COMMISSION
EUROPÉENNE

Bruxelles, le 24.7.2020
COM(2020) 605 final

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

relative à la stratégie de l'UE pour l'union de la sécurité

I. Introduction

Dans ses orientations politiques, la Commission a indiqué clairement qu'il ne fallait négliger aucun aspect pour protéger les citoyens. La sécurité est non seulement importante sur le plan personnel, mais elle protège aussi les droits fondamentaux et constitue la base de la confiance dans notre économie, dans notre société et dans notre démocratie ainsi que le fondement du dynamisme de celles-ci. Actuellement, la situation en matière de sécurité ne cesse de changer en Europe, sous l'influence de menaces qui évoluent ainsi que d'autres facteurs, dont le changement climatique, l'évolution démographique et l'instabilité politique au-delà de nos frontières. La mondialisation, la libre circulation et la transformation numérique continuent d'apporter de la prospérité, de rendre nos vies plus faciles et de stimuler l'innovation et la croissance. Toutefois, à côté de ces avantages, elles comportent également des risques et des coûts. Elles peuvent être utilisées à mauvais escient à des fins de terrorisme, de criminalité organisée, de trafic de stupéfiants et de traite des êtres humains, qui constituent autant de menaces directes pour les citoyens et notre mode de vie européen. Les cyberattaques et la cybercriminalité continuent de prendre de l'ampleur. Les menaces pesant sur la sécurité deviennent aussi plus complexes: elles se nourrissent de la possibilité d'agir à l'échelle transfrontière et de l'interconnectivité, tirent parti du flou qui caractérise désormais les frontières entre le monde réel et le monde numérique et exploitent les groupes vulnérables et les divergences socio-économiques. Des attaques peuvent survenir à tout moment et laisser très peu de traces, voire aucune; des acteurs tant étatiques que non étatiques peuvent déployer toute une série de menaces hybrides[1]; et ce qui se passe en dehors de l'UE peut avoir une incidence critique sur la sécurité à l'intérieur de l'UE.

La crise liée à la COVID-19 a également modifié notre conception des menaces pour la sûreté et la sécurité et les politiques correspondantes. Elle a mis en évidence la nécessité de garantir la sécurité tant dans l'environnement physique que dans l'environnement numérique. Elle a souligné l'importance de l'autonomie stratégique ouverte de nos chaînes d'approvisionnement en produits, services, infrastructures et technologies critiques. Elle a renforcé la nécessité d'associer chacun, et chaque secteur, à un effort commun visant à faire en sorte que l'UE soit mieux préparée et plus résiliente en amont et dispose de meilleurs outils pour réagir en cas de besoin.

La seule action individuelle des États membres ne peut suffire à protéger les citoyens. Tirer parti des points forts de chacun pour travailler ensemble n'a jamais été aussi essentiel, et l'UE est plus à même que jamais de faire la différence. Elle peut montrer l'exemple, en améliorant son système global de gestion des crises et en œuvrant à l'intérieur comme à l'extérieur de ses frontières pour contribuer à la stabilité mondiale. Bien que la responsabilité première de la sécurité incombe aux États membres, ces dernières années ont permis de mieux comprendre que la sécurité d'un État membre était la sécurité de tous. L'UE peut apporter une réponse pluridisciplinaire et intégrée, en fournissant aux acteurs de la sécurité dans les États membres les outils et les informations dont ils ont besoin[2].

---

[1] Bien qu'il existe plusieurs définitions des menaces hybrides, cette notion vise à exprimer le mélange d'activités coercitives et subversives, de méthodes conventionnelles et non conventionnelles (c'est-à-dire diplomatiques, militaires, économiques, technologiques), susceptibles d'être utilisées de façon coordonnée par des acteurs étatiques ou non étatiques en vue d'atteindre certains objectifs (sans que le seuil d'une guerre déclarée officiellement ne soit dépassé). Voir JOIN(2016) 18 (final).

[2] Par exemple, grâce aux services fournis par le programme spatial de l'UE, tels que Copernicus, qui livre des données d'observation de la Terre et a des applications dans les domaines de la surveillance des frontières, de la sûreté maritime, de la répression des infractions, de la lutte contre la piraterie, de la dissuasion en matière de trafic de stupéfiants et de la gestion des situations d'urgence.

L'UE peut aussi veiller à ce que la politique de sécurité reste fondée sur nos valeurs européennes communes, à savoir le respect de l'état de droit, de l'égalité[3] et des droits fondamentaux, ainsi que la garantie de la transparence, de l'obligation de rendre compte et du contrôle démocratique, afin de l'asseoir sur la confiance nécessaire. Elle peut mettre en place une union de la sécurité réelle et effective, caractérisée par une protection adéquate des droits et des libertés individuels. La sécurité et le respect des droits fondamentaux ne sont pas des objectifs contradictoires; ces deux éléments se complètent et forment un tout cohérent. Nos valeurs et nos droits fondamentaux doivent être à la base des politiques de sécurité, lesquelles doivent satisfaire aux principes de nécessité, de proportionnalité et de légalité et être assorties de garanties appropriées en matière d'obligation de rendre compte et de recours juridictionnel, tout en permettant de réagir efficacement pour protéger les citoyens, en particulier les plus vulnérables.

D'importants instruments juridiques, pratiques et d'appui sont déjà en place, mais ils doivent être renforcés, d'une part, et mieux mis en œuvre, d'autre part. Des progrès considérables ont été réalisés en vue d'améliorer l'échange d'informations et la coopération en matière de renseignement avec les États membres et de restreindre le périmètre d'action des terroristes et des criminels. Mais les efforts restent fragmentés.

Nous devons aussi agir au-delà des frontières de l'UE. Pour protéger l'Union et ses citoyens, il ne s'agit plus seulement de garantir la sécurité à l'intérieur des frontières de l'UE, mais aussi de s'attaquer à la dimension extérieure de la sécurité. L'approche de l'UE en matière de sécurité extérieure dans le cadre de la politique étrangère et de sécurité commune (PESC) et de la politique de sécurité et de défense commune (PSDC) restera une composante essentielle des efforts de l'UE visant à renforcer la sécurité en son sein. Face aux enjeux communs, il est fondamental de coopérer avec les pays tiers et au niveau mondial pour réagir de façon efficace et globale, la stabilité et la sécurité dans le voisinage de l'UE étant essentielles à la sécurité de l'UE.

Cette nouvelle stratégie, qui s'appuie sur les travaux antérieurs du Parlement européen[4], du Conseil[5] et de la Commission[6], montre qu'une union de la sécurité réelle et effective doit à la fois reposer sur un noyau solide d'instruments et de politiques permettant d'assurer la sécurité dans la pratique et tenir compte du fait que la sécurité a des implications pour toutes les composantes de la société et toutes les politiques publiques. L'UE doit garantir un environnement sûr à chacun, quels que soient son origine raciale ou ethnique, sa religion, ses convictions, son sexe, son âge et son orientation sexuelle.

La présente stratégie couvre la période 2020-2025 et se concentre sur le renforcement des moyens et des capacités en vue de la mise en place d'un environnement de sécurité à l'épreuve du temps. Elle présente une approche de la sécurité qui englobe l'ensemble de la société et qui permet de réagir efficacement et de manière coordonnée à des menaces évoluant rapidement. Elle définit des priorités stratégiques et les mesures correspondantes

---

[3] Une Union de l'égalité: stratégie en faveur de l'égalité entre les hommes et les femmes 2020-2025, COM(2020) 152.

[4] Par exemple, les travaux de la commission TERR du Parlement européen, qui a rendu son rapport en novembre 2018.

[5] Des conclusions du Conseil de juin 2015 sur une «stratégie de sécurité intérieure renouvelée» aux résultats plus récents du Conseil de décembre 2019.

[6] «Mise en œuvre du programme européen en matière de sécurité pour lutter contre le terrorisme et ouvrir la voie à une union de la sécurité réelle et effective», COM(2016) 230 final du 20.4.2016. Voir l'évaluation récente de la mise en œuvre de la législation dans le domaine de la sécurité intérieure: *Implementation of Home Affairs legislation in the field of internal security - 2017-2020* [SWD(2020) 135].

pour faire face aux risques numériques et physiques de façon intégrée dans l'ensemble de l'écosystème de l'union de la sécurité, en se concentrant sur les domaines dans lesquels l'UE peut apporter une valeur ajoutée. Son objectif est de parvenir à des résultats concrets sur le plan de la sécurité pour protéger tous les citoyens de l'UE.

II. Des menaces pour la sécurité qui évoluent rapidement en Europe

Aux fins de la sécurité, de la prospérité et du bien-être des citoyens, il est essentiel que ceux-ci soient à l'abri du danger. Les menaces qui pèsent sur leur sécurité dépendent du degré de vulnérabilité de leur existence et de leurs moyens de subsistance. Plus leur vulnérabilité est grande, plus le risque que celle-ci puisse être exploitée est élevé. Les vulnérabilités et les menaces sont en constante évolution, et l'UE doit s'adapter.

Notre vie quotidienne dépend de toute une série de services, dans les domaines de l'énergie, des transports, de la finance et de la santé, par exemple. Ces services s'appuient sur des infrastructures tant physiques que numériques, ce qui accroît leur vulnérabilité et les possibilités de les perturber. Pendant la pandémie de COVID-19, les nouvelles technologies ont permis à bon nombre d'entreprises et de services publics de continuer à fonctionner, que ce soit en nous donnant les moyens de rester connectés dans le cadre du télétravail ou en maintenant la logistique des chaînes d'approvisionnement. Cependant, elles ont aussi ouvert la porte à une augmentation extraordinaire des attaques malveillantes, leurs auteurs tentant de tirer parti à des fins criminelles des perturbations liées à la pandémie et du passage au travail à domicile à l'aide des technologiques numériques[7]. Les pénuries de marchandises ont offert de nouvelles occasions à la criminalité organisée. Les conséquences auraient pu être fatales, perturbant les services de santé essentiels alors qu'ils étaient soumis à une pression plus intense que jamais.

La multiplication incessante des utilisations des technologies numériques qui nous sont utiles au quotidien a également fait de la **cybersécurité** de ces technologies une question d'importance stratégique[8]. Les foyers, les banques, les services financiers et les entreprises (notamment les petites et moyennes entreprises) sont fortement touchés par les cyberattaques. Les dégâts potentiels sont d'autant plus grands que les systèmes physiques et numériques sont interdépendants: toute conséquence physique aura nécessairement une incidence sur les systèmes numériques, tandis que les cyberattaques visant les systèmes d'information et les infrastructures numériques peuvent entraîner l'arrêt de services essentiels[9]. L'essor de l'internet des objets et le recours accru à l'intelligence artificielle apporteront de nouveaux avantages, mais comporteront aussi de nouveaux risques.

Notre monde s'appuie sur des infrastructures et des technologies numériques et sur des systèmes en ligne, qui nous permettent de créer des activités économiques, de consommer

---

[7] Europol: *Beyond the pandemic. How COVID-19 will shape the serious and organised crime landscape in the EU* (avril 2020).

[8] Recommandation de la Commission intitulée «Cybersécurité des réseaux 5G», C(2019) 2335; 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.

[9] En mars 2020, l'hôpital universitaire de Brno, en Tchéquie, a subi une cyberattaque qui l'a contraint à réorienter des patients et à reporter des opérations chirurgicales (Europol: *Pandemic Profiteering. How criminals exploit the COVID-19 crisis*). L'intelligence artificielle peut être utilisée de manière abusive pour mener des attaques numériques, politiques et physiques, ainsi qu'à des fins de surveillance. Les données collectées dans le cadre de l'internet des objets peuvent être utilisées pour surveiller des personnes (montres intelligentes, assistants virtuels, etc.).

des produits et de bénéficier de services. Ces infrastructures, technologies et systèmes reposent tous sur la communication et l'interaction. La dépendance à l'égard des systèmes en ligne a ouvert la porte à une vague de **cybercriminalité**[10]. La «cybercriminalité à la demande» et l'économie cybercriminelle souterraine permettent d'accéder facilement, en ligne, à des produits et à des services relevant de la cybercriminalité. Les criminels s'adaptent rapidement de manière à utiliser les nouvelles technologies à leurs propres fins. Par exemple, des médicaments contrefaits et falsifiés se sont infiltrés dans la chaîne d'approvisionnement légale en produits pharmaceutiques[11]. La croissance exponentielle du matériel pédopornographique en ligne[12] montre les conséquences sociales de l'évolution de la criminalité. Une enquête récente a révélé que la plupart des citoyens de l'UE (55 %) étaient préoccupés par le fait que des criminels et des fraudeurs puissent accéder à leurs données[13].

Le **contexte mondial** aggrave aussi ces menaces. Les politiques industrielles offensives de certains pays tiers, associées aux vols incessants de propriété intellectuelle facilités par l'internet, sont en train de modifier le paradigme stratégique de la protection et de la promotion des intérêts européens. Cette situation est accentuée par la multiplication des applications à double usage, la robustesse du secteur technologique civil devenant un solide atout sur le plan des capacités de défense et de sécurité. L'espionnage industriel a une incidence considérable sur l'économie, l'emploi et la croissance dans l'UE: selon les estimations, le vol électronique de secrets d'affaires coûte 60 milliards d'EUR à l'UE[14]. Il est donc nécessaire de mener une réflexion approfondie sur la manière dont les dépendances et l'exposition accrue aux cybermenaces affectent la capacité de l'UE à protéger les citoyens et les entreprises.

La crise liée à la COVID-19 a également montré que les fractures et les incertitudes sociales engendraient une vulnérabilité sur le plan de la sécurité. Elles ouvrent une porte plus grande à des **attaques** plus sophistiquées et **hybrides** menées par des acteurs étatiques et non étatiques, les vulnérabilités étant exploitées au moyen d'une combinaison de cyberattaques, de dommages causés aux infrastructures critiques[15], de campagnes de désinformation et d'actions de radicalisation du discours politique[16].

Dans le même temps, les menaces plus anciennes continuent d'évoluer. On a constaté une baisse des **attentats terroristes** dans l'UE en 2019. Toutefois, les citoyens de l'UE restent exposés à une menace élevée d'attaques djihadistes perpétrées ou inspirées par Daech, Al-

---

[10] D'après certaines projections, les coûts des violations de données atteindront 5 000 milliards d'USD par an d'ici à 2024, alors qu'ils étaient de 3 000 milliards d'USD en 2015 (Juniper Research, *The Future of Cybercrime & Security*).

[11] Selon une étude réalisée en 2016 (par Legiscript), dans le monde, seulement 4 % des pharmacies en ligne opèrent de manière légale, les consommateurs de l'UE étant les principales cibles des 30 000 à 35 000 pharmacies illégales actives en ligne.

