Conseil de
l'Union européenne

**Bruxelles, le 27 mai 2022**
**(OR. en)**

**9563/22**

| | |
|---|---|
| **JAI 761** | **DROIPEN 69** |
| **COSI 149** | **COPEN 210** |
| **ENFOPOL 298** | **FREMP 110** |
| **ENFOCUSTOM 89** | **JAIEX 61** |
| **IXIM 145** | **CFSP/PESC 705** |
| **CT 99** | **COPS 238** |
| **CRIMORG 81** | **HYBRID 49** |
| **FRONT 218** | **DISINFO 47** |
| **ASIM 47** | **TELECOM 248** |
| **VISA 87** | **DIGIT 108** |
| **CYBER 191** | **COMPET 408** |
| **DATAPROTECT 175** | **RECH 307** |
| **CATS 30** | |

**NOTE DE TRANSMISSION**

| | |
|---|---|
| Origine: | Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice |
| Date de réception: | 25 mai 2022 |
| Destinataire: | Secrétariat général du Conseil |
| N° doc. Cion: | COM(2022) 252 final |
| Objet: | COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL relative au quatrième rapport sur l'état d'avancement de la mise en œuvre de la stratégie de l'UE pour l'union de la sécurité |

Les délégations trouveront ci-joint le document COM(2022) 252 final.

p.j.: COM(2022) 252 final

COMMISSION
EUROPÉENNE

Bruxelles, le 25.5.2022
COM(2022) 252 final

# COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

## relative au quatrième rapport sur l'état d'avancement de la mise en œuvre de la stratégie de l'UE pour l'union de la sécurité

# I. INTRODUCTION

La guerre d'agression menée par la Russie contre l'Ukraine domine le programme de sécurité de l'UE d'aujourd'hui. La guerre ne menace pas seulement l'Ukraine. Elle cherche également à porter atteinte à la stabilité et à la sécurité mondiales. Au sein de l'UE, elle entraîne une série de risques pour la sécurité des citoyens. De nouvelles incertitudes quant à l'approvisionnement en énergie et en matières premières se font ressentir, et des infrastructures critiques peuvent être la cible de cyberattaques. La sécurité et la sûreté internes de l'UE sont menacées par les risques d'attaques ou d'accidents chimiques, biologiques ou radiologiques dans la zone de guerre. La criminalité organisée peut rapidement exploiter les vulnérabilités des millions de personnes qui ont fui la guerre, notamment par la traite des femmes et des enfants, qui sont particulièrement exposés.

Face à ces menaces nouvelles et potentielles, l'UE demeure résolue et unie. Bien que, jusqu'à présent, les conséquences de la guerre se soient limitées principalement au territoire ukrainien, l'UE a renforcé *la vigilance et la coordination* grâce à un suivi accru du panorama des menaces et s'est employée à renforcer sa résilience afin de garantir sa *préparation*.

Dans la déclaration de Versailles des 10 et 11 mars 2022[1], les dirigeants européens ont souligné la nécessité de nous préparer aux défis surgissant rapidement, y compris «en nous protégeant contre une guerre hybride qui prend toujours plus d'ampleur, en renforçant notre cyberrésilience, en protégeant nos infrastructures – en particulier nos infrastructures critiques – et en luttant contre la désinformation».

Le cadre de l'union de la sécurité est essentiel au maintien de la sécurité dans l'ensemble de l'Union européenne. Les quatre priorités stratégiques énoncées dans la stratégie pour l'union de la sécurité[2] conservent un lien direct avec cette tâche dans le contexte géopolitique actuel: 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, et iv) un solide écosystème européen de la sécurité. La guerre a mis en évidence la nécessité, pour l'UE et ses États membres, d'exploiter pleinement les instruments législatifs et les instruments d'action déjà disponibles dans le cadre de la stratégie pour l'union de la sécurité, qui sous-tend l'aide coordonnée qu'apporte l'UE aux États membres sur des questions allant de la criminalité organisée et du terrorisme à la cybersécurité et aux menaces hybrides.

