne.

[87] Document 13007/17

[88] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52016JC0018&from=FR

réfléchir à l'interaction entre la boîte à outils cyberdiplomatique et le recours éventuel à l'article 42, paragraphe 7, du traité UE et à l'article 222 du TFUE[89].

2.4 Renforcement des capacités de cyberdéfense

L'UE et les États membres doivent renforcer leur capacité à prévenir les cybermenaces et à y faire face, conformément au niveau d'ambition de l'UE découlant de la stratégie globale de l'UE de 2016[90]. À cette fin, le haut représentant, en coopération avec la Commission, présentera un **réexamen du cadre stratégique de cyberdéfense de l'UE** afin d'accroître la coordination et la coopération entre les acteurs de l'UE[91], ainsi qu'avec et entre les États membres, y compris en ce qui concerne les missions et opérations relevant de la politique de sécurité et de défense commune (PSDC). Le cadre stratégique de cyberdéfense de l'UE devrait permettre d'éclairer les travaux dans le cadre de la future boussole stratégique (*Strategic Compass*)[92] en veillant à ce que la cybersécurité et la cyberdéfense soient davantage intégrées dans le programme de travail élargi en matière de sécurité et de défense.

En 2018, l'UE a identifié le cyberespace en tant que domaine d'opérations[93]. Le document dans lequel le Comité militaire de l'UE présentera sous peu les **«stratégie et vision militaires sur le cyberespace en tant que domaine d'opérations»** devrait définir plus précisément comment le cyberespace en tant que domaine d'opérations permet des missions et opérations militaires de l'UE dans le cadre de la PSDC. Le **réseau militaire CERT-UE**[94], mis en place par l'Agence européenne de défense (AED), contribuera à renforcer considérablement la coopération entre les États membres. En outre, afin d'assurer la cybersécurité des infrastructures spatiales critiques placées sous la responsabilité du programme spatial, l'Agence de l'Union européenne pour le programme spatial et, en particulier, le centre de surveillance de la sécurité Galileo seront renforcés et le mandat de l'Agence sera étendu à d'autres ressources essentielles du programme spatial.

L'UE et les États membres devraient donner un nouvel élan au **développement de capacités de cyberdéfense de pointe** grâce à différents instruments et politiques de l'UE, notamment le cadre stratégique de cyberdéfense de l'UE et, le cas échéant, en s'appuyant sur les travaux de l'AED. Cela nécessite de mettre fortement l'accent sur le développement et l'utilisation de technologies clés telles que l'IA, le cryptage et l'informatique quantique. Conformément aux priorités de l'UE de 2018 en matière de développement des capacités[95] et sur la base des conclusions du premier rapport complet résultant de l'examen annuel coordonné en matière de défense (EACD)[96], l'UE devrait renforcer davantage la coopération entre États membres concernant **la recherche, l'innovation et le développement en matière de cyberdéfense**, en

[89]Ces deux dispositions constituent, respectivement, la clause de défense mutuelle et la clause de solidarité.
[90]Conclusions du Conseil (document 14149/16) sur la mise en œuvre de la stratégie globale de l'UE dans le domaine de la sécurité et de la défense.
[91]Notamment le SEAE, y compris l'état-major de l'UE (EMUE), le Collège européen de sécurité et de défense (CESD), la Commission, et les agences de l'UE, en particulier l'Agence européenne de défense (AED).
[92]Conclusions du Conseil sur la sécurité et la défense du 17 juin 2020 (document 8910/20)
[93] https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/fr/pdf
[94]La mise en place d'un réseau militaire CERT-UE répond à un objectif défini dans le cadre stratégique de cyberdéfense de 2018 et vise à promouvoir une interaction et un échange d'informations, sous une forme active, entre les CERT militaires des États membres de l'UE.
[95]En juin 2018, les États membres ont convenu, au sein du comité directeur de l'AED, d'orienter la coopération en matière de défense au niveau de l'UE.
[96] Approuvé par les ministres de la défense au sein du comité directeur de l'AED en novembre 2020.
https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-(card)

encourageant les États membres à exploiter le plein potentiel de la **coopération structurée permanente (CSP)**[97] et du **Fonds européen de la défense (FED)**[98]**.**

Le futur **plan d'action de la Commission en matière de synergies entre les industries civile, de l'espace et de la défense**, qui doit être présenté au premier trimestre 2021, comprendra des mesures visant à soutenir davantage les synergies au niveau des programmes, des technologies, de l'innovation et des start-ups, conformément à la gouvernance des programmes respectifs[99].

Il convient en outre de développer des synergies et des interfaces pertinentes entre les initiatives de cyberdéfense mises en œuvre dans d'autres cadres, y compris les projets de collaboration liés au cyberespace menés[100] par les États membres dans le cadre de la coopération structurée permanente (CSP), ainsi qu'avec les structures de cybersécurité de l'UE, afin de soutenir le partage d'informations et le soutien mutuel.