[12] Stratégie de l'UE en faveur d'une lutte plus efficace contre les abus sexuels commis contre des enfants, COM(2020) 607.

[13] Agence des droits fondamentaux de l'Union européenne (2020), *Your rights matter: Security concerns and experiences, Fundamental Rights Survey*, Luxembourg, Office des publications.

[14] *The scale and impact of industrial espionage and theft of trade secrets through cyber*, 2018.

[15] Les infrastructures critiques sont indispensables au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social, et leur arrêt ou leur destruction aurait un impact significatif (directive 2008/114/CE du Conseil).

[16] 97 % des citoyens de l'UE ont déjà été confrontés à de fausses informations, et 38 % le sont quotidiennement. Voir JOIN(2020) 8 final.

Qaida ou les groupes qui leur sont affiliés[17]. Parallèlement, la menace que représente l'extrémisme de droite violent croît également[18]. Les attaques à caractère raciste doivent susciter de vives inquiétudes: les attentats terroristes antisémites mortels commis à Halle ont rappelé la nécessité d'intensifier la réaction conformément à la déclaration du Conseil de 2018[19]. Un citoyen de l'UE sur cinq se dit très préoccupé à l'idée qu'un attentat terroriste puisse être commis au cours des 12 prochains mois[20]. La grande majorité des attentats terroristes perpétrés récemment reposaient peu sur les technologies et étaient le fait d'acteurs isolés ciblant des personnes dans des espaces publics, tandis que la propagande terroriste en ligne a pris une importance nouvelle avec la diffusion en direct des attentats de Christchurch[21]. La menace que représentent les individus radicalisés reste élevée et est potentiellement renforcée par le retour de combattants terroristes étrangers et par la libération d'extrémistes qui étaient incarcérés[22].

La crise a également montré que les menaces existantes pouvaient évoluer avec les circonstances. Des **groupes criminels organisés** ont profité des pénuries de marchandises pour créer de nouveaux marchés illégaux. Le trafic de stupéfiants continue de représenter le plus grand marché criminel dans l'UE, la valeur des ventes au détail de drogues illicites y étant estimée à au moins 30 milliards d'EUR par an[23]. La traite des êtres humains reste d'actualité: selon les estimations, le bénéfice mondial annuel tiré de toutes les formes d'exploitation s'élève à près de 30 milliards d'EUR[24]. Le commerce international de produits pharmaceutiques contrefaits a atteint 38,9 milliards d'EUR[25]. Dans le même temps, les faibles taux de confiscation permettent aux criminels de continuer à développer leurs activités criminelles et d'infiltrer l'économie légale[26]. Le marché en ligne et les nouvelles technologies telles que l'impression en 3D facilitent l'accès des criminels et des terroristes aux armes à feu[27]. L'utilisation de l'intelligence artificielle, des nouvelles technologies et de la robotique augmentera encore le risque que des criminels se servent des avantages de l'innovation à des fins malveillantes[28].

---

17 Au total, 119 attentats terroristes perpétrés, avortés ou déjoués ont été signalés par 13 États membres de l'UE, causant dix morts et 27 blessés (Europol, *European Union Terrorism Situation and Trend Report*, 2020).

18 En 2019, six attentats terroristes de droite (un perpétré, un avorté et quatre déjoués) ont été signalés (par trois États membres), contre un seul en 2018, et d'autres décès ont été causés dans des affaires qui n'ont pas été qualifiées de terroristes (Europol, 2020).

19 Voir également la déclaration du Conseil sur la lutte contre l'antisémitisme et la mise en place d'une approche commune en matière de sécurité afin de mieux protéger les communautés et institutions juives en Europe.

20 Agence des droits fondamentaux de l'Union européenne: *Your rights matter: Security concerns and experiences*, 2020.

21 Entre juillet 2015 et la fin de l'année 2019, Europol a trouvé des contenus à caractère terroriste sur 361 plateformes (Europol, 2020).

22 Europol: *A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism*, 2019.

23 OEDT et Europol, *EU Drug Markets Report*, 2019.

24 Rapport d'Europol, *The Trafficking in Human Beings Financial Business Model* (2015).

25 Rapport de l'Office de l'Union européenne pour la propriété intellectuelle et de l'OCDE sur le commerce de produits pharmaceutiques contrefaits.

26 Rapport intitulé «Recouvrement et confiscation d'avoirs: Garantir que le crime ne paie pas», COM(2020) 217.

27 En 2017, des armes à feu ont été utilisées dans 41 % des attentats terroristes (Europol, 2018).

28 En juillet 2020, les autorités policières et judiciaires françaises et néerlandaises, aux côtés d'Europol et d'Eurojust, ont présenté l'enquête conjointe visant à démanteler EncroChat, un réseau téléphonique crypté utilisé par des réseaux criminels impliqués dans des attaques violentes, des actes de corruption, des tentatives d'assassinats et le transport de stupéfiants à grande échelle.

Ces menaces transcendent les catégories et touchent différentes parties de la société de différentes manières. Elles représentent toutes un danger majeur pour les citoyens et les entreprises et nécessitent une réaction globale et cohérente au niveau de l'UE. À l'heure où les vulnérabilités en matière de sécurité peuvent même venir de petits articles ménagers interconnectés, tels qu'un réfrigérateur ou une machine à café connectés à l'internet, nous ne pouvons plus compter sur les seuls acteurs étatiques traditionnels pour garantir notre sécurité. Les opérateurs économiques doivent assumer une plus grande responsabilité en ce qui concerne la cybersécurité des produits et des services qu'ils mettent sur le marché, tandis que les citoyens doivent eux aussi posséder au moins des notions de base en matière de cybersécurité pour être en mesure de se protéger.

III. Une réaction coordonnée de l'UE englobant l'ensemble de la société

L'UE a déjà montré qu'elle pouvait apporter une réelle valeur ajoutée. Depuis 2015, l'union de la sécurité a créé de nouveaux liens dans la manière dont les politiques de sécurité sont abordées au niveau de l'UE. Toutefois, davantage d'efforts sont nécessaires pour mobiliser l'ensemble de la société, y compris les pouvoirs publics à tous les niveaux, les entreprises de tous les secteurs et les citoyens de tous les États membres. La prise de conscience croissante des risques liés à la dépendance[29] et la nécessité d'une stratégie industrielle européenne solide[30] plaident en faveur d'une Union européenne dotée d'une masse critique de production industrielle et technologique et d'une chaîne d'approvisionnement résiliente. La force passe aussi par le plein respect des droits fondamentaux et des valeurs de l'UE, qui est indispensable pour que les politiques de sécurité soient légitimes, efficaces et durables. La présente stratégie pour l'union de la sécurité définit des axes de travail concrets à suivre. Elle s'articule autour des objectifs communs suivants:

- ***renforcer les moyens et les capacités de détection rapide, de prévention et de réaction rapide aux crises:*** l'Europe doit être plus résiliente pour prévenir les chocs futurs, se protéger contre ces chocs et y résister. Nous devons renforcer nos moyens et nos capacités de détection rapide et de réaction rapide aux crises qui menacent la sécurité, à l'aide d'une approche intégrée et coordonnée, à la fois sur le plan global et par des initiatives sectorielles (pour les secteurs de la finance, de l'énergie, de la justice, des services répressifs, des soins de santé, de la sûreté maritime et des transports, par exemple) et en nous appuyant sur les outils et les initiatives existants[31]. La Commission présentera aussi des propositions relatives à un vaste système de gestion des crises au sein de l'UE, qui pourrait également être utile dans le domaine de la sécurité;
- ***mettre l'accent sur les résultats:*** une stratégie axée sur les résultats doit reposer sur une évaluation minutieuse des menaces et des risques afin que les efforts puissent être ciblés au mieux. Elle doit définir et utiliser les règles et les outils adéquats. Elle doit faire en

[29] La dépendance à l'égard de pays tiers entraîne des risques qui découlent d'une exposition accrue aux menaces potentielles, allant de l'exploitation des vulnérabilités des infrastructures informatiques pour compromettre des infrastructures critiques (dans les domaines de l'énergie, des transports, de la banque ou de la santé, par exemple) à la prise du contrôle de systèmes de commande industriels, en passant par des possibilités élargies de vol de données ou d'espionnage.

[30] Communication de la Commission intitulée «Une nouvelle stratégie industrielle pour l'Europe», COM(2020) 102.

[31] Tels que le dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR), le Centre de coordination de la réaction d'urgence, la recommandation de la Commission sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs [C(2017) 6100] et le protocole opérationnel de l'UE de lutte contre les menaces hybrides («EU Playbook») [SWD(2016) 227].

sorte que les politiques de l'UE en matière de sécurité s'appuient sur des renseignements stratégiques fiables. Lorsque l'UE doit légiférer, il y a lieu que les actes adoptés fassent l'objet d'un suivi, pour veiller à ce qu'ils soient pleinement mis en œuvre, prévenir toute fragmentation et éviter la présence de lacunes susceptibles d'être exploitées. La mise en œuvre effective de la présente stratégie dépendra aussi de l'obtention d'un financement approprié au cours de la prochaine période de programmation (2021-2027), y compris pour les agences de l'UE concernées;

- ***associer l'ensemble des acteurs des secteurs public et privé à un effort commun:*** des acteurs clés des secteurs public et privé sont réticents lorsqu'il s'agit de partager des informations utiles pour la sécurité, par crainte de compromettre la sécurité nationale ou leur compétitivité[32]. Toutefois, nous sommes plus efficaces lorsque nous sommes tous équipés pour nous soutenir les uns les autres. Cela commence par une coopération plus intense entre les États membres, faisant intervenir les services répressifs et judiciaires et d'autres autorités publiques, ainsi qu'avec les institutions et agences de l'UE, afin de parvenir à la compréhension et à l'échange nécessaires à des solutions communes. La coopération avec le secteur privé est également essentielle, d'autant plus que l'industrie possède une part importante de l'infrastructure numérique et non numérique cruciale pour lutter efficacement contre la criminalité et le terrorisme. Les citoyens eux-mêmes peuvent aussi apporter leur contribution, par exemple en développant leurs compétences et leurs connaissances pour lutter contre la cybercriminalité ou la désinformation. Enfin, cet effort commun doit s'étendre au-delà de nos frontières, l'idée étant de nouer des liens plus étroits avec des partenaires partageant nos valeurs.

IV. Protéger chacun dans l'UE: priorités stratégiques pour l'union de la sécurité

L'UE est particulièrement bien placée pour réagir à ces nouvelles menaces et relever ces nouveaux défis à l'échelle mondiale. L'analyse des menaces effectuée ci-dessus fait apparaître quatre priorités stratégiques interdépendantes pour lesquelles il convient de réaliser des avancées au niveau de l'UE, dans le plein respect des droits fondamentaux: i) un environnement de sécurité à l'épreuve du temps, ii) faire face à l'évolution des menaces, iii) protéger les Européens contre le terrorisme et la criminalité organisée, iv) un solide écosystème européen de la sécurité.

1. Un environnement de sécurité à l'épreuve du temps

Protection et résilience des infrastructures critiques

Les citoyens utilisent des infrastructures clés au quotidien, que ce soit pour voyager, pour travailler, pour bénéficier de services publics essentiels (hôpitaux, transports, approvisionnement énergétique, etc.) ou pour exercer leurs droits démocratiques. Si ces infrastructures ne sont pas suffisamment protégées et résilientes, des attaques peuvent causer d'énormes perturbations, tant physiques que numériques, dans des États membres individuels et, potentiellement, dans l'ensemble de l'UE.

Le cadre existant de l'UE en matière de protection et de résilience des infrastructures critiques[33] n'a pas suivi le rythme de l'évolution des risques. En raison des interdépendances

[32] Communication conjointe intitulée «Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide», JOIN(2017) 450.

[33] Directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, JO L 194 du 19.7.2016; directive 2008/114/CE du

croissantes, les perturbations touchant un secteur peuvent avoir une incidence immédiate sur le fonctionnement d'autres secteurs: une attaque visant la production d'électricité pourrait provoquer l'arrêt des télécommunications, des hôpitaux, des banques ou des aéroports, tandis qu'une attaque contre des infrastructures numériques pourrait entraîner des perturbations dans les réseaux d'électricité ou le secteur financier. À mesure que l'internet joue un rôle de plus en plus important dans notre économie et notre société, les risques de ce type s'aggravent. Le cadre législatif doit tenir compte de cette interconnexion et de cette interdépendance accrues, en prévoyant des mesures solides de protection et de résilience des infrastructures critiques, sur les plans tant numérique que physique. Les services essentiels, y compris ceux qui reposent sur des infrastructures spatiales, doivent être protégés de manière adéquate contre les menaces actuelles et anticipées, mais aussi être résilients. À cet effet, les systèmes doivent être capables de se préparer aux événements indésirables, de planifier leur réaction à ces derniers, d'y résister, de s'en relever et de mieux s'y adapter.

Dans le même temps, les États membres ont exercé leur pouvoir d'appréciation en mettant en œuvre la législation existante de différentes manières. La fragmentation qui en résulte peut nuire au marché intérieur et rendre la coordination transfrontière plus difficile, les difficultés étant les plus manifestes dans les régions frontalières. Les opérateurs fournissant des services essentiels dans différents États membres doivent se conformer à différents régimes d'information. La Commission examine si de **nouveaux cadres relatifs aux infrastructures tant physiques que numériques** pourraient apporter une plus grande cohérence et conduire à une approche plus homogène quant à la manière d'assurer la fiabilité de la fourniture des services essentiels. Ces cadres devraient s'accompagner d'**initiatives sectorielles** visant à s'attaquer aux risques spécifiques auxquels sont confrontées les infrastructures critiques, dans les domaines des transports, de l'espace, de l'énergie, de la finance et de la santé[34], par exemple. Compte tenu de la forte dépendance du secteur financier à l'égard des services informatiques et de sa grande vulnérabilité aux cyberattaques, une première initiative portera sur la résilience opérationnelle numérique de ce secteur. En raison de la sensibilité et du poids particuliers du système énergétique, une initiative spécifique tendra à renforcer la résilience des infrastructures énergétiques critiques face aux menaces physiques, numériques et hybrides, en garantissant des conditions égales aux opérateurs du secteur de l'énergie par-delà les frontières.

Les effets sur la sécurité des investissements directs étrangers (IDE) susceptibles d'affecter des infrastructures ou des technologies critiques seront également soumis aux évaluations effectuées par les États membres de l'UE et la Commission au titre du nouveau cadre européen pour le filtrage des investissements directs étrangers[35].

Conseil concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection.