Les agences européennes dans le domaine de la justice et des affaires intérieures ont elles aussi intensifié leurs efforts en réaction à la guerre en Ukraine et jouent un rôle clé dans l'évaluation des menaces et dans l'appui des réponses opérationnelles[3]. Le renforcement continu de la pratique et de la gouvernance opérationnelles de l'espace Schengen constitue un autre facteur important.

Ce quatrième rapport sur l'état d'avancement de la stratégie de l'UE pour l'union de la sécurité se concentre sur les évolutions observées au cours des derniers mois, depuis le début de la guerre d'agression menée par la Russie contre l'Ukraine. Il donne un aperçu des mesures prises pour tous les volets de l'union de la sécurité et examine les besoins de préparation aux menaces pour la sécurité qui pourraient découler de la guerre en Ukraine.

---

1 https://www.consilium.europa.eu/media/54777/20220311-versailles-declaration-fr.pdf

2 COM(2020) 605.

3 Déclaration conjointe des agences de l'UE chargées de la justice et des affaires intérieures au sujet de la situation en Ukraine | Agence de l'Union européenne pour l'asile (europa.eu)

L'état d'avancement des autres dossiers relatifs à l'union de la sécurité est indiqué dans l'annexe.

## II. CYBERSÉCURITÉ ET INFRASTRUCTURES CRITIQUES

Depuis que la guerre a éclaté, des acteurs privés et des organisations criminelles ont fait savoir qu'ils menaient des cyberactivités en faveur de l'un des deux camps. L'hacktivisme[4] constitue une menace en raison du risque de retombées négatives dans l'UE sur des services critiques, du risque d'attaques provenant de réseaux officiels ou d'autres répercussions imprévues. Bien que, jusqu'à présent, la guerre ait été, pour l'essentiel, menée par des moyens conventionnels et que les retombées aient été limitées, le risque d'escalade dans ce domaine est réel.

L'UE a donc renforcé sa coordination et sa préparation. Les menaces qui découlent de la guerre soulignent la nécessité de mettre en place une culture du partage de l'information et de l'expertise entre l'UE, ses États membres et les communautés de cybersécurité. Il s'agit notamment d'acquérir une connaissance intégrée de la situation, partagée par les institutions, organes et organismes de l'UE et par les États membres, en particulier en ce qui concerne les infrastructures critiques dont dépend le bon fonctionnement du marché intérieur.

**Imputation des cyberattaques menées contre l'Ukraine**

Les cyberattaques menées contre l'Ukraine ont commencé avant l'agression russe et ont, lors des premiers jours de la guerre[5], cherché à compromettre les comptes d'utilisateurs de membres de l'armée ukrainienne et à perturber les services essentiels, y compris le contrôle des frontières et les télécommunications.

Le 14 janvier 2022, dans une déclaration[6] au nom de l'Union européenne, le haut représentant a condamné les cyberattaques menées contre l'Ukraine et a réaffirmé le soutien sans équivoque de l'UE à cette dernière.

Le 10 mai dernier, l'Union européenne et ses États membres, ainsi que ses partenaires internationaux, ont fermement condamné[7] les actes de cybermalveillance commis contre l'Ukraine le 24 février, qui ciblaient le réseau satellitaire KA-SAT, propriété de Viasat, et ont directement imputé cette attaque à la Fédération de Russie. Les répercussions de cette cyberattaque ont été considérables, puisque plusieurs autorités publiques, entreprises et

[4] Un exemple récent d'«hacktivisme» est l'utilisation d'un «protestware» pour diffuser des logiciels malveillants à des adresses IP russes au moyen d'un paquet open source populaire, ce qui pourrait menacer la chaîne d'approvisionnement et entraîner une perte de confiance au sein de la communauté de l'open source. La Commission a clairement fait savoir que les cyberattaques (même celles dont les intentions sont louables) menées contre la Russie sont illégales.

[5] Rapport spécial de Microsoft: An overview of Russia's cyberattack activity in Ukraine; The hybrid war in Ukraine - Microsoft On the Issues

[6] https://www.consilium.europa.eu/fr/press/press-releases/2022/01/14/ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union-on-the-cyberattack-against-ukraine/

[7] Cyberopérations russes contre l'Ukraine: Déclaration du haut représentant au nom de l'Union européenne - Consilium (europa.eu)

utilisateurs en Ukraine ont vu leurs communications systématiquement interrompues et perturbées, et que plusieurs États membres de l'UE ont été touchés.