Initiatives stratégiques

L'UE devrait:

- achever le cadre européen de gestion des crises en matière de cybersécurité et définir le processus, les étapes et un calendrier pour la mise en place de l'unité conjointe de cybersécurité;
- poursuivre la mise en œuvre du programme en matière de cybercriminalité dans le cadre de la stratégie pour l'union de la sécurité;
- encourager et faciliter la mise en place d'un groupe de travail des États membres sur le cyber-renseignement au sein de l'INTCEN de l'UE;
- faire progresser la position de l'UE en matière de cyberdissuasion pour empêcher les actes de cybermalveillance, les décourager, les prévenir et y faire face;
- réexaminer le cadre stratégique de cyberdéfense;
- faciliter l'élaboration des «stratégie et vision militaires de l'UE sur le cyberespace en tant que domaine d'opérations» pour les missions et opérations militaires de la PSDC;
- soutenir les synergies entre les industries civile, de la défense et de l'espace; et
- renforcer la cybersécurité des infrastructures spatiales critiques dans le cadre du programme spatial.

[97]Il existe actuellement plusieurs projets dans le cadre de la coopération structurée permanente (CSP) liés au cyberespace, notamment la Plateforme de partage d'informations en matière de réaction aux menaces et incidents informatiques, les équipes d'intervention rapide en cas d'incident informatique et l'assistance mutuelle dans le domaine de la cybersécurité, l'Académie et la Plateforme d'innovation de l'UE dans le domaine du cyber et le Centre de coordination dans le domaine du cyber et de l'information (CIDCC).

[98]Dans le cadre du Fonds européen de la défense (FED), la Commission a déjà recensé les possibilités d'éventuelles actions collaboratives de recherche et de développement en matière de cyberdéfense visant à renforcer la coopération, la capacité d'innovation et la compétitivité de l'industrie de la défense.

[99] Comme Horizon Europe, le programme pour une Europe numérique (*Digital Europe*) et le Fonds européen de la défense (FED).

[100] https://pesco.europa.eu/

3. PROMOUVOIR UN CYBERESPACE OUVERT ET MONDIAL

L'UE devrait continuer à collaborer avec ses partenaires internationaux pour promouvoir une vision et un modèle politique du cyberespace fondés sur l'État de droit, les droits de l'homme, les libertés fondamentales et les valeurs démocratiques qui apportent le développement social, économique et politique au niveau mondial et contribuent à une union de la sécurité. La coopération internationale est essentielle pour faire en sorte que le cyberespace demeure mondial, ouvert, stable et sûr. À cette fin, l'UE devrait continuer de collaborer avec les pays tiers, les organisations internationales et la communauté pluripartite afin d'élaborer et de mettre en œuvre une politique internationale cohérente et globale relative au cyberespace, en tenant compte de l'interconnexion croissante entre les aspects économiques des nouvelles technologies, la sécurité intérieure et les politiques étrangère, de sécurité et de défense. L'UE, en tant que bloc économique et commercial fort, fondé sur des valeurs démocratiques essentielles, le respect de l'état de droit et des droits fondamentaux, occupe aussi une position unique pour jouer un rôle moteur dans la définition et la promotion de normes et règles internationales.

3.1. Rôle de chef de file de l'UE en matière de normes, de règles et de cadres dans le cyberespace

Renforcement de la normalisation internationale

Pour promouvoir et défendre sa vision du cyberespace au niveau international, l'UE doit **renforcer son engagement et son rôle de chef de file s'agissant des procédures de normalisation internationales, et renforcer sa représentation au sein des organismes de normalisation internationaux et européens ainsi que d'autres organismes d'élaboration de normes**[101]. Les technologies numériques évoluant à un rythme rapide, les normes internationales sont de plus en plus importantes pour compléter les efforts réglementaires traditionnels dans des domaines tels que l'IA, l'informatique en nuage, l'informatique quantique et la communication quantique. La normalisation internationale est de plus en plus utilisée par les pays tiers pour faire progresser leur programme politique et idéologique, qui, souvent, ne correspond pas aux valeurs de l'UE. En outre, il existe un risque croissant de voir apparaître des cadres concurrents en matière de normalisation internationale, entraînant une fragmentation.

Il est essentiel d'élaborer des normes internationales dans les domaines des technologies émergentes et de l'architecture de base de l'internet conformément aux valeurs de l'UE pour garantir que l'internet reste mondial et ouvert, que les technologies soient centrées sur l'humain et axées sur le respect de la vie privée et que leur utilisation soit licite, sûre et éthique. Dans le cadre de sa future stratégie de normalisation, l'UE devrait définir ses **objectifs en matière de normalisation internationale** et mener des actions de sensibilisation proactives et coordonnées afin de les promouvoir au niveau international. Il convient de s'efforcer de renforcer la coopération et le partage des charges avec des partenaires attachés aux mêmes valeurs et les parties prenantes européennes.