[34] Compte tenu du fait que le secteur de la santé a été mis à rude épreuve, en particulier pendant la crise liée à la COVID-19, la Commission envisagera également des initiatives visant à renforcer le cadre de sécurité sanitaire de l'UE et les agences de l'UE compétentes en la matière pour faire face aux menaces transfrontières graves pesant sur la santé.

[35] Lorsqu'il entrera pleinement en application le 11 octobre 2020, le règlement (UE) 2019/452 du Parlement européen et du Conseil du 19 mars 2019 établissant un cadre pour le filtrage des investissements directs étrangers dans l'Union dotera l'UE d'un nouveau dispositif de coopération concernant les investissements directs en provenance de l'extérieur de l'UE susceptibles d'affecter la sécurité ou l'ordre public. Conformément au règlement, les États membres et la Commission évalueront les risques potentiels liés à ces IDE et, s'il y a lieu et si les risques en question concernent plus d'un État membre, ils proposeront des moyens adéquats de les atténuer.

L'UE peut également élaborer de nouveaux outils pour soutenir la résilience des infrastructures critiques. L'internet mondial a jusqu'à présent fait montre d'un niveau élevé de résilience, en particulier pour ce qui est de sa capacité à supporter l'augmentation des volumes de trafic. Toutefois, nous devons nous préparer à d'éventuelles crises futures qui menaceront la sécurité, la stabilité et la résilience de l'internet. Pour faire en sorte que l'internet continue de fonctionner, il convient d'assurer sa solidité face aux incidents de cybersécurité et aux activités malveillantes en ligne et de limiter sa dépendance à l'égard d'infrastructures et de services situés en dehors de l'Europe. À cette fin, il faudra à la fois légiférer, en revoyant les règles existantes afin de garantir un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'UE, investir davantage dans la recherche et l'innovation et envisager le déploiement ou le renforcement d'infrastructures et de ressources fondamentales pour l'internet, notamment le système de noms de domaines[36].

Pour protéger les actifs numériques clés de l'UE et des États membres, il est primordial d'offrir aux infrastructures critiques un canal de communication sécurisé. La Commission travaille avec les États membres à la mise en place d'une infrastructure quantique de bout en bout sécurisée et certifiée, terrestre et spatiale, en combinaison avec le système de télécommunications gouvernementales par satellite sécurisées prévu dans le règlement relatif au programme spatial[37].

Cybersécurité

Le nombre de cyberattaques continue d'augmenter[38]. Ces attaques sont plus sophistiquées que jamais, proviennent de sources très diverses à l'intérieur et à l'extérieur de l'UE et ciblent des domaines dont la vulnérabilité est maximale. Des acteurs étatiques ou soutenus par un État sont souvent impliqués et visent des infrastructures numériques essentielles, comme les principaux fournisseurs de services en nuage[39]. Les cyber-risques sont également devenus une menace importante pour le système financier. Le Fonds monétaire international a estimé la perte annuelle due aux cyberattaques à 9 % du revenu net des banques dans le monde, soit environ 100 milliards de dollars[40]. Alors que le passage à des appareils connectés aura de nombreux avantages pour les utilisateurs, moins de données seront stockées et traitées dans les centres de données et plus de données seront traitées plus près de l'utilisateur, «à la périphérie»[41], si bien que la cybersécurité ne pourra plus se concentrer sur la protection des points centraux[42].

---

[36] Un système de noms de domaines (DNS) est un système de nommage hiérarchique et décentralisé pour les ordinateurs, les services ou d'autres ressources connectés à l'internet ou à un réseau privé. Il traduit les noms de domaines en adresses IP nécessaires pour localiser et identifier les services et les appareils informatiques.

[37] Proposition de règlement établissant le programme spatial de l'Union et l'Agence de l'Union européenne pour le programme spatial, COM(2018) 447.

[38] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[39] Les attaques par déni de service distribué continuent de représenter une menace permanente: de grands fournisseurs ont dû atténuer les effets d'attaques massives de ce type, par exemple une attaque contre les services web d'Amazon en février 2020.

[40] https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/.

[41] Le traitement des données à la périphérie est une architecture informatique ouverte et distribuée, caractérisée par une puissance de traitement décentralisé facilitant l'informatique mobile et l'internet des objets (IdO). Dans le traitement à la périphérie, les données sont traitées par l'appareil lui-même ou par un ordinateur ou serveur local, au lieu d'être transmises à un centre de données.

[42] Communication intitulée «Une stratégie européenne pour les données», COM(2020) 66 final.

En 2017, l'UE a présenté une approche de la cybersécurité fondée sur le développement de la résilience, une réaction rapide et une dissuasion efficace[43]. L'UE doit maintenant faire en sorte que ses capacités en matière de cybersécurité restent en phase avec la réalité, pour assurer tant la résilience que la réaction. Cela nécessite une approche associant véritablement toutes les composantes de la société et selon laquelle les institutions, organes et organismes de l'UE, les États membres, les entreprises, les milieux universitaires et les particuliers accordent la priorité à la cybersécurité[44]. Cette approche horizontale doit également être complétée par des approches sectorielles de la cybersécurité dans des domaines tels que l'énergie, les services financiers, les transports ou la santé. Les travaux réalisés par l'UE au cours de la prochaine phase devraient être rassemblés dans une stratégie européenne de cybersécurité révisée.

L'exploration de formes nouvelles et améliorées de coopération entre les services de renseignement, le Centre de situation et du renseignement de l'UE (INTCEN) et d'autres organisations s'occupant de sécurité devrait faire partie des efforts visant à renforcer la cybersécurité, ainsi que la lutte contre le terrorisme, l'extrémisme, le radicalisme et les menaces hybrides.

Compte tenu du déploiement en cours des **infrastructures liées à la 5G** dans l'ensemble de l'UE et de la dépendance potentielle de nombreux services critiques à l'égard des réseaux 5G, les conséquences de perturbations systémiques et généralisées seraient particulièrement graves. Le processus mis en place par la recommandation de la Commission de 2019 sur la cybersécurité des réseaux 5G[45] a conduit les États membres à mener des actions spécifiques en ce qui concerne les mesures essentielles définies dans une «boîte à outils» relative à la 5G[46].

L'un des principaux besoins à long terme est de développer une culture de la **cybersécurité dès la conception**, la sécurité étant intégrée aux produits et services dès le départ. Le nouveau cadre de certification de cybersécurité, prévu par le règlement sur la cybersécurité, constituera une contribution importante à cet égard[47]. Le cadre existe déjà, puisque deux schémas de certification sont en préparation et que les priorités d'autres schémas doivent être définies dans le courant de l'année. La coopération entre l'Agence de l'Union européenne pour la cybersécurité (ENISA), les autorités chargées de la protection des données et le comité européen de la protection des données[48] revêt une importance capitale dans ce domaine.

La Commission a déjà mis en évidence la nécessité de mettre sur pied une **unité conjointe de cybersécurité**, afin d'assurer une coopération opérationnelle structurée et coordonnée, qui pourrait comprendre un mécanisme d'assistance mutuelle en temps de crise au niveau de l'UE. Dans le prolongement de la mise en œuvre de la recommandation relative au plan

---

43 Communication conjointe intitulée «Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide», JOIN(2017) 450 final.

44 Le rapport du Centre commun de recherche intitulé «Cybersecurity – our digital Anchor» donne un aperçu multidimensionnel de la croissance de la cybersécurité au cours des 40 dernières années.

45 Recommandation de la Commission sur la cybersécurité des réseaux 5G, COM(2019) 2335 final. La recommandation prévoit qu'elle doit être réexaminée au cours du dernier trimestre de 2020.

46 Voir le rapport du 24 juillet 2020 du groupe de coopération SRI sur la mise en œuvre de la boîte à outils.

47 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 de cybersécurité des technologies de l'information et des communications (règlement sur la cybersécurité).

48 Communication intitulée «La protection des données: un pilier de l'autonomisation des citoyens et de l'approche de l'Union à l'égard de la transition numérique – deux années d'application du règlement général sur la protection des données», COM(2020) 264.

d'action[49], l'unité conjointe de cybersécurité pourrait renforcer la confiance entre les différents acteurs de l'écosystème européen de cybersécurité et offrir un service essentiel aux États membres. La Commission lancera des discussions avec les parties prenantes concernées (en commençant par les États membres) et définira un processus clair, des étapes et un calendrier avant la fin de l'année 2020.

Il importe également d'établir des règles communes en matière de sécurité de l'information et de cybersécurité pour l'ensemble des institutions, organes et organismes de l'UE. L'objectif devrait être de créer des normes communes élevées et obligatoires en vue de l'échange sécurisé d'informations et de la sécurité des infrastructures et systèmes numériques dans l'ensemble des institutions, organes et organismes de l'UE. Ce nouveau cadre devrait appuyer une coopération opérationnelle poussée et efficiente en matière de cybersécurité dans l'ensemble des institutions, organes et organismes de l'UE, centrée sur le rôle que joue auprès d'eux l'équipe d'intervention en cas d'urgence informatique (CERT-UE).

Compte tenu de la nature mondiale des cyberattaques, il est essentiel de mettre en place et de préserver des **partenariats internationaux** solides pour continuer à les prévenir, à les décourager et à y réagir. Le cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance («boîte à outils cyberdiplomatique»)[50] définit des mesures au titre de la politique étrangère et de sécurité commune, y compris des mesures restrictives (sanctions), qui peuvent être utilisées contre des activités qui portent atteinte aux intérêts politiques, économiques et de sécurité de l'UE. L'Union devrait également intensifier les actions qu'elle mène au moyen de fonds destinés au développement et à la coopération afin de permettre aux États partenaires de renforcer leurs capacités et de les aider à améliorer leurs écosystèmes numériques, à adopter des réformes législatives nationales et à respecter les normes internationales. Cela accroît la résilience globale et la capacité de tous à faire face et à réagir efficacement aux cybermenaces. Il s'agit notamment d'actions spécifiques visant à promouvoir les normes de l'UE et la législation pertinente en vue d'accroître la cybersécurité des pays partenaires du voisinage européen[51].

Protéger les espaces publics

Les récents attentats terroristes visaient des **espaces publics**, y compris des lieux de culte et des plateformes de transport, en exploitant leur nature ouverte et accessible. La montée du terrorisme provoquée par l'extrémisme politique ou idéologique a rendu cette menace encore plus aiguë. Elle impose à la fois le renforcement de la protection matérielle de ces lieux et des systèmes de détection adéquats, sans qu'il soit porté atteinte aux libertés des citoyens[52]. La Commission favorisera la coopération entre les secteurs public et privé en matière de protection des espaces publics par le financement, l'échange d'expériences et de bonnes pratiques, des orientations spécifiques[53] et des recommandations[54]. La

[49] Recommandation (UE) 2017/1584 de la Commission sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs.

[50] http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/fr/pdf

[51] Voir les lignes de conduite de l'UE concernant le renforcement des cybercapacités externes de l'UE, adoptées dans les conclusions du Conseil du 26 juin 2018.

[52] Les systèmes d'identification biométrique à distance méritent un examen spécifique. La position initiale de la Commission est exposée dans son livre blanc du 19 février 2020 sur l'intelligence artificielle, COM(2020) 65.

[53] Voir, par exemple, le document d'orientation sur le choix de solutions appropriées en matière de barrières de sécurité aux fins de la protection de l'espace public (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120307/hvm_v3.pdf).

sensibilisation, l'établissement d'exigences de performance et la réalisation d'essais pour les équipements de détection ainsi que l'amélioration de la vérification des antécédents pour faire face aux menaces intérieures feront également partie de l'approche. Il importe de tenir compte du fait que les minorités et les personnes vulnérables peuvent être touchées de manière disproportionnée, notamment lorsque les personnes sont visées en raison de leur religion ou de leur sexe, et qu'elles nécessitent donc une attention particulière. Les pouvoirs publics régionaux et locaux ont un rôle important à jouer pour améliorer la sécurité des espaces publics. La Commission contribue également à favoriser l'innovation dans les villes en ce qui concerne la sécurité dans les espaces publics[55]. Le lancement, en novembre 2018, d'un nouveau partenariat en matière de «sécurité dans les espaces publics» dans le cadre du programme urbain[56] reflète la ferme détermination des États membres, de la Commission et des villes à mieux faire face aux menaces qui pèsent sur la sécurité dans l'espace urbain.

Le marché des **drones** continue à se développer, le recours à ceux-ci étant souvent très utile et légitime. Toutefois, ils peuvent également être utilisés abusivement par des criminels et des terroristes, les espaces publics étant exposés à une menace particulière. Les cibles peuvent être des personnes, des rassemblements de personnes, des infrastructures critiques, des autorités répressives, des frontières ou des espaces publics. Le savoir acquis en ce qui concerne l'utilisation des drones dans les conflits pourrait revenir en Europe, soit directement (via les combattants terroristes étrangers de retour), soit en ligne. Les règles déjà élaborées par l'Agence européenne de la sécurité aérienne constituent une première étape importante dans des domaines tels que l'enregistrement des utilisateurs de drones et l'identification à distance obligatoire des drones. Les drones devenant de plus en plus largement disponibles, abordables et performants, il est nécessaire de prendre des mesures supplémentaires. Il pourrait notamment s'agir de partage d'informations, d'orientations et de bonnes pratiques à l'usage de tous, y compris en matière répressive, ainsi que d'une expérimentation plus large de mesures visant à lutter contre les drones[57]. En outre, les implications de l'utilisation de drones dans les espaces publics pour la protection de la vie privée et des données devraient faire l'objet d'une analyse et d'une action plus poussées.

Actions clés
• Législation sur la protection et la résilience des infrastructures critiques • Révision de la directive sur les réseaux et les systèmes d'information • Une initiative sur la résilience opérationnelle du système financier. • Protection et cybersécurité des infrastructures énergétiques critiques et code de réseau sur la cybersécurité pour les flux transfrontaliers d'électricité • Une stratégie européenne de cybersécurité

[54] Le document SWD(2019) 140 donne des indications sur les bonnes pratiques, notamment dans une section consacrée à la coopération entre les secteurs public et privé. Le financement au titre du FSI-Police est en particulier axé sur le renforcement de la coopération entre les secteurs public et privé.

[55] Trois villes (le Pirée en Grèce, Tampere en Finlande et Turin en Italie) expérimenteront de nouvelles solutions dans le cadre des actions innovatrices urbaines, cofinancées par le Fonds européen de développement régional (FEDER).

[56] Le programme urbain de l'UE représente une nouvelle méthode de travail à plusieurs niveaux qui encourage la coopération entre les États membres, les villes, la Commission européenne et d'autres parties prenantes afin de stimuler la croissance, la qualité de vie et l'innovation dans les villes d'Europe, et de recenser et relever avec succès les défis sociaux.