### *Vigilance et coordination*

Depuis le début de la guerre d'agression menée par la Russie contre l'Ukraine, le suivi de la situation en matière de cybersécurité dans les États membres et dans les institutions de l'UE a été renforcé. L'Agence de l'Union européenne pour la cybersécurité (ENISA), le Centre européen de lutte contre la cybercriminalité d'Europol, l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'Union européenne (CERT-EU) et le Centre de situation et du renseignement de l'UE (INTCEN) ont tous contribué à une connaissance partagée de la situation de l'UE, y compris en assurant un suivi régulier des cyberactivités suspectes, notamment dans des secteurs spécifiques tels que l'énergie, les transports et l'aviation. Tous ont fourni des évaluations pour orienter les actions préventives.

Une coordination et des échanges d'informations accrus ont eu lieu avec des réseaux de cybersécurité tels que le réseau européen pour la préparation et la gestion des crises cyber (CyCLONe), qui regroupe des agences nationales chargées de la cybersécurité, de la Commission et de l'ENISA. Reproduisant cette démarche en interne, au sein des institutions de l'UE, un mécanisme de coordination, la task force chargée des crises cyber, permet de partager des informations entre tous les services, organes et organismes concernés, y compris l'ENISA, le Centre européen de lutte contre la cybercriminalité d'Europol et la CERT-EU. Des efforts constants sont nécessaires pour garantir la présence de canaux de communication entre les niveaux politique, opérationnel et technique, ainsi que pour renforcer la coopération avec le réseau des centres de réponse aux incidents de sécurité informatiques (CSIRT).

Europol a également déclenché le protocole de réaction d'urgence des services répressifs de l'UE, qui permet un suivi renforcé des cybermenaces et un partage d'informations entre un large éventail de parties prenantes afin de dresser un tableau complet du cyber-renseignement.

Au-delà des cybermenaces, les États membres, le SEAE et la Commission font preuve d'une vigilance accrue en ce qui concerne l'exposition des infrastructures critiques aux menaces physiques, non informatiques. Les infrastructures critiques et les entités qui les exploitent peuvent être exposées à des risques physiques, tels que le sabotage par des acteurs étatiques ou soutenus par un État dans le cadre d'éventuelles mesures de représailles contre l'UE.

### *Préparation*

La préparation dans le domaine de la cybersécurité et de la sécurité des infrastructures critiques n'a jamais été aussi essentielle, compte tenu de l'exposition accrue de l'Europe à une multiplication des menaces découlant de la guerre. Les efforts visant à renforcer la préparation ont comporté un certain nombre d'actions directes, dont certaines étaient déjà prévues avant l'agression de la Russie contre l'Ukraine. Il s'agit notamment d'exercices, d'orientations, de mesures législatives, d'un renforcement de la résilience dans des secteurs critiques et d'une collaboration avec les partenaires.

La présidence française du Conseil de l'Union européenne a organisé avec le SEAE et l'ENISA, début 2022, un exercice fondé sur des scénarios intitulé «EU Cycles» (Cyber Crisis Linking Exercise on Solidarity), dont l'objectif était de sensibiliser les acteurs politiques et de renforcer la coopération entre les niveaux politique et opérationnel en cas de cyberattaque de grande ampleur.

L'ENISA et la CERT-UE ont publié en février des **lignes directrices** sur la manière de renforcer la résilience et la préparation dans l'UE[8]. Ces dernières encouragent toutes les organisations des secteurs public et privé de l'UE à adopter un ensemble minimal de bonnes pratiques en matière de cybersécurité afin d'améliorer sensiblement la culture de la cybersécurité. En mars dernier, la CERT-EU a publié des orientations techniques de suivi, avec l'aide de l'ENISA[9], ainsi que des orientations en matière de sécurité pour renforcer la configuration des applications Signal[10]. Elle a aussi publié un certain nombre de recommandations pratiques destinées aux organisations afin que celles-ci améliorent leur posture de cybersécurité.