[101]Par exemple l'Organisation internationale de normalisation (ISO), la Commission électrotechnique internationale (CEI), l'Union internationale des télécommunications (UIT), le Comité européen de normalisation (CEN), le Comité européen de normalisation électrotechnique(CENELEC), l'Institut européen de normalisation des télécommunications (ETSI), l'Internet Engineering Task Force (IETF), le Projet de partenariat de troisième génération (3GPP) et l'Institut de l'ingénierie électrique et électronique (IEEE).

Favoriser le comportement responsable des États dans le cyberespace

L'UE continue de collaborer avec ses partenaires internationaux pour renforcer et promouvoir un cyberespace mondial, ouvert, stable et sûr dans lequel **le droit international, en particulier la charte des Nations unies (ONU)[102], est respecté,** et **les normes, règles et principes non contraignants volontaires sur le comportement responsable des États**[103] sont suivis. Le débat multilatéral sur la sécurité internationale dans le cyberespace s'étant enlisé, il est clairement nécessaire que l'UE et les États membres adoptent une position plus proactive dans les discussions menées au sein des Nations unies et d'autres enceintes internationales compétentes. L'UE est la mieux placée pour **renforcer, coordonner et consolider les positions des États membres** dans les **enceintes** internationales et elle devrait **mettre au point une position de l'UE sur l'application du droit international dans le cyberespace**. Le haut représentant, aux côtés des États membres, a également pour objectif de faire avancer une proposition inclusive et consensuelle d'engagement politique en faveur d'un **programme d'action visant à renforcer le comportement responsable des États dans le cyberespace**[104] au sein des Nations unies. S'appuyant sur l'acquis existant tel qu'il a été approuvé par l'Assemblée générale des Nations unies[105], ce programme d'action offre une plateforme de coopération et d'échange de bonnes pratiques au sein des Nations unies et propose de mettre en place un mécanisme pour mettre en pratique les normes de comportement responsable des États et promouvoir le renforcement des capacités. En outre, le haut représentant veut consolider et encourager la mise en œuvre de **mesures de renforcement de la confiance** entre les États, y compris en partageant les meilleures pratiques aux niveaux régional et multilatéral et en contribuant à la coopération transrégionale.

L'accroissement de la connectivité mondiale ne doit pas entraîner de censure, de surveillance de masse, de violation de la vie privée ni de répression à l'encontre de la société civile, du monde universitaire ou des citoyens. L'UE devrait continuer à jouer un rôle moteur dans la protection et la promotion des **droits de l'homme et des libertés fondamentales** en ligne. Pour ce faire, l'UE devrait promouvoir davantage de conformité avec le droit et les normes internationaux relatifs aux droits de l'homme[106], mettre en œuvre son plan d'action en faveur des droits de l'homme et de la démocratie 2020-2024[107], et renforcer ses orientations dans le domaine des droits de l'homme relatives à la liberté d'expression en ligne et hors ligne[108], **donnant ainsi un nouvel élan à l'application pratique des instruments de l'UE**. L'UE devrait redoubler d'efforts pour **protéger les défenseurs des droits de l'homme, la société civile et les universitaires qui travaillent sur des questions telles que la cybersécurité, la confidentialité des données, la surveillance et la censure en ligne.** À cette fin, l'UE devrait fournir de nouvelles orientations pratiques, promouvoir les bonnes pratiques et intensifier ses

[102] https://www.un.org/fr/charter-united-nations/index.html

[103] Comme le montrent les rapports pertinents des groupes d'experts gouvernementaux chargés d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, approuvés par l'Assemblée générale des Nations unies, notamment les rapports de 2015, 2013 et 2010.

[104] https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf

[105] Comme le montrent les rapports pertinents des groupes d'experts gouvernementaux chargés d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, approuvés par l'Assemblée générale des Nations unies, notamment les rapports de 2015, 2013 et 2010.

[106] Notamment la charte des Nations unies et la déclaration universelle des droits de l'homme.

[107] https://www.consilium.europa.eu/fr/press/press-releases/2020/11/19/council-approves-conclusions-on-the-eu-action-plan-on-human-rights-and-democracy-2020-2024/

[108] https://www.consilium.europa.eu/media/28348/142549.pdf

efforts pour prévenir l'utilisation abusive des technologies émergentes, notamment en recourant, le cas échéant, à des mesures diplomatiques, ainsi qu'au contrôle des exportations de ces technologies. L'UE devrait également continuer à lutter pour la protection des membres de la société qui sont les plus vulnérables en ligne, en proposant une législation visant à mieux protéger les enfants contre les abus sexuels et l'exploitation sexuelle, ainsi qu'une stratégie sur les droits de l'enfant.