[57] Un programme d'expérimentation pluriannuel destiné à aider les États membres à mettre au point une méthodologie et une plateforme d'expérimentation communes dans ce domaine a été récemment mis en place.

- Prochaines étapes en vue de la création d'une unité conjointe de cybersécurité
- Des règles communes en matière de sécurité de l'information et de cybersécurité pour les institutions, organes et organismes de l'UE
- Renforcement de la coopération en vue de la protection des espaces publics, y compris les lieux de culte
- Mise en commun des bonnes pratiques en matière de lutte contre l'utilisation abusive des drones

2. Faire face à l'évolution des menaces

Cybercriminalité

Si la technologie offre de nouvelles opportunités à la société ainsi que de nouveaux outils aux juges et aux services répressifs, elle ouvre aussi des perspectives aux criminels. Les logiciels malveillants, les vols de données à caractère personnel ou commercial par piratage et l'interruption d'activité numérique, source de préjudice financier ou d'atteinte à la réputation, sont tous en hausse. Le premier moyen de défense consiste à créer un environnement résilient grâce à une cybersécurité solide. Les autorités répressives doivent pouvoir mener des activités dans le domaine des enquêtes numériques en disposant de règles claires pour enquêter sur les infractions et les poursuivre et offrir la protection nécessaire aux victimes. Ces activités devraient s'appuyer sur la force d'action anticybercriminalité européenne d'Europol et sur le protocole de réaction d'urgence des services répressifs, créé pour coordonner la réaction aux cyberattaques de grande envergure. Des mécanismes efficaces permettant d'établir des partenariats et une coopération entre les secteurs public et privé sont également essentiels.

Parallèlement, la lutte contre la cybercriminalité devrait devenir une priorité stratégique en matière de communication dans toute l'UE, afin d'alerter les Européens sur les risques et les mesures de prévention qu'ils pourraient prendre. Cela devrait s'inscrire dans le cadre d'une approche proactive. La mise en œuvre intégrale du cadre juridique actuel[58] constitue aussi une étape essentielle: la Commission sera prête à recourir aux procédures d'infraction, le cas échéant, tout en continuant à réexaminer ce cadre afin de faire en sorte qu'il reste adapté à sa finalité. La Commission étudiera également, conjointement avec Europol et l'Agence de l'Union européenne pour la cybersécurité (ENISA), la faisabilité d'un système d'alerte rapide de l'UE en matière de cybercriminalité, qui pourrait garantir la circulation de l'information et des réactions rapides en cas de poussée de la cybercriminalité.

La cybercriminalité est un défi mondial face auquel une coopération internationale efficace est nécessaire. L'UE soutient la convention de Budapest sur la cybercriminalité du Conseil de l'Europe, qui constitue un cadre utile et bien établi permettant à tous les pays de déterminer quels sont les systèmes et les canaux de communication qu'ils doivent mettre en place pour pouvoir travailler efficacement les uns avec les autres.

Près de la moitié des citoyens de l'Union s'inquiètent de l'utilisation abusive des données[59] et **l'usurpation d'identité** constitue un sujet de préoccupation majeure[60]. Si l'utilisation

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

[59] 46 % (enquête Eurobaromètre sur les attitudes des Européens à l'égard de la cybersécurité, janvier 2020).

[60] Lors de l'enquête Eurobaromètre de 2018 sur «Les attitudes des Européens à l'égard de la sécurité de l'internet», la grande majorité des personnes interrogées (95 %) considérait l'usurpation d'identité comme un crime grave, et sept personnes sur dix affirmaient qu'il s'agissait d'un crime très grave. L'enquête Eurobaromètre publiée en janvier 2020 a confirmé les préoccupations relatives à la cybercriminalité, à la

frauduleuse d'une identité à des fins lucratives en est un aspect, les conséquences personnelles et psychologiques peuvent aussi être considérables, dès lors que les messages illégaux mis en ligne par l'usurpateur d'identité peuvent y demeurer pendant des années. La Commission étudiera les mesures concrètes qui pourraient être prises pour protéger les victimes contre toutes les formes d'usurpation d'identité, compte tenu du lancement prochain de l'initiative relative à une identité numérique européenne[61].

La lutte contre la cybercriminalité suppose de se tourner vers l'avenir. Alors que la société utilise les nouvelles avancées technologiques pour renforcer l'économie et la société, les criminels peuvent également chercher à exploiter ces outils à des fins négatives. Par exemple, ils peuvent recourir à l'intelligence artificielle pour détecter et découvrir des mots de passe ou pour simplifier la création de logiciels malveillants, afin d'exploiter des images et des sons qui peuvent ensuite être utilisés à des fins d'usurpation d'identité ou de fraude.

Des services répressifs modernes

Les professionnels de la répression et de la justice doivent s'adapter aux nouvelles technologies. L'évolution technologique et les menaces émergentes exigent que les autorités répressives aient accès aux nouveaux outils, acquièrent de nouvelles compétences et élaborent de nouvelles techniques d'enquête. Pour compléter les mesures législatives visant à améliorer l'accès transfrontière aux preuves électroniques dans le cadre des enquêtes pénales, l'UE peut aider les autorités répressives à se doter de la capacité nécessaire pour repérer, obtenir et lire les données nécessaires aux enquêtes concernant des infractions et pour utiliser ces données comme éléments de preuve devant les tribunaux. La Commission étudiera des mesures visant à **renforcer les capacités répressives dans le cadre des enquêtes numériques**, en définissant les moyens de tirer le meilleur parti possible de la recherche et du développement pour créer de nouveaux outils répressifs et en précisant comment la formation peut permettre aux membres des services répressifs et aux juges de disposer du meilleur profil de compétences. Il s'agira aussi de proposer des évaluations scientifiques rigoureuses et des méthodes d'essai par l'intermédiaire du Centre commun de recherche de la Commission.

Des approches communes peuvent également garantir que **l'intelligence artificielle, les capacités spatiales, les mégadonnées** et **le calcul à haute performance sont intégrés** dans la politique de sécurité d'une manière qui soit efficace tant pour lutter contre la criminalité que pour assurer la protection des droits fondamentaux. L'intelligence artificielle pourrait constituer un outil puissant pour lutter contre la criminalité, en créant d'énormes capacités d'enquête grâce à l'analyse de grandes quantités d'informations et à la mise en évidence de modèles et d'anomalies[62]. Elle peut aussi fournir des outils concrets, notamment pour contribuer à détecter les contenus à caractère terroriste en ligne, à découvrir les transactions suspectes dans les ventes de produits dangereux ou à offrir une assistance aux citoyens en cas d'urgence. Pour réaliser ce potentiel, il convient d'adjoindre à la recherche, à l'innovation et aux utilisateurs de l'intelligence artificielle la gouvernance et les infrastructures techniques adéquates, en y faisant activement participer le secteur privé et les milieux universitaires. Cela suppose également de garantir les normes les plus strictes en matière de respect des droits fondamentaux, tout en veillant à une protection efficace des citoyens. En particulier, les décisions qui ont une incidence sur les particuliers doivent faire

---

fraude en ligne et à l'usurpation d'identité, deux tiers des personnes interrogées se déclarant préoccupées par la fraude bancaire (67 %) ou l'usurpation d'identité (66 %).

[61] Communication du 19 février 2020 intitulée «Façonner l'avenir numérique de l'Europe», COM(2020) 67.

[62] Par exemple, en matière de criminalité financière.

l'objet d'un contrôle par un être humain et être conformes au droit de l'Union pertinent qui est applicable[63].

Des informations et des preuves électroniques sont nécessaires dans environ 85 % des enquêtes relatives à des infractions graves, tandis que 65 % des demandes totales à cet effet sont adressées à des prestataires établis dans une autre juridiction[64]. Le fait que les traces matérielles traditionnelles se trouvent désormais en ligne élargit encore le fossé entre les services répressifs et les capacités des criminels. Il est essentiel de mettre en place des règles claires en matière d'accès transfrontière aux preuves électroniques dans le cadre des enquêtes pénales. C'est pourquoi 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. L'accès transfrontière aux preuves électroniques à l'issue de négociations internationales multilatérales et bilatérales est également crucial, afin d'établir des règles compatibles au niveau international[65].

L'accès aux preuves numériques dépend aussi de la disponibilité des informations. Si les données sont effacées trop rapidement, il se peut que des éléments de preuve importants disparaissent, de sorte qu'il n'est plus possible d'identifier et de localiser les suspects et les réseaux criminels (ainsi que les victimes). Par ailleurs, les régimes de conservation des données soulèvent des questions relatives à la protection de la vie privée. En fonction de l'issue des affaires pendantes devant la Cour de justice, la Commission évaluera la marche à suivre en matière de conservation des données.

L'accès aux informations concernant l'enregistrement des noms de domaine sur l'internet («données WHOIS»)[66] est important pour les enquêtes pénales, la cybersécurité et la protection des consommateurs. Toutefois, l'accès à ces informations devient de plus en plus difficile dans l'attente de l'adoption, par la Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN), d'une nouvelle politique en matière de données WHOIS. La Commission continuera à collaborer avec l'ICANN et la communauté des diverses parties prenantes pour faire en sorte que les personnes qui souhaitent y accéder légitimement, y compris les membres des services répressifs, puissent se voir accorder un accès efficient aux données WHOIS conformément aux règles internationales et de l'UE en matière de protection des données. Il s'agira en particulier d'évaluer les solutions possibles, en déterminant notamment s'il peut être nécessaire de légiférer pour clarifier les règles d'accès à ces informations.

Les autorités répressives et judiciaires devront également être à même d'obtenir les données et les éléments de preuve nécessaires une fois que l'**architecture 5G pour les télécommunications mobiles** sera pleinement déployée dans l'UE, d'une manière qui respecte la confidentialité des communications. La Commission soutiendra une approche renforcée et coordonnée lors de l'élaboration de normes internationales, en définissant les

---

[63] Cela implique le respect de la législation en vigueur, notamment le règlement (UE) 2016/679 (règlement général sur la protection des données) et la directive (UE) 2016/680 (directive en matière de protection des données dans le domaine répressif) régissant le traitement des données à caractère personnel à des fins de détection et de prévention des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales.

[64] SWD(2018) 118 final.

[65] En particulier, le deuxième protocole additionnel à la convention de Budapest sur la cybercriminalité du Conseil de l'Europe et un accord entre l'Union européenne et les États-Unis sur l'accès transfrontière aux preuves électroniques.

[66] Conservées dans des bases de données gérées par 2 500 bureaux d'enregistrement établis dans le monde entier.

meilleures pratiques, les processus et l'interopérabilité technique dans des domaines technologiques essentiels tels que l'IA, l'internet des objets ou les technologies des chaînes de blocs.

Aujourd'hui, dans une grande partie des enquêtes menées contre toutes les formes de criminalité et de terrorisme, des **informations cryptées** sont en jeu. Le cryptage est essentiel pour le monde numérique, en ce qu'il permet de sécuriser les systèmes et les transactions numériques et de protéger une série de droits fondamentaux, y compris la liberté d'expression, la protection de la vie privée et la protection des données. Toutefois, s'il est utilisé à des fins criminelles, il peut également masquer l'identité des criminels et dissimuler le contenu de leurs communications. La Commission étudiera et soutiendra des solutions équilibrées d'ordre technique, opérationnel et juridique aux difficultés rencontrées et favorisera une approche qui préserve l'efficacité du cryptage pour ce qui est de la protection de la vie privée et de la sécurité des communications, tout en apportant une réponse efficace à la criminalité et au terrorisme.

Lutte contre les contenus illicites en ligne

Pour garantir un niveau de sécurité comparable pour les environnements en ligne et physique, il est nécessaire de progresser en permanence dans la **lutte contre les contenus illicites en ligne**. De plus en plus, les menaces fondamentales qui pèsent sur les citoyens, telles que le terrorisme, l'extrémisme ou les abus sexuels commis contre des enfants passent par l'environnement numérique, d'où la nécessité d'une action concrète et d'un cadre garantissant le respect des droits fondamentaux. Une première mesure essentielle consiste à conclure rapidement les négociations sur la proposition de législation relative à la prévention de la diffusion de contenus à caractère terroriste en ligne[67] et à veiller à sa mise en œuvre. Il est également primordial de renforcer la coopération volontaire entre les services répressifs et le secteur privé dans le **forum de l'UE sur l'internet** afin de lutter contre l'utilisation abusive de l'internet par les terroristes, les extrémistes violents et les criminels. L'unité de signalement des contenus sur l'internet de l'UE à Europol continuera de jouer un rôle crucial dans la surveillance des activités des groupes terroristes en ligne et des mesures prises par les plateformes[68], ainsi que dans la poursuite de l'élaboration du **protocole européen de crise**[69]. En outre, la Commission continuera de collaborer avec des partenaires internationaux, notamment en participant au **forum mondial de l'internet contre le terrorisme,** afin de relever ces défis à l'échelle planétaire. Des efforts supplémentaires seront consentis en vue de soutenir l'élaboration de contre-discours et de contre-récits au moyen du programme visant à renforcer les moyens d'action de la société civile[70].

Pour prévenir et endiguer la propagation des discours de haine illégaux en ligne, la Commission a instauré, en 2016, le code de conduite visant à combattre les discours de haine illégaux en ligne, assorti d'un engagement volontaire des plateformes en ligne à supprimer les contenus relevant du discours de haine. La dernière évaluation en date révèle que les entreprises concernées examinent 90 % des contenus signalés en l'espace de 24 heures et retirent 71 % des contenus considérés comme des discours de haine illégaux. Toutefois, les plateformes doivent encore améliorer la transparence et le retour

[67] Proposition de règlement relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne, COM(2018) 640 du 12.9.2018.

[68] Europol, novembre 2019.

[69] Une Europe qui protège - Protocole européen de crise: lutter contre les contenus à caractère terroriste en ligne. (octobre 2019).

[70] En rapport avec les travaux du programme de sensibilisation à la radicalisation (voir section IV.3 ci-dessous).

d'informations aux utilisateurs et veiller à la cohérence de l'évaluation des contenus signalés[71].

Le forum de l'UE sur l'internet facilitera aussi les échanges sur les technologies existantes et en cours de développement afin de relever les défis liés à la pédopornographie en ligne. La lutte contre la pédopornographie en ligne est au cœur d'une nouvelle stratégie visant à intensifier la **lutte contre les abus sexuels commis contre des enfants**[72], dont l'objectif consistera à optimiser le recours aux outils disponibles au niveau de l'UE pour combattre ces infractions. Les entreprises du secteur doivent être en mesure de poursuivre leur action de détection et de suppression des contenus pédopornographiques en ligne, les dommages causés par ces contenus requérant un cadre définissant des obligations claires et permanentes pour lutter contre ce problème. La stratégie annoncera aussi que la Commission s'apprête également à élaborer des dispositions législatives sectorielles visant à combattre plus efficacement la pédopornographie en ligne, dans le strict respect des droits fondamentaux.