*Initiatives législatives*

La situation actuelle souligne à quel point il est urgent de **mettre en œuvre la législation existante** et d'accélérer l'**adoption des initiatives en suspens**.

La Commission aide les États membres à mettre en œuvre la **directive relative aux réseaux et aux systèmes d'information (SRI)**[11], qui exige que les États membres disposent de moyens suffisants, notamment de centres de réponse aux incidents de sécurité informatique (CSIRT) ainsi que d'autorités compétentes. Cette directive constitue un socle de coopération efficace entre les États membres. L'accord politique auquel sont parvenus les colégislateurs en ce qui concerne la **directive SRI 2**[12] est une avancée supplémentaire dans la mise en place d'un cadre solide de préparation de à l'échelle de l'UE.

**SRI 2 — poursuite du renforcement de la préparation**

- La nouvelle directive SRI remédiera aux lacunes de la précédente directive SRI, afin de l'adapter aux besoins actuels et de la rendre pérenne. Elle énonce des règles minimales pour un cadre réglementaire et établit des mécanismes pour une coopération efficace entre les autorités concernées dans chaque État membre.
- Elle élargit le champ d'application des règles et y inclut de nouveaux secteurs essentiels pour l'économie et la société (par exemple le secteur pharmaceutique et celui des dispositifs médicaux ou encore celui de la production de denrées alimentaires). Toutes les entités de taille moyenne et de grande taille qui sont actives dans les secteurs couverts ou qui fournissent des services couverts par la directive relèveront de son champ d'application. Les entités de l'administration publique des gouvernements centraux (à l'exception du pouvoir judiciaire, des parlements et des banques centrales) et régionaux

[8] Boosting your Organisation's Cyber Resilience — Joint Publication, 14.02.2022.
[9] Security Guidance 2022-01 — Cybersecurity mitigation measures against critical threats.
[10] CERT-EU Security Guidance 22-002 - Hardening Signal.
[11] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.
[12] COM(2020) 823.

sont également couvertes. De plus, les États membres peuvent décider d'appliquer la directive à ces entités au niveau local.

- La SRI 2 établira les valeurs de référence pour les mesures de gestion des risques en matière de cybersécurité et instaurera officiellement le réseau européen pour la préparation et la gestion des crises cyber (UE-CyCLONe), qui soutiendra la gestion coordonnée des incidents de cybersécurité de grande ampleur.
- La proposition introduit également des dispositions plus précises au sujet du processus de signalement des incidents, du contenu des signalements et des délais, et prévoit des voies de recours et des sanctions pour garantir le respect des dispositions.
- Les États membres disposeront d'un délai de 21 mois à compter de l'entrée entrée en vigueur de la directive pour transposer ces dispositions dans leur droit national.

Les progrès réalisés en ce qui concerne la SRI 2 devraient être suivis dès que possible par l'achèvement des négociations relatives à la proposition de **directive sur la résilience des entités critiques**[13] («directive CER»), qui, une fois adoptée et mise en œuvre, devrait accroître la résilience des entités critiques face à toute une série de menaces telles que les attentats terroristes, les menaces internes et les actes de sabotage. Il est également essentiel que la directive sur la résilience des entités critiques soit aussi ambitieuse que la proposition de la Commission, et que la cohérence avec le compromis politique incarné par la SRI 2 soit maintenue. Ensemble, ces mesures renforceront la résilience et la préparation en mettant en place un système plus cohérent et plus robuste, notamment grâce aux plans nationaux d'intervention en cas d'incident et de crise. Elles faisaient d'ailleurs partie de la recommandation de la Commission de l'année dernière[14] sur la création de **l'unité conjointe de cybersécurité**, qui définit la manière dont les différents acteurs de l'écosystème de la cybersécurité (dans les domaines de la diplomatie, de la police, de la société civile et, s'il y a lieu, de la défense) doivent coopérer au niveau opérationnel. Le panorama actuel des menaces met en évidence la valeur d'une telle coopération efficace entre les acteurs clés.