La convention de Budapest sur la cybercriminalité

L'UE continue de soutenir les pays tiers qui souhaitent adhérer à la **convention de Budapest sur la cybercriminalité du Conseil de l'Europe**, et d'œuvrer pour achever le **deuxième protocole additionnel à la convention de Budapest** qui contient des mesures et des garanties pour améliorer la coopération internationale entre les services répressifs et les autorités judiciaires, ainsi qu'entre les autorités et les fournisseurs de services d'autres pays. C'est la Commission qui participe aux négociations sur ce protocole au nom de l'UE[109]. L'actuelle initiative relative à un nouvel instrument juridique sur la cybercriminalité au niveau des Nations unies risque d'accroître les divisions et de ralentir les réformes nationales indispensables et les efforts de renforcement des capacités qui s'imposent. Elle pourrait entraver l'efficacité d'une coopération internationale contre la cybercriminalité. L'UE ne voit pas la nécessité d'un nouvel instrument juridique sur la cybercriminalité au niveau des Nations unies. L'UE continue de participer aux **échanges multilatéraux sur la cybercriminalité** afin de garantir le respect des droits de l'homme et des libertés fondamentales, grâce à l'inclusion et à la transparence, et en tenant compte de l'expertise disponible, dans le but d'apporter une valeur ajoutée à tous.

3.2 Coopération avec les partenaires et la communauté multipartite

L'UE devrait **intensifier et élargir ses dialogues sur le cyberespace avec les pays tiers** afin de promouvoir ses valeurs et sa vision concernant le cyberespace, en partageant les meilleures pratiques et en cherchant à coopérer plus efficacement. L'UE devrait également instaurer **des échanges structurés avec des organisations régionales** telles que l'Union africaine, le Forum régional de l'ASEAN, l'Organisation des États américains et l'Organisation pour la sécurité et la coopération en Europe. Dans le même temps, l'UE devrait s'efforcer de trouver un terrain d'entente, lorsque cela est possible et opportun, avec d'autres partenaires autour de questions d'intérêt commun. En collaboration avec les délégations de l'UE et, le cas échéant, avec les ambassades des États membres dans le monde entier, l'UE devrait constituer un **réseau européen informel de cyberdiplomatie** afin de promouvoir la vision de l'UE en matière de cyberespace, d'échanger des informations et de se coordonner régulièrement en ce qui concerne l'évolution du cyberespace[110].

Forte des déclarations communes du 8 juillet 2016[111] et du 10 juillet 2018[112], l'UE devrait continuer de faire progresser la **coopération UE-OTAN**, notamment en ce qui concerne les exigences d'interopérabilité en matière de cyberdéfense. Dans ce contexte, l'UE devrait poursuivre l'intégration des structures concernées de la PSDC au «Federated Mission Networking» de l'OTAN, afin de permettre l'interopérabilité des réseaux avec l'OTAN et ses

[109] Décision du Conseil de juin 2019 (ref 9116/19)
[110] L'UE pourrait également, le cas échéant, tirer parti des activités du réseau européen informel de diplomatie numérique qui rassemble les ministères des affaires étrangères des États membres.
[111] http://www.consilium.europa.eu/fr/press/press-releases/2016/07/08-eu-nato-joint-declaration/
[112] https://www.consilium.europa.eu/fr/press/press-releases/2018/07/10/eu-nato-joint-declaration/

partenaires, le cas échéant. En outre, la coopération entre l'UE et l'OTAN en matière d'éducation, de formation et d'exercices devrait être approfondie, notamment en recherchant des synergies entre le Collège européen de sécurité et de défense et le centre d'excellence de cyberdéfense coopérative de l'OTAN.

Conformément à ses valeurs, l'UE soutient et promeut résolument le **modèle multipartite de gouvernance de l'internet**. Aucun gouvernement, entité ou organisation internationale ne devrait chercher à contrôler l'internet seul. L'UE devrait poursuivre son engagement dans les enceintes[113] pour renforcer la coopération et garantir la protection des libertés et droits fondamentaux, notamment le droit à la dignité, le droit à la vie privée et la liberté d'expression et d'information. Afin de faire progresser la coopération multipartite sur les questions de cybersécurité, la Commission et le haut représentant, en fonction de leurs compétences respectives, ont pour objectif de renforcer **les échanges réguliers et structurés avec les parties prenantes**, y compris le secteur privé, le monde universitaire et la société civile, en soulignant que la nature interconnectée du cyberespace exige que toutes les parties prenantes échangent entre elles et assument leurs propres responsabilités pour maintenir un cyberespace mondial, ouvert, stable et sûr. Ces efforts apporteront une précieuse contribution aux éventuelles actions clés au niveau de l'UE.