D'une manière plus générale, la législation à venir sur les services numériques clarifiera et modernisera également les règles en matière de responsabilité et de sécurité des services numériques, tout en supprimant les freins à l'adoption de mesures destinées à lutter contre les contenus, les biens ou les services illégaux.

En outre, la Commission continuera de collaborer avec des partenaires internationaux et le **forum mondial de l'internet contre le terrorisme**, y compris par l'intermédiaire du comité consultatif indépendant, afin d'examiner comment relever ces défis au niveau international, tout en préservant les valeurs de l'UE et les droits fondamentaux. Il y a lieu également d'aborder de nouveaux thèmes, tels que les algorithmes ou les sites de jeux en ligne[73].

Menaces hybrides

L'ampleur et la diversité des menaces hybrides sont aujourd'hui sans précédents. La crise de la COVID-19 l'a montré avec encore plus d'acuité, plusieurs acteurs étatiques et non étatiques cherchant à instrumentaliser la pandémie (notamment en manipulant l'environnement de l'information et en s'en prenant à des infrastructures de base). La cohésion sociale risque de s'en trouver affaiblie et la confiance dans les institutions de l'UE et dans les gouvernements des États membres amoindrie.

L'approche suivie par l'UE en matière de lutte contre les menaces hybrides est exposée dans le cadre commun de 2016[74] et dans la communication conjointe de 2018 sur le renforcement de la résilience face aux menaces hybrides[75]. L'action à l'échelle de l'UE peut s'appuyer sur toute une panoplie d'outils, dont le lien entre les aspects intérieurs et les aspects extérieurs, reposant sur une approche qui englobe l'ensemble de la société et sur une coopération étroite avec des partenaires stratégiques, notamment l'OTAN et le G7. Un rapport sur la mise en œuvre de l'approche de l'UE en matière de lutte contre les menaces hybrides est publié avec

[71] https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf

[72] Stratégie de l'UE en faveur d'une lutte plus efficace contre les abus sexuels commis contre des enfants, COM(2020) 607.

[73] Les terroristes utilisent de plus en plus le système de messagerie des plateformes de jeux en ligne pour leurs échanges, tandis que les terroristes en herbe rejouent certaines attaques violentes en jeux vidéo.

[74] Cadre commun en matière de lutte contre les menaces hybrides: une réponse de l'Union européenne, JOIN (2016) 18.

[75] Accroître la résilience et renforcer la capacité à répondre aux menaces hybrides, JOIN(2018) 16.

la présente stratégie[76]. S'appuyant sur la cartographie[77] présentée parallèlement à la présente stratégie, les services de la Commission et le Service européen pour l'action extérieure créeront une **plateforme en ligne restreinte** sur laquelle les États membres indiqueront les outils et mesures de lutte utilisés contre les menaces hybrides à l'échelle de l'UE.

Si la lutte contre les menaces hybrides incombe au premier chef aux États membres (en raison de liens intrinsèques avec les politiques de sécurité et de défense nationales), certaines vulnérabilités sont le lot de tous les États membres et certaines menaces transcendent les frontières, notamment celles visant les réseaux ou les infrastructures transfrontières. La Commission et le haut représentant élaboreront une approche de l'UE en matière de lutte contre les menaces hybrides qui intègre les dimensions externe et interne dans un flux continu et réunit les considérations nationales et européennes. Cette approche devra couvrir l'éventail complet des actions, allant de la détection précoce à la réaction aux crises et à la gestion de leurs conséquences en passant par l'analyse, la sensibilisation, le renforcement de la résilience et la prévention.

Outre le renforcement de la mise en œuvre, les menaces hybrides évoluant constamment, un accent particulier sera mis sur **l'intégration des considérations hybrides dans l'élaboration des politiques**, afin d'éviter de prendre du retard sur la dynamique de l'évolution et de faire en sorte qu'aucune initiative potentiellement utile ne soit laissée de côté. Les effets des nouvelles initiatives seront aussi évalués en tenant compte des menaces hybrides, y compris pour les initiatives prises dans des domaines ne relevant pas jusque-là du cadre de lutte contre les menaces hybrides, tels que l'éducation, la technologie et la recherche. Cette approche pourrait bénéficier des travaux réalisés en matière de conceptualisation des menaces hybrides, laquelle donne une vision globale des divers outils susceptibles d'être utilisés par des adversaires[78]. L'objectif devrait être de faire en sorte que le processus de prise de décision se fonde sur des rapports sur l'évolution des menaces hybrides, rapports qui devront être à la fois réguliers, complets et fondés sur le renseignement. Ces rapports s'appuieront fortement sur les services de renseignements des États membres et sur le renforcement de la coopération en matière de renseignement avec les services compétents des États membres, par l'intermédiaire du Centre de situation et du renseignement de l'UE (INTCEN).

Afin de développer la **conscience situationnelle**, les services de la Commission et le Service européen pour l'action extérieure étudieront la possibilité d'intégrer les flux d'information provenant de sources différentes, y compris des États membres, ainsi que d'agences de l'UE, telles qu'ENISA, Europol et Frontex. La cellule de fusion de l'Union européenne contre les menaces hybrides demeurera le point focal de l'UE pour l'évaluation des menaces hybrides. Il est capital de **renforcer la résilience** pour prévenir les menaces hybrides et nous protéger d'elles. Il est par conséquent primordial d'établir un suivi systématique des progrès réalisés dans ce domaine et de les mesurer de manière objective. Une première mesure consistera à recenser les exigences de base sectorielles en matière de résilience face aux menaces hybrides, à la fois pour les États membres et pour les institutions et organes de l'UE. Enfin, pour intensifier **la préparation de la réaction aux crises liées aux menaces hybrides,** il

[76] SWD(2020) 153 Rapport sur la mise en œuvre du cadre commun de 2016 en matière de lutte contre les menaces hybrides (disponible en anglais uniquement) et la communication conjointe de 2018 intitulée «Accroître la résilience et renforcer la capacité à répondre aux menaces hybrides».

[77] SWD(2020) 152 Cartographie des mesures destinées à renforcer la résilience et à lutter contre les menaces hybrides (disponible en anglais uniquement).

[78] Tour d'horizon des menaces hybrides: modèle conceptuel JRC117280, élaboré conjointement par le Centre commun de recherche et le Centre d'excellence pour la lutte contre les menaces hybrides.

convient de réexaminer le protocole existant, défini dans le protocole opérationnel de l'UE de lutte contre les menaces hybrides de 2016 («EU Playbook»)[79], en tenant compte du réexamen plus large et du renforcement du système de réaction aux crises de l'UE actuellement à l'étude[80]. Le but est d'optimiser l'effet de l'action de l'UE en associant rapidement diverses réponses sectorielles et en assurant une coopération fluide avec nos partenaires, à commencer par l'OTAN.

Actions clés
• Veiller à ce que la législation en matière de cybercriminalité soit mise en œuvre et adaptée à sa finalité. • Stratégie en faveur d'une lutte plus efficace contre les abus sexuels commis contre des enfants. • Propositions en matière de détection et de suppression des contenus pédopornographiques. • Approche de l'UE en matière de lutte contre les menaces hybrides. • Réexamen du protocole opérationnel de l'UE pour la lutte contre les menaces hybrides («EU Playbook»). • Évaluation des moyens de renforcer les capacités des services répressifs en matière d'enquêtes numériques.

3. Protéger les Européens contre le terrorisme et la criminalité organisée

Terrorisme et radicalisation

La menace terroriste reste forte dans l'UE. Bien que le nombre d'attentats ait diminué globalement, ceux-ci peuvent toujours avoir des effets dévastateurs. La radicalisation peut aussi conduire à une plus grande polarisation et déstabiliser la cohésion sociale. La lutte contre le terrorisme et la radicalisation continue de relever, au premier chef, de la responsabilité des États membres. Toutefois, la dimension de plus en plus transfrontière et intersectorielle de la menace demande davantage de mesures en matière de coopération et de coordination au niveau de l'UE. La mise en œuvre effective de la législation de l'UE en matière de lutte contre le terrorisme, y compris en ce qui concerne les mesures restrictives est une priorité[81]. L'extension du mandat du Parquet européen aux infractions terroristes transfrontières demeure un objectif à atteindre.

Pour lutter contre le terrorisme, il convient tout d'abord de s'attaquer à ses causes profondes. La polarisation de la société, les discriminations réelles ou perçues et d'autres facteurs psychologiques et sociologiques peuvent renforcer la vulnérabilité des personnes aux discours radicaux. Dans ce contexte, la lutte contre la **radicalisation** se conjugue avec la promotion de la cohésion sociale à l'échelon local, national et européen. Au cours de la

[79] Protocole opérationnel de l'Union européenne pour la lutte contre les menaces hybrides («EU Playbook»), SWD(2016) 227, disponible en anglais uniquement.

[80] À l'issue de leur vidéoconférence du 26 mars 2020, les membres du Conseil européen ont adopté une déclaration sur les mesures prises par l'UE en réaction à l'épidémie de COVID-19, invitant la Commission à faire des propositions en vue d'un système de gestion des crises plus ambitieux et au champ d'action plus large au sein de l'UE.

[81] Le Conseil a adopté des mesures restrictives à l'égard de l'EIIL/Daech et d'Al-Qaida, ainsi que des mesures restrictives spécifiques visant certaines personnes et entités en vue de combattre le terrorisme. Voir la carte des sanctions imposées par l'UE (https://www.sanctionsmap.eu/#/main) pour avoir un aperçu de l'ensemble des mesures restrictives.

décennie écoulée, plusieurs initiatives et politiques suivies d'effets ont vu le jour, en particulier dans le cadre du réseau de sensibilisation à la radicalisation et de l'initiative «Les villes de l'UE contre la radicalisation».[82] Le moment est venu d'envisager l'adoption de mesures rendant plus efficaces les politiques, les initiatives et les fonds de l'UE en matière de lutte contre la radicalisation. De telles mesures peuvent soutenir le développement des capacités et des compétences, améliorer la coopération, enrichir le corpus des données factuelles et contribuer à l'évaluation des progrès accomplis, en associant l'ensemble des parties prenantes, y compris les intervenants de première ligne, les décideurs politiques et les milieux universitaires[83]. Des politiques non contraignantes, comme l'éducation, la culture, la jeunesse et les sports, pourraient contribuer à la prévention de la radicalisation, en offrant des perspectives aux jeunes à risque et en apportant une certaine cohésion au sein de l'UE[84]. Au nombre des domaines prioritaires figurent les actions sur la détection précoce et la gestion des risques, le renforcement de la résilience et le désengagement, ainsi que sur la réhabilitation et la réinsertion dans la société.

Les terroristes ont cherché à acquérir des agents **chimiques, biologiques, radiologiques et nucléaires** (CBRN)[85] et à les transformer en armes, tout en se dotant des connaissances et des moyens nécessaires pour les utiliser[86]. Le possible recours à des attaques CBRN figure en bonne place dans la propagande terroriste. Compte tenu des dégâts potentiels très élevés qu'elles pourraient infliger, il est nécessaire de leur accorder une attention particulière. Se fondant sur l'approche suivie pour réglementer l'accès aux précurseurs d'explosifs, la Commission réfléchira à la manière de restreindre l'accès à certains produits chimiques dangereux susceptibles d'être utilisés pour mener des attaques. Le développement de capacités de réaction de l'UE en matière de protection civile (rescEU) dans le domaine chimique, biologique, radiologique et nucléaire sera également déterminant. La coopération avec des pays tiers joue aussi un rôle important dans l'élaboration d'une culture commune de la sûreté et de la sécurité CBRN, en mettant pleinement à profit l'action des centres d'excellence CBRN de l'UE d'envergure internationale. Cette coopération portera notamment sur des évaluations des lacunes et des risques au niveau national, le soutien aux plans d'action CBRN nationaux et régionaux, des échanges de bonnes pratiques et des activités de renforcement des capacités CBRN.

L'UE a élaboré la législation la plus avancée au monde pour limiter l'accès aux **précurseurs d'explosifs**[87] et détecter les transactions suspectes visant à fabriquer des engins explosifs improvisés. La menace que représentent les explosifs artisanaux reste toutefois élevée, ces

[82] L'initiative pilote «Les villes de l'UE contre la radicalisation» poursuit le double objectif d'encourager l'échange d'expertise entre villes de l'UE, d'une part, et de recueillir des avis sur la manière de soutenir au mieux les communautés locales au niveau de l'UE, d'autre part.

[83] Par exemple, les financements alloués au titre du fonds européen pour la sécurité et du programme «Droits, égalité et citoyenneté».

[84] Actions de l'UE, telles que le projet d'échanges virtuels Erasmus + et le jumelage électronique.

[85] Ces deux dernières années, on a ainsi observé plusieurs cas, en Europe (France, Allemagne et Italie) et ailleurs dans le monde (Tunisie et Indonésie), d'utilisation d'agents biologiques (généralement des toxines d'origine végétale).

[86] Le Conseil a adopté des mesures restrictives de lutte contre la prolifération et l'utilisation d'armes chimiques.

[87] Produits chimiques susceptibles d'être utilisés d'une manière détournée pour la fabrication d'explosifs artisanaux. Ces produits sont régis par le règlement (UE) 2019/1148 relatif à la commercialisation et à l'utilisation de précurseurs d'explosifs.

derniers ayant été utilisés dans de multiples attentats à travers l'UE[88]. La première mesure à prendre consiste à appliquer les règles et aussi à faire en sorte que l'environnement en ligne ne permette pas d'échapper aux contrôles.

La poursuite effective des individus ayant commis des infractions terroristes, y compris des **combattants terroristes étrangers** actuellement présents en Syrie et en Iraq, constitue aussi un élément important de la politique de lutte contre le terrorisme. Si ces questions relèvent en premier lieu des compétences des États membres, la coordination et le soutien de l'UE peuvent aider ces derniers à relever des défis communs. Les mesures prises en ce moment en vue de mettre pleinement en œuvre la législation relative à la sécurité des frontières[89] et de faire pleinement usage de toutes les bases de données de l'UE pertinentes pour partager des renseignements sur les suspects connus joueront un rôle important à cet égard. Outre l'identification des individus présentant un risque élevé, il importe de disposer d'une politique de réintégration et de réinsertion. La coopération interprofessionnelle, associant notamment le personnel pénitentiaire et les agents de probation, renforcera la compréhension judiciaire des processus de radicalisation menant à l'extrémisme violent et consolidera l'approche du secteur judiciaire en matière de sanctions et de recours à des solutions autres que la détention.