La Commission continue de suivre la mise en œuvre de la boîte à outils de l'UE pour la sécurité des réseaux **5G**[15]. C'est dans ce contexte que, le 11 mai dernier, le groupe de coopération SRI a adopté un rapport sur la sécurité de l'OpenRAN[16]. Le groupe continue par ailleurs de travailler aux côtés des États membres pour rendre le Centre de compétences européen en matière de cybersécurité pleinement opérationnel.

Le 22 mars 2022, la Commission a proposé de **nouvelles règles visant à établir des mesures communes en matière de cybersécurité et de sécurité de l'information dans les institutions, organes et organismes de l'UE.** Ces règles renforceront la résilience et la capacité de réaction de l'administration de l'UE face aux menaces et incidents de cybersécurité. Grâce à l'intégration de ces activités dans un cadre commun, la coopération interinstitutionnelle sera renforcée et l'exposition aux risques réduite autant que possible. La proposition de **règlement sur la cybersécurité dans les institutions, organes et organismes**

[13] COM(2020) 829.
[14] Recommandation sur la création d'une unité conjointe de cybersécurité | Façonner l'avenir numérique de l'Europe (europa.eu)
[15] https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures
[16] Groupe de coopération SRI, rapport sur la cybersécurité de l'OPEN RAN, 11 mai 2022.

**de l'UE**[17] élargira le mandat de la CERT-UE, conduira à la création d'un nouveau conseil interinstitutionnel de cybersécurité, renforcera les capacités en matière de cybersécurité, encouragera la conduite régulière d'évaluations de la maturité et favorisera une meilleure hygiène informatique. La proposition de **règlement sur la sécurité de l'information**[18] créera un ensemble minimal de normes et de règles en matière de sécurité de l'information pour le traitement et l'échange sécurisés d'informations de l'ensemble des institutions, organes et organismes de l'UE afin d'assurer une protection renforcée et cohérente contre les menaces en constante évolution qui pèsent sur leurs informations. La Commission invite à présent le Parlement européen et le Conseil à adopter rapidement ces mesures.

La Commission a clôturé sa consultation publique sur les mesures visant à renforcer la **cyberrésilience** des produits numériques, en vue d'une proposition qui sera publiée cet automne[19]. Cette proposition traitera des vulnérabilités des produits numériques et des services accessoires qui, bien qu'ils élargissent le champ des possibles pour les économies de l'UE, posent aussi de nouveaux défis. En effet, plus le monde est interconnecté, plus les incidents de cybersécurité sont susceptibles de gripper un système entier et donc de perturber les activités économiques et sociales.

Le 9 mars 2022, les ministres des télécommunications de l'UE ont adopté à l'unanimité l'appel de Nevers à renforcer les capacités de l'UE en matière de cybersécurité, qui comprenait la «mise en œuvre d'un nouveau Fonds d'intervention d'urgence pour la cybersécurité qui sera mis en place par la Commission»[20]. La Commission réfléchit à la meilleure utilisation possible des fonds existants pour soutenir les actions de prévention et de réaction.

*Secteurs critiques*

La sécurité de l'**approvisionnement énergétique** de l'UE est essentielle au bien-être des citoyens et au bon fonctionnement de nos économies. La situation actuelle a mis en évidence le besoin d'établir des règles claires en matière de cybersécurité dans ce secteur. La Commission travaille actuellement à l'élaboration d'un code de réseau sur la cybersécurité des flux transfrontaliers d'électricité, comme l'exige le règlement sur l'électricité[21], afin de définir des règles sur l'évaluation des risques, sur les exigences minimales communes, la planification, la surveillance, les rapports et la gestion de crise. Depuis le début de l'agression menée par la Russie contre l'Ukraine, les objectifs prévus pour le code de réseau sur la cybersécurité sont encore plus pertinents. La Commission a aussi lancé une coopération structurelle entre l'ENISA, le REGRT-E[22], le REGRT pour le gaz[23] et la Communauté de