3.3. Renforcer les capacités mondiales pour accroître la résilience mondiale

Pour que tous les pays puissent tirer parti des avantages sociaux, économiques et politiques offerts par l'internet et l'utilisation des technologies, l'UE continue d'aider ses partenaires à renforcer leur cyber-résilience, leurs capacités d'enquêtes et de poursuites dans le domaine de la cybercriminalité et leurs moyens de lutte contre les cybermenaces. Afin de garantir la cohérence globale, l'UE devrait élaborer un **programme de renforcement des cybercapacités externes de l'UE** afin d'orienter ces efforts conformément à ses lignes de conduite concernant le renforcement de ses cybercapacités externes[114] et au programme de développement durable à l'horizon 2030[115]. Ce programme devrait exploiter l'expertise des États membres et des institutions, organes, organismes et initiatives de l'UE concernés, y compris le réseau de l'UE pour le renforcement des cybercapacités[116], conformément à leurs mandats respectifs. Un **comité européen pour le renforcement des cybercapacités** sera créé pour réunir les parties prenantes institutionnelles concernées de l'UE et pour suivre les progrès accomplis, ainsi que pour recenser de nouvelles synergies et d'éventuelles lacunes. Il pourrait en outre favoriser une coopération renforcée avec les États membres, ainsi qu'avec les partenaires des secteurs public et privé et d'autres organismes internationaux compétents, afin d'assurer la coordination des efforts et d'éviter les doubles emplois.

Le renforcement des cybercapacités de l'UE devrait continuer d'être axé sur les Balkans occidentaux et le voisinage de l'UE, ainsi que sur les pays partenaires qui connaissent un développement numérique rapide. L'UE devrait soutenir par ces actions l'élaboration de législation et de politiques dans les pays partenaires qui soient conformes aux politiques et aux normes de cyberdiplomatie de l'UE en la matière. Dans ce contexte, les efforts de renforcement des capacités de l'UE dans le domaine de la numérisation devraient inclure la

[113] Comme la Société pour l'attribution des noms de domaines et des numéros sur Internet (ICANN) et le Forum sur la gouvernance de l'internet (FGI).
[114] https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf
[115] https://ec.europa.eu/environment/sustainable-development/SDGs/index_en.htm
[116] https://www.eucybernet.eu/

cybersécurité comme une caractéristique standard. À cette fin, l'UE devrait élaborer un programme de formation destiné à son personnel chargé de la mise en œuvre du renforcement des capacités numériques et des cybercapacités externes de l'UE. Conformément aux efforts déployés dans le cadre du plan d'action pour la démocratie européenne, l'UE devrait également aider les pays de ces régions à relever le défi croissant que posent les actes de cybermalveillance, qui nuisent au développement de leur société ainsi qu'**à l'intégrité et à la sécurité des systèmes démocratiques**. L'apprentissage entre pairs et entre les États membres de l'UE ainsi qu'avec les organes compétents de l'UE et les pays tiers pourrait s'avérer particulièrement utile à cet égard.

Enfin, dans le cadre du pacte en matière de PSDC civile de 2018[117], les missions PSDC civiles peuvent également contribuer à la réponse plus large de l'UE pour relever les défis en matière de cybersécurité, notamment en renforçant l'État de droit dans les pays partenaires, ainsi que les capacités de leurs services répressifs et administrations civiles.

Initiatives stratégiques

L'UE devrait:

- définir un ensemble d'objectifs pour les processus internationaux de normalisation et les promouvoir au niveau international;
- faire progresser la sécurité et la stabilité internationales dans le cyberespace, notamment grâce à la proposition de l'UE et de ses États membres relative à un programme d'action visant à renforcer le comportement responsable des États dans le cyberespace au sein des Nations unies;
- fournir des orientations pratiques sur l'application des droits de l'homme et des libertés fondamentales dans le cyberespace;
- mieux protéger les enfants contre les abus sexuels et l'exploitation sexuelle, et présenter une stratégie sur les droits de l'enfant;
- renforcer et promouvoir la convention de Budapest sur la cybercriminalité, en particulier à travers ses travaux sur le deuxième protocole additionnel à la convention de Budapest;
- élargir le dialogue de l'UE sur le cyberespace avec les pays tiers et les organisations régionales et internationales, notamment au moyen d'un réseau européen informel de cyberdiplomatie;
- renforcer les échanges avec la communauté multipartite, notamment grâce à des échanges réguliers et structurés avec le secteur privé, le monde universitaire et la société civile; et
- proposer un programme de renforcement des cybercapacités externes de l'UE et un comité européen pour le renforcement des cybercapacités.