Le défi posé par les combattants terroristes étrangers est emblématique du lien qui existe entre **sécurité intérieure et extérieure**. La coopération en matière de lutte contre le terrorisme ainsi qu'en matière de prévention de la radicalisation et de l'extrémisme violent et de lutte contre ces phénomènes est essentielle pour la sécurité au sein de l'UE[90]. D'autres mesures sont nécessaires pour favoriser les partenariats et la coopération en matière de lutte contre le terrorisme avec les pays de notre voisinage et au-delà, en tirant parti du savoir-faire du réseau des experts de l'UE en matière de sécurité et de lutte contre le terrorisme. Le plan d'action conjoint relatif à la lutte contre le terrorisme dans les Balkans occidentaux est une bonne référence pour ce genre de coopération ciblée. Des efforts sont nécessaires en particulier pour soutenir la capacité des pays partenaires à identifier et à localiser les combattants terroristes étrangers. L'UE continuera aussi à promouvoir la coopération multilatérale en œuvrant aux côtés des principaux acteurs mondiaux dans ce domaine, comme les Nations unies, l'OTAN, le Conseil de l'Europe, Interpol et l'OSCE. Elle entend collaborer également avec le forum mondial contre le terrorisme et la coalition internationale contre Daech, ainsi qu'avec les acteurs de la société civile concernés. Les instruments de politique extérieure de l'Union, notamment en matière de développement et de coopération, jouent aussi un rôle important dans la coopération avec les pays tiers en vue de prévenir le terrorisme et la piraterie. La coopération internationale est essentielle aussi pour assécher toutes les sources de **financement du terrorisme**, par exemple au moyen du groupe d'action financière.

---

[88] On citera comme exemples de tels attentats dévastateurs ceux perpétrés à Oslo (en 2011), à Paris (en 2015), à Bruxelles (en 2016), et à Manchester (en 2017). Un attentat à l'explosif artisanal commis à Lyon (en 2019) a blessé 13 personnes.

[89] Dont le nouveau mandat de l'Agence européenne de garde-frontières et de garde-côtes (Frontex).

[90] Les conclusions du Conseil du 16 juin 2020 ont souligné la nécessité de protéger les citoyens de l'UE contre le terrorisme et l'extrémisme violent sous toutes leurs formes et quelle qu'en soit l'origine, et de renforcer encore l'action et l'engagement extérieur de l'UE en matière de lutte contre le terrorisme dans certains domaines géographiques et thématiques prioritaires.

Criminalité organisée

Le coût économique et personnel de la criminalité organisée est énorme. Selon les estimations, la criminalité organisée et la corruption engendrent chaque année des pertes économiques comprises entre 218 et 282 milliards d'EUR[91]. En 2017, plus de 5 000 organisations criminelles faisaient l'objet d'enquêtes en Europe – soit une hausse de 50 % par rapport à 2013[92]. La criminalité organisée opère de plus en plus au niveau transfrontière, y compris dans le voisinage immédiat de l'UE, ce qui requiert une coopération opérationnelle et un échange d'informations renforcés avec les partenaires du voisinage.

De nouveaux défis apparaissent et de nouvelles formes d'infractions voient le jour sur l'internet; ainsi, dans le cadre de la pandémie de COVID-19, les escroqueries en ligne visant les groupes vulnérables ont augmenté considérablement et les produits sanitaires et de santé ont été la cible de vols et de cambriolages[93]. L'UE doit intensifier son action de lutte contre la criminalité organisée, y compris au niveau international, en élargissant la panoplie d'outils capables de démanteler le modèle économique de la criminalité organisée. La lutte contre la criminalité organisée requiert également une coopération étroite avec les administrations locales et régionales ainsi qu'avec la société civile, qui sont des partenaires essentiels pour prévenir la criminalité et aider et soutenir les victimes, les administrations des régions frontalières devant faire l'objet d'une attention particulière dans ce combat. Ces actions seront réunies dans un **programme de lutte contre la criminalité organisée**.

Plus d'un tiers des organisations criminelles actives dans l'UE sont impliquées dans la production, le trafic ou la vente de stupéfiants. En 2019, la toxicomanie a provoqué plus de huit mille décès par overdose dans l'UE. Le **trafic de stupéfiants** opère pour l'essentiel au niveau transfrontière et une partie importante des bénéfices générés par ce trafic infiltre l'économie légale[94]. Grâce à son nouveau programme antidrogue[95], l'UE renforcera les efforts qu'elle et ses États membres déploient pour réduire l'offre et la demande de drogue; ce programme définira des actions conjointes pour résoudre un problème commun et renforcer le dialogue et la coopération entre l'UE et les partenaires extérieurs sur les questions liées à la drogue. Sur la base d'une évaluation de l'Observatoire européen des drogues et des toxicomanies, la Commission examinera si le mandat de ce dernier doit être actualisé pour répondre aux nouveaux défis.

Les organisations criminelles et les terroristes sont également des acteurs majeurs du commerce des **armes à feu illégales**. Entre 2009 et 2018, 23 tueries de masse ont eu lieu en Europe, faisant plus de 340 victimes[96]. Les armes à feu sont souvent introduites dans l'UE depuis son voisinage immédiat[97] dans le cadre de trafics, ce qui souligne la nécessité de renforcer la coordination et la coopération tant au sein de l'UE qu'avec les partenaires internationaux, en particulier Interpol, afin d'harmoniser la collecte d'informations et

[91] Calculée en pourcentage du produit intérieur brut (PIB); rapport d'Europol: «Does crime still pay?» – Criminal asset recovery in the EU, 2016.

[92] Europol, Serious and Organised Threat Assessments (SOCTA), 2013 et 2017.

[93] Europol, 2020.

[94] OEDT et Europol, rapport 2019 sur les marchés de la drogue dans l'UE (novembre 2019).

[95] Programme et plan d'action antidrogue de l'UE (2021-2025), COM(2020) 606.

[96] Flemish Peace Institute, Armed to kill (octobre 2019).

[97] L'UE finance la lutte contre la prolifération et le trafic des armes légères et de petit calibre dans la région depuis 2002; elle a notamment financé le réseau d'experts en armes à feu de l'Europe du Sud-Est (SEEFEN). Depuis 2019, les partenaires des Balkans occidentaux sont pleinement associés à la priorité relative aux armes à feu de la plateforme pluridisciplinaire européenne contre les menaces criminelles (EMPACT).

l'établissement de rapports sur les saisies d'armes à feu. Il est également essentiel d'améliorer la traçabilité des armes, y compris sur l'internet, et de garantir l'échange d'informations entre les autorités chargées de l'octroi des permis et les services répressifs. La Commission présente un nouveau **plan d'action de l'UE en matière de lutte contre le trafic d'armes à feu**[98] et examinera également si les règles applicables aux autorisations d'exportation et aux mesures concernant l'importation et le transit d'armes à feu sont toujours adaptées[99].

Les organisations criminelles considèrent les migrants et les personnes ayant besoin d'une protection internationale comme une marchandise. 90 % des migrants en situation irrégulière arrivent dans l'UE par l'intermédiaire d'un réseau criminel[100]. Le trafic de migrants est souvent étroitement lié à d'autres formes de criminalité organisée, en particulier la traite des êtres humains[101]. Outre le coût humain considérable de cette traite, Europol estime que les bénéfices annuels générés au niveau mondial par toutes les formes d'exploitation de la traite des êtres humains s'élèvent à 29,4 milliards d'EUR. Il s'agit d'une criminalité transnationale qui repose sur des demandes illégales provenant à la fois de l'UE et des pays tiers et qui touche tous les États membres de l'UE. Les difficultés rencontrées pour identifier, poursuivre et condamner ces criminels montrent qu'il est nécessaire d'adopter une nouvelle approche pour renforcer les mesures. Une nouvelle **approche globale de la traite des êtres humains** permettra de regrouper les lignes d'action. La Commission présentera également un **nouveau plan d'action de l'UE contre le trafic de migrants** pour la période 2021-2025. Ces deux volets seront axés sur la lutte contre les réseaux criminels, le renforcement de la coopération et le soutien à l'action des services répressifs.

Les organisations criminelles – ainsi que les terroristes – sont également à la recherche de sources de revenus dans d'autres domaines, en particulier ceux qui génèrent des bénéfices élevés et qui présentent un faible risque de détection, tels que la **criminalité environnementale**. Le braconnage et le commerce illégal d'espèces sauvages, l'exploitation minière illégale, l'exploitation forestière ainsi que l'élimination et les transferts illicites de déchets sont passés au quatrième rang des principales activités criminelles au niveau mondial[102]. Les systèmes d'échange de quotas d'émission et les régimes de certificats énergétiques ont également été exploités à des fins criminelles et des fonds alloués à la résilience environnementale et au développement durable ont été détournés. En plus d'encourager l'UE, les États membres et la communauté internationale à agir pour intensifier les efforts de lutte contre la criminalité environnementale[103], la Commission examine si la directive sur la protection de l'environnement par le droit pénal[104] est toujours adaptée. Le **trafic de biens culturels**, qui connaît un essor, est également devenu l'une des activités criminelles les plus lucratives et constitue une source de financement du terrorisme et de la criminalité organisée. Il convient d'étudier comment améliorer la traçabilité en ligne et hors ligne des biens culturels dans le marché intérieur et la coopération avec les pays tiers

[98] COM(2020) 608.
[99] Règlement (UE) nº 258/2012 portant application de l'article 10 du protocole des Nations unies contre la fabrication et le trafic illicites d'armes à feu.
[100] Source: Europol.
[101] Europol, EMSC, 4e rapport annuel.
[102] UNEP-INTERPOL Rapid Response Assessment: The Rise of Environmental Crime, juin 2016.
[103] Voir le pacte vert pour l'Europe, COM(2019) 640 final.
[104] Directive 2008/99/CE relative à la protection de l'environnement par le droit pénal.

victimes des vols, ainsi que de fournir un soutien actif aux services répressifs et aux milieux universitaires.

Les **délits économiques et financiers** sont extrêmement complexes, mais ils touchent chaque année des millions de citoyens et des milliers d'entreprises dans l'UE. La lutte contre la fraude est primordiale et nécessite une action au niveau de l'UE. Europol, ainsi qu'Eurojust, le Parquet européen et l'Office européen de lutte antifraude, aident les États membres et l'UE à protéger les marchés économiques et financiers et à veiller sur l'argent des contribuables européens. Le Parquet européen sera pleinement opérationnel pour la fin de l'année 2020 et sera chargé de rechercher, poursuivre et juger les infractions portant atteinte au budget de l'Union, telles que la fraude, la corruption et le blanchiment de capitaux. Il luttera également contre la fraude transfrontière à la TVA qui coûte aux contribuables au moins 50 milliards d'EUR chaque année.

La Commission soutiendra également le développement d'une expertise et la mise en place d'un cadre législatif dans le domaine des risques émergents, tels que les crypto-actifs et les nouveaux systèmes de paiement. Elle examinera en particulier la réponse à apporter face à l'émergence de crypto-actifs tels que le bitcoin, ainsi que les effets qu'auront ces nouvelles technologies sur l'émission, l'échange et le partage d'actifs financiers et sur l'accès à ceux-ci.

L'argent illicite doit faire l'objet d'une tolérance zéro dans l'Union européenne. En l'espace de trente ans, l'UE s'est dotée d'un solide cadre réglementaire pour prévenir et combattre le **blanchiment de capitaux** et le financement du terrorisme, et ce tout en respectant pleinement la nécessité de protéger les données à caractère personnel. Le consensus se fait pourtant de plus en plus large sur le besoin d'améliorer en profondeur la mise en œuvre du cadre existant. Il faut s'attaquer aux divergences profondes dans ses modalités d'application, mais aussi aux graves lacunes dans l'exécution des règles. Comme indiqué dans le plan d'action de mai 2020[105], des travaux sont en cours pour évaluer les différentes options visant à renforcer le cadre européen de lutte contre le blanchiment de capitaux et le financement du terrorisme. Parmi les pistes à explorer figure l'interconnexion des registres nationaux centralisés des comptes bancaires, qui pourrait considérablement accélérer l'accès des cellules de renseignement financier et des autorités compétentes aux informations financières.

Les **profits des organisations criminelles sont estimés à 110 milliards d'EUR par an** dans l'UE. La réponse actuelle comprend une législation harmonisée sur la confiscation et le recouvrement des avoirs[106] dans le but d'améliorer le gel et la confiscation des avoirs d'origine criminelle dans l'UE et de faciliter la confiance mutuelle et une coopération transfrontière effective entre les États membres. Toutefois, seul 1 % de ces profits sont confisqués[107], ce qui permet aux organisations criminelles d'investir pour élargir leurs activités criminelles et infiltrer l'économie légale, et en particulier les petites et moyennes entreprises, qui ont du mal à accéder au crédit et qui constituent une cible privilégiée pour le blanchiment de capitaux. La Commission analysera la mise en œuvre de la législation[108] et

[105] Plan d'action en matière de prévention du blanchiment de capitaux et du financement du terrorisme, C(2020) 2800.

[106] Selon le droit de l'Union, des bureaux de recouvrement des avoirs doivent être mis en place dans tous les États membres.

[107] Rapport intitulé «Recouvrement et confiscation d'avoirs: Garantir que le crime ne paie pas», COM(2020) 217 final.

[108] Directive 2014/42/UE concernant le gel et la confiscation des instruments et des produits du crime dans l'Union européenne.

la nécessité éventuelle d'adopter de nouvelles règles communes, y compris en ce qui concerne la confiscation non fondée sur une condamnation. Les bureaux de recouvrement des avoirs[109], acteurs clés du processus de recouvrement des avoirs, pourraient également être dotés de meilleurs outils pour identifier et dépister plus rapidement les avoirs d'origine criminelle dans l'ensemble de l'UE afin d'augmenter les taux de confiscation.

La criminalité organisée et la **corruption** sont intimement liées. Selon des estimations, la corruption à elle seule coûte environ 120 milliards d'EUR par an à l'économie de l'UE[110]. La prévention de la corruption et la lutte contre celle-ci continueront à faire l'objet d'un suivi régulier dans le cadre du mécanisme de protection de l'état de droit et du Semestre européen. Le Semestre européen s'est penché sur certains secteurs problématiques dans la lutte contre la corruption, tels que les marchés publics, l'administration publique, l'environnement des entreprises ou les soins de santé. Le nouveau rapport annuel de la Commission sur l'état de droit portera sur la lutte contre la corruption et permettra la mise en place d'un dialogue préventif avec les autorités nationales et les parties intéressées au niveau de l'UE et au niveau national. Les organisations de la société civile peuvent aussi jouer un rôle essentiel pour encourager les pouvoirs publics à agir pour prévenir et combattre la criminalité organisée et la corruption, et ces groupes pourraient être réunis de manière constructive dans une enceinte commune. En raison de la nature transfrontière de la criminalité organisée et de la corruption, la coopération et l'assistance avec les régions du voisinage de l'UE jouent un rôle clé.