[17] COM(2022) 122.
[18] COM(2022) 119.
[19] Législation sur la cyberrésilience – nouvelles règles en matière de cybersécurité concernant les produits numériques et les services accessoires (europa.eu)
[20] 08/03/2022 - Déclaration conjointe des ministres de l'Union européenne chargés du numérique et des communications électroniques adressée au secteur numérique - Presse - Ministère des Finances (economie.gouv.fr)
[21] Règlement (UE) 2019/943 du Parlement européen et du Conseil du 5 juin 2019 sur le marché intérieur de l'électricité, JO L 158 du 14.6.2019, p. 54. Une proposition est en cours d'examen par l'Agence de coopération des régulateurs de l'énergie.
[22] Réseau européen des gestionnaires de réseaux de transport d'électricité.
[23] Réseau européen des gestionnaires de réseau de transport pour le gaz.

l'énergie pour le suivi régulier de la situation en matière de cybersécurité dans le secteur de l'énergie.

L'UE œuvre à protéger la sécurité de ses partenaires, tout en évitant de s'exposer à de nouveaux risques. La synchronisation d'urgence des réseaux électriques de l'Ukraine et de la Moldavie avec le réseau d'Europe continentale a eu lieu en mars 2022, après l'adoption de mesures d'atténuation des risques, notamment en matière de cybersécurité.

La guerre et les sanctions ont créé de nombreux défis pour les **transports** de l'UE, parmi lesquels les risques pour la sécurité de l'aviation civile de l'UE et des conducteurs de camions bloqués dans les zones de conflit, la destruction des infrastructures de transport ukrainiennes, la rupture des chaînes d'approvisionnement et la menace pour la sécurité alimentaire mondiale. L'Agence de l'Union européenne pour la sécurité aérienne, en étroite collaboration avec la Commission et Eurocontrol, l'Organisation européenne pour la sécurité de la navigation aérienne, conseillent depuis le début de la guerre aux opérateurs de ne pas emprunter l'espace aérien ukrainien et d'éviter l'espace aérien situé à moins de 100 milles marins des frontières de l'Ukraine avec la Biélorussie et la Russie.

La Commission œuvre aussi au renforcement de la préparation et de la résilience du secteur des transports de l'UE. En particulier, un nouveau plan d'urgence pour les transports[24], adopté le 23 mai, tire les enseignements de la pandémie de COVID-19 et de l'agression militaire menée par la Russie contre l'Ukraine. Ce plan propose une boîte à outils comprenant 10 actions destinées à guider l'UE et ses États membres lorsqu'ils mettent en place des mesures d'urgence pour faire face à une crise, notamment des actions visant à garantir une connectivité minimale, à renforcer la résilience face aux cybermenaces et aux menaces hybrides et à améliorer la coopération avec les partenaires internationaux en matière de préparation et de réaction aux crises. Il souligne aussi l'importance de procéder régulièrement à des tests de résilience fondés sur différents scénarios de crise, en réunissant les agences compétentes de l'UE ou d'autres acteurs et en s'appuyant sur les processus existants.

Dans le **cadre de l'UE en matière de sécurité alimentaire**, les échanges d'informations sur la base du système d'alerte précoce et de réaction, y compris ceux concernant l'aide apportée aux évacuations médicales depuis l'Ukraine, doivent être protégés contre les cyberattaques. La sécurité du système est par conséquent en train d'être renforcée.

*Coopération avec les partenaires*

L'UE continue de collaborer avec ses partenaires internationaux pour prévenir, décourager et empêcher les actes malveillants dans le cyberespace. La guerre d'agression menée par la Russie contre l'Ukraine a rendu la coopération dans ce domaine plus importante que jamais. À cet égard, le SEAE travaille à l'échange d'informations sur la connaissance de la situation et à la coordination de la réaction aux actes de cybermalveillance ciblant l'Ukraine, ainsi qu'au soutien à l'Ukraine et aux autres acteurs de la région, en collaborant avec des partenaires, dont les États-Unis et l'OTAN, pour assurer la complémentarité et éviter les chevauchements.

La coopération étroite avec les États-Unis s'est également intensifiée dans le cadre du Conseil du commerce et des technologies UE-États-Unis (CCT). La déclaration commune[25]

[24] COM(2022) 21.