[117] https://data.consilium.europa.eu/doc/document/ST-14611-2019-INIT/fr/pdf

III. LA CYBERSÉCURITÉ DANS LES INSTITUTIONS, ORGANES ET ORGANISMES DE L'UE

Compte tenu de leur grande visibilité politique, de leurs missions critiques visant à coordonner des questions très sensibles et de leur rôle dans la gestion d'importantes sommes d'argent public, **les institutions, organes et organismes de l'UE sont régulièrement la cible de cyberattaques**, en particulier de cyberespionnage. Toutefois, le degré de cyber-résilience et la capacité à détecter les actes de cybermalveillance et à y réagir varient considérablement entre les entités, en fonction de leur maturité. Il est donc nécessaire d'améliorer le niveau global de cybersécurité au moyen de règles cohérentes et homogènes.

Dans le domaine de la sécurité de l'information, des progrès ont été réalisés en vue d'une plus grande cohérence des **règles relatives à la protection des informations classifiées de l'UE ainsi que des informations sensibles non classifiées**. Toutefois, l'interopérabilité des systèmes d'informations classifiées reste limitée, ce qui empêche un transfert sans heurts d'informations entre les différentes entités. Des progrès supplémentaires devraient être accomplis pour permettre une approche interinstitutionnelle du traitement des informations classifiées et des informations sensibles non classifiées de l'UE, qui pourrait également servir de modèle d'interopérabilité entre les États membres. Une base de référence devrait également être établie afin de simplifier les procédures avec les États membres. L'UE devrait également développer sa capacité à communiquer de manière sécurisée avec les partenaires concernés, en s'appuyant, dans la mesure du possible, sur les modalités et procédures existantes.

Comme annoncé dans la stratégie pour l'union de la sécurité, en 2021, la Commission présentera dès lors des propositions **de règles communes contraignantes en matière de sécurité de l'information et en matière de cybersécurité pour l'ensemble des institutions, organes et organismes de l'UE**, sur la base des discussions interinstitutionnelles sur la cybersécurité qui sont en cours au niveau de l'UE[118].

Les tendances actuelles et futures en matière de télétravail nécessiteront également des investissements supplémentaires dans des équipements, des infrastructures et des outils sécurisés qui permettent de travailler à distance sur des dossiers sensibles et classifiés.

En outre, le panorama de plus en plus hostile des cybermenaces et l'incidence croissante des cyberattaques plus sophistiquées touchant les institutions, organes et organismes de l'UE font qu'il est indispensable d'accroître les investissements pour atteindre un niveau élevé de cybermaturité. Un programme de sensibilisation à la cybersécurité est actuellement mis en place; il s'adresse à l'ensemble des institutions, organismes et organes de l'UE et vise à sensibiliser le personnel, à améliorer l'hygiène informatique et à soutenir une culture commune de la cybersécurité.

Le **renforcement de CERT-UE grâce à un mécanisme de financement amélioré** est nécessaire pour accroître sa capacité à aider les institutions, organes et organismes de l'UE à appliquer les nouvelles règles de cybersécurité et à améliorer leur cyber-résilience. Le mandat de CERT-UE doit également être renforcé afin de la doter de moyens stables pour atteindre ces objectifs.

[118] Les discussions régulières sur la cybersécurité entre les institutions de l'UE s'inscrivent dans le cadre d'échanges plus larges sur les possibilités et les défis qu'implique la transformation numérique pour les institutions de l'UE.

Initiatives stratégiques

1. Règlement sur la sécurité de l'information dans les institutions, organes et organismes de l'UE
2. Règlement sur les règles communes de cybersécurité pour les institutions, organes et organismes de l'UE
3. Nouvelle base juridique pour CERT-UE afin de renforcer son mandat et son financement

IV. CONCLUSION

La mise en œuvre concertée de cette stratégie contribuera à une décennie numérique cybersécurisée pour l'UE, à la réalisation d'une union de la sécurité et au renforcement de la position de l'UE à l'échelle mondiale.

L'UE devrait fixer des normes pour des solutions mondiales et des normes de cybersécurité pour les services essentiels et les infrastructures critiques, ainsi que pour la mise au point et l'application de nouvelles technologies. Chaque organisation et chaque personne utilisant l'internet est partie prenante de la solution afin de garantir une transformation numérique cybersécurisée.