Actions clés
• Programme de lutte contre le terrorisme pour l'UE, comprenant de nouvelles actions de lutte contre la radicalisation dans l'UE. • Nouvelle coopération avec des pays tiers et des organisations internationales stratégiques en matière de lutte contre le terrorisme. • Programme de lutte contre la criminalité organisée, y compris la traite des êtres humains. • Programme et plan d'action antidrogue de l'UE 2021-2025. • Évaluation de l'Observatoire européen des drogues et des toxicomanies. • Plan d'action de l'UE en matière de lutte contre le trafic d'armes à feu pour la période 2020-2025. • Réexamen de la législation sur le gel et la confiscation des avoirs et sur les bureaux de recouvrement des avoirs. • Évaluation de la directive sur la protection de l'environnement par le droit pénal. • Plan d'action de l'UE contre le trafic de migrants pour la période 2021-2025.

4. Un solide écosystème européen de la sécurité

La mise en place d'une union de la sécurité réelle et effective doit être un combat commun à toutes les composantes de la société. Les gouvernements, les services répressifs, le secteur privé, le secteur de l'éducation et les citoyens eux-mêmes doivent s'y investir et être équipés

[109] Décision 2007/845/JAI du Conseil relative à la coopération entre les bureaux de recouvrement des avoirs des États membres en matière de dépistage et d'identification des produits du crime ou des autres biens en rapport avec le crime.

[110] Il est difficile d'estimer les coûts économiques totaux de la corruption, même si des efforts ont été consentis en ce sens par des organismes tels que la Chambre internationale de commerce, Transparency International, le pacte mondial des Nations unies et le Forum économique mondial; selon leurs estimations, elle représenterait 5 % du PIB mondial.

et bien connectés pour renforcer la préparation et la résilience pour tous, en particulier les plus vulnérables, les victimes ainsi que les témoins.

Toutes les politiques doivent intégrer la dimension de la sécurité et l'UE peut apporter une contribution à tous les niveaux. Dans les foyers, la violence domestique constitue l'un des risques les plus graves en matière de sécurité. Ainsi, 22 % des femmes de l'UE ont déjà subi des violences commises par leur partenaire[111]. L'adhésion de l'UE à la convention d'Istanbul sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique demeure une priorité essentielle. Si les négociations restent au point mort, la Commission prendra d'autres mesures pour atteindre les mêmes objectifs que la convention, notamment en proposant d'ajouter la violence à l'égard des femmes à la liste des infractions pénales de l'UE définies dans le traité.

Coopération et échange d'informations

L'une des contributions les plus importantes que l'UE peut apporter en matière de protection des citoyens consiste à aider les responsables de la sécurité à collaborer de manière efficace. La coopération et le partage d'informations sont les outils les plus efficaces pour lutter contre la criminalité et le terrorisme et rendre la justice. Pour être efficaces, ils doivent être ciblés et mis en œuvre au moment opportun. Pour être fiables, ils doivent être assortis de garanties et de contrôles communs.

L'UE a prévu un certain nombre d'instruments et de stratégies sectorielles spécifiques[112] pour renforcer la **coopération opérationnelle entre les services répressifs** des États membres. Un des principaux instruments de l'UE à l'appui de la coopération entre les services répressifs des États membres est le système d'information Schengen, utilisé pour échanger en temps réel des données sur des personnes et des objets recherchés ou disparus. Il a ainsi été possible de procéder à l'arrestation de criminels, à des saisies de drogue et au sauvetage de victimes potentielles[113]. Le niveau de coopération pourrait toutefois être encore amélioré en rationalisant et en modernisant les instruments disponibles. La majeure partie du cadre juridique de l'UE sous-tendant la coopération opérationnelle entre les services répressifs a été pensée il y a trente ans. Le réseau complexe d'accords bilatéraux qu'ont tissé les États membres, accords dont beaucoup sont devenus obsolètes ou sous-exploités, risque de se fragmenter. Dans les pays plus petits ou enclavés, les agents des services répressifs exerçant des activités transfrontières doivent mener des actions opérationnelles en se référant parfois à sept réglementations différentes; il s'ensuit que certaines opérations, telles que les poursuites transfrontières de suspects entre États membres n'ont tout simplement pas lieu. La coopération opérationnelle en matière de nouvelles technologies, telles que les drones, n'est pas non plus couverte par le cadre actuel de l'UE.

L'efficacité opérationnelle peut être renforcée par une coopération spécifique entre les services répressifs, ce qui peut également contribuer à apporter un soutien essentiel à d'autres objectifs stratégiques – tels que la fourniture d'informations en matière de sécurité pour la nouvelle évaluation des investissements directs étrangers. La Commission examinera l'utilité qu'un code de coopération policière pourrait avoir à cet égard. Les services répressifs des États membres ont de plus en plus eu recours au soutien et à l'expertise disponible au niveau de l'UE, tandis que l'INTCEN de l'UE a joué un rôle essentiel dans la

[111] Une Union de l'égalité: stratégie en faveur de l'égalité entre les hommes et les femmes 2020-2025, COM(2020) 152.

[112] Tels que le plan d'action pour la stratégie de sûreté maritime de l'UE, qui a permis de réaliser d'importantes avancées en matière de coopération sur les fonctions de garde-côtes entre les agences compétentes de l'UE.

[113] Action de l'UE contre la criminalité organisée en 2019 (Conseil, 2020).

promotion de l'échange d'informations stratégiques entre les services de renseignement et de sécurité des États membres, en fournissant une appréciation de la situation aux institutions de l'UE[114]. **Europol** peut également jouer un rôle clé en étendant sa coopération avec les pays tiers dans le domaine de la lutte contre la criminalité et le terrorisme, dans le respect des autres politiques et instruments de l'action extérieure de l'UE. Cependant, Europol doit aujourd'hui faire face à un certain nombre de contraintes importantes – notamment en ce qui concerne l'échange direct de données à caractère personnel avec des parties privées – qui l'empêchent de soutenir efficacement les États membres dans la lutte contre le terrorisme et la criminalité. Son mandat est actuellement à l'étude afin de déterminer comment l'améliorer pour que l'agence puisse remplir pleinement ses missions. Dans ce contexte, les autorités compétentes au niveau de l'UE (telles que l'OLAF, Europol, Eurojust et le Parquet européen) devraient également coopérer plus étroitement et améliorer l'échange d'informations.

Un autre point fondamental est la poursuite du développement d'**Eurojust** afin de maximiser les synergies entre la coopération des services répressifs et la coopération judiciaire. L'UE bénéficierait également d'une meilleure cohérence stratégique: **EMPACT**[115], le cycle politique de l'UE pour lutter contre la grande criminalité internationale organisée, fournit aux autorités une méthodologie fondée sur le renseignement en matière pénale afin de leur permettre de faire face conjointement aux menaces criminelles les plus importantes qui pèsent sur l'UE. Cette plateforme a produit d'importants résultats opérationnels[116] au cours de la dernière décennie. Sur la base de l'expérience des acteurs de terrain, il convient de rationaliser et de simplifier le mécanisme existant afin de mieux faire face aux menaces criminelles les plus urgentes et en mutation pour un nouveau cycle politique 2022-2025.

Il est essentiel de disposer d'**informations** pertinentes et opportunes pour le travail quotidien des services répressifs. En dépit du développement de nouvelles bases de données en matière de sécurité et de gestion des frontières au niveau de l'UE, de nombreuses informations figurent encore dans les bases de données nationales ou sont échangées sans recourir à ces outils. Il en résulte une surcharge de travail importante, des retards et un risque accru que des informations clés ne soient pas prises en compte. Des processus plus efficaces, plus rapides et plus simples, associant l'ensemble de la communauté de la sécurité, permettraient d'obtenir de meilleurs résultats. Il est essentiel de disposer des outils adéquats pour que l'échange d'informations soit pleinement exploité dans le cadre d'une lutte efficace contre la criminalité, avec toutes les garanties nécessaires pour que le partage des données respecte la législation en matière de protection des données et les droits fondamentaux. Au vu des évolutions constatées dans les technologies, la police scientifique et la protection des données, ainsi que des nouveaux besoins opérationnels, l'UE pourrait examiner s'il convient de moderniser certains instruments tels que les **décisions Prüm de 2008**, en prévoyant un échange automatisé des données ADN, des données dactyloscopiques et des données relatives à l'immatriculation des véhicules, afin de permettre l'échange automatisé de catégories supplémentaires de données qui sont déjà disponibles dans les bases de données pénales ou autres des États membres aux fins des enquêtes pénales. En outre, la Commission examinera la possibilité d'échanger les extraits de casier judiciaire afin

[114] L'INTCEN de l'UE est le point d'accès unique qui permet aux services de renseignement et de sécurité des États membres de fournir à l'UE une appréciation de la situation fondée sur le renseignement.
[115] EMPACT: plateforme pluridisciplinaire européenne contre les menaces criminelles.
[116] https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf.

de déterminer si une personne possède un casier judiciaire dans d'autres États membres et d'en faciliter l'accès, le cas échéant, avec toutes les garanties nécessaires.

Les **informations sur les voyageurs** ont permis l'amélioration des contrôles aux frontières, la réduction de la migration irrégulière et l'identification de personnes présentant un risque pour la sécurité. Les informations préalables sur les passagers (données API) sont des données biographiques que les transporteurs aériens collectent pour chaque passager lors de l'enregistrement, puis qu'ils envoient aux autorités du pays de destination chargées des contrôles frontaliers. Le réexamen du cadre juridique[117] pourrait permettre une utilisation plus efficace de ces informations, tout en garantissant le respect de la législation sur la protection des données et en facilitant le flux des voyageurs. Les données des dossiers passagers (données PNR) sont des informations fournies par les passagers lors de la réservation des vols. La mise en œuvre de la directive PNR[118] est essentielle, et la Commission continuera de la soutenir et de la faire respecter. En outre, la Commission lancera à mi-parcours un réexamen des pratiques actuelles en matière de **transfert de données PNR vers des pays tiers**.

La **coopération judiciaire** constitue un complément nécessaire des efforts déployés par les services de police en matière de lutte contre la criminalité transfrontière. Elle a profondément évolué au cours des 20 dernières années. Des instances telles que le **Parquet européen** et **Eurojust** doivent disposer des moyens nécessaires pour pouvoir fonctionner pleinement ou voir leurs capacités renforcées. La coopération entre les professionnels de la justice pourrait également être intensifiée grâce à des mesures supplémentaires ayant trait à la reconnaissance mutuelle des décisions de justice, à la formation judiciaire et à l'échange d'informations. L'objectif devrait être d'accroître la confiance mutuelle entre les magistrats, essentielle afin de faciliter les procédures transfrontières. L'utilisation des **technologies numériques** peut aussi améliorer l'efficacité de nos systèmes judiciaires. Un nouveau système d'échange de preuves numériques est actuellement mis en place afin de permettre la transmission des décisions d'enquête européennes, des demandes d'entraide judiciaire et des communications y afférentes entre les États membres, avec l'appui d'Eurojust. La Commission collaborera avec les États membres en vue d'accélérer le déploiement des systèmes informatiques nécessaires au niveau national.

La coopération internationale est également essentielle pour garantir l'efficacité des services répressifs et la coopération judiciaire. Les accords bilatéraux avec des partenaires clés jouent un rôle essentiel dans l'obtention d'informations et d'éléments de preuve provenant de pays tiers. **Interpol,** l'une des plus grandes organisations de police criminelle intergouvernementales, joue un rôle important à cet égard. La Commission examinera comment intensifier sa coopération avec cette organisation, y compris les possibilités d'accès aux bases de données de celle-ci et le renforcement de la coopération opérationnelle et stratégique. Les services répressifs de l'UE s'appuient également sur les principaux pays partenaires pour détecter les criminels et les terroristes et enquêter sur ceux-ci. Les **partenariats conclus entre l'Union et les pays tiers concernant la sécurité** pourraient être renforcés en vue d'une coopération accrue en matière de lutte contre des menaces communes telles que le terrorisme, la criminalité organisée, la cybercriminalité, les abus sexuels sur les enfants et la traite des êtres humains. Une telle approche, fondée sur des

[117] Directive 2004/82/CE du Conseil concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers.

[118] Directive (UE) 2016/681 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.

intérêts communs en matière de sécurité, s'appuie sur les dialogues mis en place dans les domaines de la coopération et de la sécurité.

Comme pour l'information, l'échange d'expertise peut revêtir un intérêt particulier pour la préparation des services répressifs face aux menaces **non traditionnelles**. En plus d'encourager les échanges de bonnes pratiques, la Commission examinera la possibilité d'un **mécanisme de coordination des forces de police au niveau de l'UE** dans le cadre d'événements de force majeure tels que les pandémies. L'actuelle pandémie a également montré qu'une police de proximité adaptée à l'ère numérique, dotée de cadres juridiques visant à faciliter les activités policières en ligne, sera essentielle dans la lutte contre la criminalité et le terrorisme. Les partenariats entre la police et les communautés, hors ligne et en ligne, peuvent contribuer à prévenir la criminalité et à atténuer les effets de la criminalité organisée, de la radicalisation et des activités terroristes. L'interconnexion entre les solutions policières de portées locale, régionale, nationale et européenne constitue un élément de réussite essentiel de l'union de la sécurité dans son ensemble.

La contribution de frontières extérieures solides

Une gestion moderne et efficace des frontières extérieures a le double avantage de maintenir l'intégrité de l'espace Schengen et de garantir la sécurité des citoyens de l'Union. Mobiliser l'ensemble des acteurs concernés pour tirer le meilleur parti de la sécurité aux frontières peut avoir une réelle incidence sur la prévention de la criminalité et du terrorisme transfrontières. Les activités opérationnelles conjointes du corps européen de garde-frontières et de garde-côtes[119], qui a été renforcé récemment, contribuent à la prévention et à la détection de la criminalité transfrontière aux **frontières extérieures** et au-delà de l'UE. Les activités douanières visant à détecter les risques pour la sécurité et la sûreté présentés par l'ensemble des biens avant qu'ils atteignent l'UE et à contrôler ces biens à leur arrivée jouent un rôle essentiel dans la lutte contre la criminalité transfrontière et le terrorisme. Le futur plan d'action sur l'union douanière annoncera des actions ayant également pour objet de renforcer la gestion des risques et d'accroître la sécurité intérieure, notamment en évaluant la faisabilité de l'établissement de liens entre les systèmes d'information pertinents pour l'analyse des risques à des fins de sécurité.