[25] https://ec.europa.eu/commission/presscorner/detail/fr/STATEMENT_22_3108

au terme de la réunion ministérielle qui s'est tenue à Paris en mai a mis en évidence le rôle central du CCT dans le partenariat transatlantique renouvelé, lequel permet de coordonner des mesures conjointes entre l'UE et les États-Unis face à l'agression russe contre l'Ukraine. Les deux parties sont convenues qu'une coopération étroite visant à renforcer la résilience des chaînes d'approvisionnement était plus importante que jamais. En outre, un groupe de travail spécial sur le financement public d'infrastructures numériques sûres et résilientes dans les pays tiers a été créé pour ouvrir la voie au financement public conjoint, par les États-Unis et l'UE, de projets numériques dans les pays tiers, sur la base d'un ensemble de principes généraux communs.

La boussole stratégique adoptée en mars 2022 (voir la section VII) renforcera encore la boîte à outils cyberdiplomatique de l'UE et la politique de l'UE en matière de cyberdéfense afin d'améliorer la préparation et la réaction aux cyberattaques, dans le cadre d'une stratégie plus large visant à renforcer la capacité de l'UE à agir en cas de crise et à défendre ses intérêts.

**Soutien à l'Ukraine et aux pays voisins en matière de cybersécurité**

L'UE soutenait déjà la cyberrésilience de l'Ukraine avant la guerre. Dès juin 2021, l'UE et l'Ukraine ont tenu un premier dialogue sur le cyberespace, et l'UE a fourni à ce pays une aide à la cybersécurité et à la transformation numérique résiliente par l'intermédiaire du programme EU4Digital pour l'Ukraine, pour un montant de 25 000 000 EUR. Un autre programme de jumelage doté de 1 500 000 EUR est conçu pour aider les institutions ukrainiennes chargées de la cybersécurité à s'aligner sur les normes de l'UE.

Depuis le déclenchement de la guerre, l'UE encourage la coopération entre les experts informatiques de l'UE et ukrainiens et coordonne la fourniture d'une assistance technique, d'équipements, de logiciels et de services pertinents, afin de renforcer la cyberrésilience et la cyberdéfense de l'Ukraine.

En outre, l'UE examine la possibilité d'un soutien à moyen terme à la Moldavie, à la Géorgie et aux Balkans occidentaux. Une mission d'évaluation conjointe sur les besoins en matière de cybersécurité a été effectuée en Moldavie les 3 et 4 mars 2022 et a conduit à l'adoption d'une mesure spécifique de réaction à la crise visant à renforcer rapidement la cybersécurité dans le pays. Une aide à la réaction rapide similaire est en cours d'élaboration pour un certain nombre de pays des Balkans occidentaux, considérés comme particulièrement exposés au risque du fait de leur alignement sur les sanctions de l'UE. Une éventuelle assistance supplémentaire à la Moldavie par l'intermédiaire de la facilité européenne pour la paix est également à l'étude.

## III. CRIMINALITÉ ORGANISÉE ET TERRORISME

La guerre d'agression menée par la Russie contre l'Ukraine a forcé des millions de personnes à quitter leur foyer, ce qui a fortement accru le nombre de déplacements aux frontières extérieures de l'UE. Au 18 mai, près de 6 millions de personnes étaient arrivées dans l'UE depuis l'Ukraine et la Moldavie, et à ce jour, 2,8 millions de personnes sont enregistrées pour bénéficier d'une protection temporaire dans l'UE. L'UE a cherché à réserver l'accueil le plus rapide et le plus souple possible aux personnes fuyant la guerre, sans compromettre la sécurité à ses frontières extérieures. Elle a pris des mesures sans précédent pour offrir une protection temporaire à ceux qui fuient la guerre et est déterminée à traiter tous les nouveaux arrivants sans discrimination. Dans le même temps, les risques potentiels susceptibles de

découler du déplacement d'un si grand nombre de personnes ne peuvent être négligés, et l'UE, bien aidée par les agences compétentes de l'Union, reste vigilante quant aux nouvelles évolutions en matière de criminalité organisée et de terrorisme.

**Un espace Schengen fort à l'heure de l'accroissement des menaces**

Il n'a jamais été aussi important d'assurer un niveau élevé de sécurité dans l'espace **Schengen** et au sein de l'UE que dans le contexte de l'accroissement des menaces liées à la guerre qui se déroule juste au-delà des frontières extérieures de l'UE.