La Commission et le haut représentant, en fonction de leurs compétences respectives, suivront les progrès réalisés dans le cadre de la présente stratégie et élaboreront des critères d'évaluation. Ce suivi s'appuiera sur les rapports de l'ENISA et les rapports réguliers de la Commission sur l'union de la sécurité. Les résultats nourriront les prochains objectifs de la décennie numérique[119]. Conformément à leurs compétences respectives, la Commission et le haut représentant continueront de dialoguer avec les États membres en vue de définir des mesures pratiques pour rapprocher les quatre communautés de la cybersécurité dans l'UE des infrastructures critiques et de la résilience du marché intérieur, de la justice et des services répressifs, de la cyberdiplomatie et de la cyberdéfense, le cas échéant. En outre, la Commission et le haut représentant poursuivront leurs échanges avec la communauté multipartite, en soulignant que tous les utilisateurs de l'internet doivent jouer leur rôle dans le maintien d'un cyberespace mondial, ouvert, stable et sûr, où chacun peut vivre sa vie numérique en toute sécurité.

[119] Comme annoncé dans le programme de travail de la Commission pour 2021.

Appendice: les prochaines étapes concernant la cybersécurité des réseaux 5G

Sur la base des résultats de l'examen de la recommandation de la Commission sur la cybersécurité des réseaux 5G[120], les prochaines étapes des travaux coordonnés au niveau de l'UE devraient s'articuler autour de trois objectifs clés et des principales actions à court et à moyen terme présentées dans le tableau ci-dessous, qui seront mises en œuvre par les autorités des États membres, la Commission et l'ENISA.

Premièrement, la priorité pour la prochaine phase est d'**achever la mise en œuvre de la boîte à outils au niveau national et de résoudre les problèmes recensés dans le rapport d'avancement de juillet 2020**. Dans ce contexte, certaines des mesures stratégiques de la boîte à outils bénéficieraient **d'un travail de coordination ou d'un échange d'informations renforcé** dans le cadre du groupe ad hoc SRI, comme cela a déjà été indiqué dans le rapport d'avancement, ce qui pourrait conduire à l'élaboration de **bonnes pratiques ou d'orientations**. En ce qui concerne les mesures techniques, l'ENISA pourrait apporter un soutien supplémentaire, en s'appuyant sur le travail qu'elle a déjà accompli et en enquêtant sur certains sujets de manière plus approfondie, ainsi qu'**en dressant un aperçu complet de toutes les lignes directrices pertinentes concernant les exigences de cybersécurité applicables aux opérateurs de réseaux mobiles dans le domaine de la 5G.**

Deuxièmement, les États membres ont souligné qu'il importait de se tenir au courant des évolutions **de la technologie, de l'architecture 5G, des menaces et des différents usages et applications de la 5G, ainsi que des facteurs externes en les suivant de manière continue**, afin d'être en mesure **de repérer et de faire face aux risques nouveaux ou émergents**. En outre, un certain nombre d'aspects de l'analyse initiale des risques devraient faire l'objet d'un examen plus approfondi, notamment pour veiller à ce que celle-ci porte sur l'ensemble de l'écosystème 5G, y compris tous les éléments pertinents de l'infrastructure du réseau et de la chaîne d'approvisionnement de la 5G. Bien que la boîte à outils ait été conçue comme un instrument souple et adaptable, si nécessaire, des mesures pourraient être prises à moyen terme pour l'agrandir ou la modifier, afin de garantir qu'elle reste complète et à jour.

Troisièmement, il convient de continuer à prendre des **mesures au niveau de l'UE** pour soutenir et compléter les objectifs de la boîte à outils et pour les intégrer pleinement dans les politiques pertinentes de l'Union et de la Commission, notamment dans le prolongement des actions annoncées par la Commission dans sa communication du 29 janvier 2020 relative à la boîte à outils[121] dans un large éventail de domaines (par exemple, le financement par l'UE de réseaux 5G sécurisés, les investissements dans les technologies 5G et post-5G, les instruments de défense commerciale et la concurrence afin d'éviter les distorsions du marché de l'offre de la 5G, etc.).

Le cas échéant, les acteurs de premier plan devraient se mettre d'accord, début 2021, sur les modalités et les étapes des principales actions exposées ci-après.

Objectif clé n° 1: assurer une convergence des approches nationales en faveur d'une atténuation

[120] Rapport de la Commission relatif aux effets de la recommandation 2019/534 de la Commission du 26 mars 2019 sur la cybersécurité des réseaux 5G.

[121] Communication de la Commission du 29.1.2020 intitulée «Sécurité du déploiement de la 5G dans l'UE – Mise en œuvre de la boîte à outils de l'UE», COM(2020) 50.