Le cadre pour l'**interopérabilité des systèmes d'information de l'UE** dans le domaine de la justice et des affaires intérieures a été adopté en mai 2019. Ce nouveau cadre vise à améliorer l'efficience et l'efficacité des systèmes d'information nouveaux ou ayant été modernisés[120]. Il permettra aux policiers, aux garde-frontières et aux agents des services de migration d'obtenir des informations plus rapidement et de façon plus systématique. Il contribuera à l'identification correcte des personnes et à la lutte contre la fraude à l'identité. Pour que ce cadre fonctionne dans les faits, il convient de donner la priorité à la mise en œuvre de l'interopérabilité, tant au niveau politique que sur le plan technique. Une étroite collaboration entre les agences de l'UE et l'ensemble des États membres sera capitale pour atteindre l'objectif d'une interopérabilité totale d'ici à 2023.

La **fraude liée aux documents de voyage** est considérée comme l'un des délits les plus fréquents. Elle facilite les mouvements clandestins des criminels et des terroristes et joue un

[119] Constitué de l'Agence européenne de garde-frontières et de garde-côtes (Frontex) et des garde-frontières et garde-côtes des États membres.

[120] À savoir, le système d'entrée/de sortie (EES), le système européen d'information et d'autorisation concernant les voyages (ETIAS), le système européen étendu d'information sur les casiers judiciaires (ECRIS-TCN), le système d'information Schengen, le système d'information sur les visas et le futur Eurodac actualisé.

rôle essentiel dans la traite des êtres humains et le trafic de stupéfiants[121]. La Commission examinera les possibilités d'extension des travaux actuellement menés sur les normes de sécurité applicables aux documents de voyage et aux titres de séjour de l'UE, au moyen de la numérisation notamment. À partir d'août 2021, les États membres commenceront à délivrer des cartes d'identité et des titres de séjour qui répondent à des normes de sécurité harmonisées et qui comportent une puce contenant des identifiants biométriques pouvant être vérifiés par l'ensemble des autorités frontalières de l'UE. La Commission suivra la mise en œuvre de ces nouvelles règles, y compris le remplacement progressif des documents actuellement en circulation.

Renforcer la recherche et l'innovation en matière de sécurité

Les travaux menés en vue de garantir la cybersécurité et de lutter contre la criminalité organisée, la cybercriminalité et le terrorisme reposent en grande partie sur l'élaboration d'outils devant permettre de développer de nouvelles technologies plus sûres, de relever les défis d'ordre technologique et de soutenir le travail des services répressifs, l'élaboration de ces outils dépendant elle-même des partenaires privés et du secteur industriel.

L'innovation doit être considérée comme un outil stratégique dans la lutte contre les menaces actuelles et l'anticipation des risques et des perspectives futurs. Les technologies innovantes peuvent déboucher sur la mise au point de nouveaux outils venant en aide aux services répressifs et aux autres acteurs de la sécurité. L'intelligence artificielle et l'analyse des mégadonnées pourraient tirer parti du calcul à haute performance afin de permettre une meilleure détection et une analyse rapide et exhaustive[122]. Des ensembles de données de qualité élevée, permettant aux autorités compétentes d'entraîner, de tester et de valider les algorithmes, constituent une condition préalable essentielle au développement de technologies fiables[123]. D'une manière plus générale, le risque de dépendance technologique est actuellement élevé: l'UE est, par exemple, un importateur net de produits et de services de cybersécurité, avec tout ce que cela implique pour l'économie et les infrastructures critiques. Pour maîtriser la technologie et garantir la continuité de l'approvisionnement également en cas d'événements préjudiciables et lors de crises, l'Europe doit être présente et disposer de capacités dans les parties critiques des chaînes de valeur concernées.

La **recherche, l'innovation et le développement technologique** de l'UE permettent la prise en compte de la dimension «sécurité» au fur et à mesure du développement de ces technologies et de leur application. La prochaine génération de propositions de financement de l'UE peut jouer un rôle majeur à cet égard[124]. Les initiatives relatives aux espaces européens des données et aux infrastructures en nuage intègrent d'emblée l'aspect sécurité. Le Centre européen de compétences industrielles, technologiques et de recherche en matière

[121] Le lien entre la fraude documentaire et la traite des êtres humains est exposé dans le deuxième rapport sur les progrès réalisés dans la lutte contre la traite des êtres humains [COM(2018) 777] et dans le document de travail de services de la Commission qui l'accompagne [SWD (2018) 473], ainsi que dans le rapport d'Europol de 2016 intitulé «Situation Report Trafficking in human beings in the EU» (Situation concernant la traite des êtres humains dans l'UE).

[122] Il convient à cet effet de s'appuyer sur la stratégie de la Commission en matière d'intelligence artificielle.

[123] Une stratégie européenne pour les données, COM(2020) 66 final.

[124] Les propositions de la Commission concernant Horizon Europe, le Fonds pour la sécurité intérieure, le Fonds pour la gestion intégrée des frontières, le programme EUInvest, le Fonds européen de développement régional et le programme pour une Europe numérique soutiendront le développement et le déploiement de technologies et de solutions innovantes en matière de sécurité tout au long de la chaîne de valeur de la sécurité.

de cybersécurité et le Réseau de centres nationaux de coordination[125] ont pour ambition de mettre en place une structure efficace et efficiente permettant la mise en commun et le partage des capacités de recherche et des résultats dans le domaine de la cybersécurité. Le programme spatial de l'UE fournit des services visant à assurer la sécurité de l'UE, de ses États membres et de ses citoyens[126].

Avec plus de 600 projets lancés depuis 2007, à hauteur d'un montant global de près de 3 milliards d'EUR, la recherche en matière de sécurité, qui bénéficie du soutien financier de l'UE, constitue un instrument essentiel dans la promotion de la technologie et des connaissances en faveur de solutions de sécurité. Dans le cadre du réexamen du mandat d'Europol, la Commission se penchera sur la création d'un **pôle d'innovation européen pour la sécurité intérieure**[127], qui serait chargé de définir des solutions conjointes à des défis communs en matière de sécurité et face à des opportunités que les États membres ne peuvent exploiter seuls. Il est crucial de collaborer pour pouvoir tirer le meilleur parti possible des investissements et développer des technologies innovantes offrant un avantage à la fois économique et en matière de sécurité.

Compétences et sensibilisation

La sensibilisation aux aspects sécuritaires et l'acquisition des compétences nécessaires pour faire face aux menaces potentielles sont essentielles pour bâtir une société plus résiliente caractérisée par des entreprises, des administrations et des citoyens mieux préparés. Les difficultés rencontrées par les infrastructures informatiques et les systèmes électroniques ont mis en évidence la nécessité de renforcer notre capital humain en matière de préparation et de riposte dans le domaine de la cybersécurité. La pandémie a également souligné l'importance de la numérisation dans tous les pans de l'économie et de la société de l'Union.

Même une **connaissance de base des menaces pesant sur la sécurité** et de la manière d'y faire face peut avoir une incidence réelle sur la résilience de la société. La conscience des risques liés à la cybercriminalité et la nécessité de s'en protéger peuvent venir renforcer la protection fournie par les prestataires de services pour contrer les cyberattaques. L'information sur les dangers et les risques liés au trafic de stupéfiants peut gêner les criminels. L'UE peut encourager la diffusion des meilleures pratiques, notamment par l'intermédiaire du réseau des centres pour un internet plus sûr[128], et veiller à la prise en compte de ces objectifs dans ses propres programmes.

Le futur plan d'action en matière d'éducation numérique devrait inclure des mesures ciblées visant à renforcer les compétences informatiques de l'ensemble de la population dans le domaine de la sécurité. La stratégie en matière de compétences[129] adoptée récemment encourage le développement des compétences tout au long de la vie. Elle comprend des

[125] Proposition de règlement du Parlement européen et du Conseil du 12 septembre 2018 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.

[126] Le programme Copernicus, par exemple, fournit des services permettant la surveillance des frontières extérieures et la surveillance maritime de l'UE, contribuant à la lutte contre la piraterie et la contrebande et au soutien des infrastructures critiques. Une fois pleinement opérationnel, il s'agira d'un outil essentiel pour les missions et les opérations civiles et militaires.

[127] Ce pôle travaillerait également avec Frontex, CEPOL, eu-LISA et le Centre commun de recherche.

[128] Voir www.betterinternetforkids.eu: le portail central et les centres nationaux pour un internet plus sûr sont actuellement financés au titre du volet «télécommunications» du mécanisme pour l'interconnexion en Europe (MIE), et un financement futur a été proposé au titre du programme pour une Europe numérique.

[129] Stratégie européenne en matière de compétences en faveur de la compétitivité durable, de l'équité sociale et de la résilience, COM(2020) 274 final.

actions spécifiques visant à augmenter le nombre de diplômés en sciences, technologies, ingénierie, arts et mathématiques dans des domaines de pointe tels que la cybersécurité. Des actions supplémentaires, financées au titre du programme pour une Europe numérique, permettront aux professionnels de suivre l'évolution du panorama des menaces pour la sécurité, tout en comblant les lacunes constatées dans ce domaine sur le marché du travail de l'UE. L'objectif général sera de permettre aux citoyens d'acquérir des compétences leur permettant de faire face aux menaces pesant sur la sécurité, et aux entreprises de trouver les professionnels dont ils ont besoin dans ce domaine. Les futurs espaces européens de la recherche et de l'éducation encourageront également les carrières dans les domaines des sciences, des technologies, de l'ingénierie, des arts et des mathématiques.

L'accès des **victimes** à leurs droits est tout aussi important; les victimes doivent bénéficier de l'assistance et du soutien dont elles ont besoin en fonction de de leur situation spécifique. Des efforts particuliers doivent être consentis à l'égard des minorités et des victimes les plus vulnérables, comme les enfants ou les femmes qui sont victimes de la traite à des fins d'exploitation sexuelle ou qui sont exposées aux violences domestiques[130].

Le renforcement des **compétences en matière de répression** joue un rôle particulier. Les menaces technologiques actuelles et nouvelles requièrent davantage d'investissements en faveur du renforcement des compétences des membres des forces de l'ordre, au stade le plus précoce et tout au long de leur carrière. Le CEPOL est un partenaire essentiel des États membres dans cette tâche. La formation des services répressifs dans les domaines du racisme et de la xénophobie et, d'une manière plus générale, des droits des citoyens doit constituer un aspect essentiel d'une culture européenne de la sécurité. Les systèmes judiciaires nationaux et les professionnels de la justice doivent également être dotés de moyens leur permettant de s'adapter et de répondre à des défis sans précédent. La formation est essentielle pour permettre aux autorités sur le terrain d'exploiter ces instruments dans une situation opérationnelle. En outre, il convient de tout mettre en œuvre pour renforcer l'intégration des questions d'égalité entre les hommes et les femmes et accroître la participation des femmes au maintien de l'ordre.

Actions clés
• Renforcement du mandat d'Europol • Étude d'un «code de coopération policière» européen et d'une coordination policière entre les services de police en temps de crise • Consolidation d'Eurojust afin d'assurer un lien entre les autorités judiciaires et les services répressifs • Réexamen de la directive concernant l'information préalable sur les passagers • Communication sur la dimension extérieure des dossiers passagers • Renforcement de la coopération entre l'UE et Interpol • Définition d'un cadre de négociation avec les principaux pays tiers en ce qui concerne le partage d'informations • Amélioration des normes de sécurité applicables aux documents de voyage • Étude d'un pôle d'innovation européen pour la sécurité intérieure

[130] Voir la stratégie en faveur de l'égalité entre les hommes et les femmes, COM(2020) 152; la stratégie de l'UE relative au droit des victimes, COM(2020) 258; et la stratégie européenne pour un Internet mieux adapté aux enfants, COM(2012) 196.

V. Conclusions

Dans un monde de plus en plus instable, l'Union européenne reste largement perçue comme l'un des endroits les plus sûrs . Cela ne peut toutefois être considéré comme un fait acquis.

La nouvelle stratégie sur l'union de la sécurité pose les jalons d'un écosystème de la sécurité qui couvre l'ensemble de la société européenne. Elle repose sur la constatation selon laquelle la sécurité relève de la responsabilité partagée. La question de la sécurité touche tous les citoyens. L'ensemble des administrations publiques, des entreprises, des organisations sociales, des institutions et des citoyens doivent assumer leurs propres responsabilités afin de rendre nos sociétés plus sûres.

Les questions de sécurité doivent à présent être considérées sous un angle beaucoup plus large que par le passé. Il faut surmonter les distinctions erronées établies entre les besoins physiques et les besoins numériques. La stratégie de l'UE sur l'union de la sécurité regroupe l'ensemble des besoins en matière de sécurité et met l'accent sur les domaines qui seront les plus importants pour la sécurité de l'UE dans les années à venir. Elle reconnaît également le fait que les menaces pour la sécurité ne respectent pas les frontières géographiques, de même que l'interconnexion croissante entre la sécurité intérieure et la sécurité extérieure[131]. Dans ce contexte, il importera que l'UE coopère avec ses partenaires internationaux pour protéger l'ensemble de ses citoyens et veille au maintien d'une coordination étroite avec l'action extérieure de l'UE dans le cadre de la mise en œuvre de cette stratégie.

Notre sécurité est liée à nos valeurs fondamentales. Toutes les actions et initiatives proposées dans le cadre de cette stratégie respecteront pleinement les droits fondamentaux et nos valeurs européennes. Ceux-ci constituent le fondement de notre mode de vie européen et doivent rester au centre de tous nos travaux.

Enfin, la Commission demeure pleinement consciente du fait qu'une stratégie ou une action, quelle qu'elle soit, ne vaut jamais que par sa mise en œuvre. Il convient donc d'insister sans relâche sur la mise en application et le respect corrects de la législation européenne existante et future. Ceux-ci feront l'objet de rapports réguliers portant sur l'union de la sécurité, et la Commission informera dûment le Parlement européen, le Conseil et les parties prenantes et les associera à toutes les actions pertinentes. En outre, la Commission est disposée à prendre part à des débats conjoints avec les autres institutions concernant la stratégie pour l'union de la sécurité ou à organiser de tels débats afin de dresser avec elles un état des lieux des progrès accomplis et d'examiner les défis futurs.

La Commission invite le Parlement européen et le Conseil à approuver la stratégie pour l'union de la sécurité, fondement de la coopération et de l'action conjointe en matière de sécurité pour les cinq prochaines années.

[131] Voir la stratégie globale de l'UE