efficace des risques dans l'ensemble de l'UE		
Domaines	**Principales actions à court et à moyen terme**	**Acteurs de premier plan**
Mise en œuvre de la boîte à outils par les États membres	Achever la mise en œuvre des mesures préconisées dans les conclusions de la boîte à outils d'ici au deuxième trimestre de 2021, en procédant à un bilan périodique dans le cadre du groupe ad hoc SRI.	Autorités des États membres
Échange d'informations et de bonnes pratiques sur les mesures stratégiques relatives aux fournisseurs	Intensifier les échanges d'informations et examiner les bonnes pratiques possibles, notamment en ce qui concerne: - les restrictions applicables aux fournisseurs à haut risque (MS03) et les mesures liées à la fourniture de services gérés (MS04); - la sécurité et la résilience de la chaîne d'approvisionnement, en particulier dans le prolongement de l'enquête menée par l'ORECE au sujet des MS05 et 06.	Autorités des États membres, Commission
Renforcement des capacités et orientations sur les mesures techniques	Procéder à des enquêtes techniques approfondies et élaborer des orientations et des outils communs, notamment: - une matrice complète et dynamique des contrôles de sécurité et des bonnes pratiques pour la sécurité des réseaux 5G; des orientations pour mettre en œuvre une sélection de mesures techniques issues de la boîte à outils.	ENISA, autorités des États membres
Objectif clé n° 2: soutenir l'échange continu de connaissances et le renforcement des capacités		
Domaines	**Principales actions à court et à moyen terme**	**Acteurs de premier plan**
Consolidation continue des connaissances	Organiser des activités de consolidation des connaissances sur la technologie et les défis connexes (architectures ouvertes, caractéristiques 5G — par exemple virtualisation, conteneurisation, découpage en tranches, etc.), l'évolution du panorama des menaces, les incidents réels, etc.	ENISA, autorités des États membres, autres parties prenantes
Évaluations des risques	Mettre à jour et échanger des informations sur les évaluations des risques nationales actualisées	Autorités des États membres, Commission, ENISA
Projets communs financés par l'UE soutenant la mise en œuvre de la boîte à outils	Apporter un soutien financier aux projets soutenant la mise en œuvre de la boîte à outils grâce à des fonds de l'UE, notamment dans le cadre du programme pour une Europe numérique (par exemple, projets de renforcement des capacités destinés aux autorités nationales, bancs d'essai ou autres capacités de pointe, etc.)	Autorités des États membres, Commission
Coopération entre les parties prenantes	Encourager la collaboration et la coopération entre les autorités nationales responsables de la cybersécurité de la 5G (par exemple, le groupe de coopération SRI, les autorités de cybersécurité, les autorités de régulation des télécommunications) et avec les parties prenantes privées	Autorités des États membres, Commission, ENISA
Objectif clé n° 3: promouvoir la résilience de la chaîne d'approvisionnement et d'autres objectifs de sécurité stratégique de l'UE		

Domaines	**Principales actions à court et à moyen terme**	**Acteurs de premier plan**
Normalisation	Définir et mettre en œuvre un plan d'action concret visant à renforcer la représentation de l'UE au sein des organismes de normalisation dans le cadre des prochaines étapes des travaux du sous-groupe SRI sur la normalisation, afin d'atteindre des objectifs spécifiques en matière de sécurité, y compris la promotion d'interfaces interopérables pour faciliter la diversification des fournisseurs.	Autorités des États membres
Résilience de la chaîne d'approvisionnement	- Procéder à une analyse approfondie de l'écosystème et de la chaîne d'approvisionnement de la 5G afin de mieux recenser et observer les principaux atouts et les dépendances critiques potentielles - Veiller à ce que le fonctionnement du marché et de la chaîne d'approvisionnement de la 5G soit conforme aux règles et aux objectifs de l'UE en matière de commerce et de concurrence, tels que définis dans la communication de la Commission du 29 janvier 2020, et à ce que le mécanisme filtrage des IDE soit appliqué aux investissements dont l'évolution risque d'affecter la chaîne de valeur de la 5G, en tenant compte des objectifs de la boîte à outils - Suivre l'évolution actuelle et attendue du marché et évaluer les risques et les opportunités dans le domaine du RAN ouvert, notamment au moyen d'une étude indépendante	Autorités des États membres, Commission
Certification	Entamer la préparation du ou des schémas de certification candidats pertinents pour les composants clés de la 5G et les processus des fournisseurs, afin de contribuer à couvrir certains risques liés aux vulnérabilités techniques, tels que définis dans les plans d'atténuation des risques de la boîte à outils.	Commission, ENISA, autorités nationales, autres parties prenantes
Capacités de l'UE et déploiements des réseaux sécurisés	- Investir dans la R&I et les capacités, notamment par l'adoption du partenariat pour des réseaux et services intelligents - Appliquer les conditions de sécurité pertinentes dans le cadre des programmes et instruments de financement (intérieur et extérieur) de l'UE, comme annoncé dans la communication de la Commission du 29 janvier 2020	États membres, Commission, acteurs du secteur de la 5G
Aspects extérieurs	Répondre favorablement aux demandes des pays tiers qui souhaiteraient comprendre et éventuellement utiliser l'approche de la boîte à outils élaborée par l'UE	États membres, Commission, SEAE, délégations de l'UE