Conformément au programme ambitieux pour l'espace Schengen défini dans la stratégie de juin 2021, la Commission a adopté en mai le premier rapport sur la situation dans l'espace Schengen[26]. Le cycle annuel de Schengen fournit un nouveau modèle de gouvernance pour l'espace Schengen, avec un bilan de santé régulier de l'espace Schengen. Cela contribuera à une détection rapide des manquements et à des procédures de suivi efficaces, afin de rendre l'espace Schengen plus fort et plus résilient.

Ce premier rapport reconnaît la nécessité de redoubler d'efforts pour mettre en œuvre des initiatives clés au niveau de l'UE, y compris des contrôles systématiques de tous les voyageurs aux frontières extérieures, en tirant pleinement parti des mandats de Frontex et d'Europol, ainsi que des outils de coopération policière transfrontière proposés et disponibles.

En particulier, la nouvelle architecture des systèmes d'information de l'UE pour les frontières, les migrations et la sécurité ainsi que l'interopérabilité de ces systèmes sont la pierre angulaire des efforts visant à améliorer la sécurité intérieure et la gestion des frontières. Une mise en œuvre effective de tous les éléments du cadre d'interopérabilité conformément aux calendriers convenus sera essentielle.

### *Vigilance et coordination*

Une coopération accrue en matière de répression entre les États membres et avec les pays tiers est essentielle pour faire en sorte que les menaces criminelles et terroristes émergentes soient connues, et pour agir contre les réseaux criminels et les individus qui pourraient essayer de tirer profit de la guerre contre l'Ukraine. Les États membres et les partenaires opérationnels échangent activement les informations et les renseignements criminels pertinents disponibles avec Europol, qui recoupe et analyse les informations et les transforme en notifications de renseignements opérationnels exploitables, comme les avis d'alerte précoce et les évaluations de la menace, qui sont partagées avec les partenaires.

*Criminalité organisée*

La criminalité organisée trouve déjà des moyens d'exploiter la situation actuelle. L'analyse initiale des renseignements a permis de déceler des schémas criminels dans plusieurs domaines, notamment la traite des êtres humains, les fausses déclarations de marchandises

[26] COM(2022) 301.

importées et exportées, la fraude en ligne, la cybercriminalité et le trafic d'armes à feu. Certains éléments indiquent que des cybercriminels se font passer pour des collecteurs de fonds pour l'Ukraine afin de voler de l'argent et des cryptomonnaies[27]. Des organisations criminelles ukrainiennes pourraient essayer de se déplacer en raison de la situation actuelle et de poursuivre leurs activités dans l'UE.

La Commission et la présidence française du Conseil ont travaillé ensemble, ainsi qu'avec les agences JAI de l'UE, dont Europol, pour mobiliser la plateforme pluridisciplinaire européenne contre les menaces criminelles (**EMPACT**), afin d'évaluer, de prévoir, de prévenir et de contrer les menaces existantes ou émergentes que représente la grande criminalité organisée. Le 7 avril 2022, Europol a accueilli une réunion de l'EMPACT, à laquelle ont participé des représentants et des experts des États membres de l'UE et de la communauté de la sécurité de l'UE, afin de se pencher sur les menaces liées à la grande criminalité organisée qui ont émergé en raison de la guerre en Ukraine. Parmi les mesures concrètes examinées figurent la collecte accrue de renseignements, la mise en œuvre d'actions opérationnelles d'urgence et le recentrage de celles existantes, ainsi que des journées d'action conjointe ad hoc.

L'équipe d'experts douaniers de la frontière terrestre est et sud-est (**CELBET**), un projet collaboratif financé par la Commission européenne, suit l'évolution de la situation à la frontière dans le cadre de sa mission consistant à fournir un soutien opérationnel et des orientations aux agents des douanes et contrôle les saisies douanières aux points de passage frontaliers entre l'UE (Pologne, Slovaquie, Hongrie et Roumanie) et l'Ukraine.

*Activités criminelles et terroristes*

Bien qu'aucune menace terroriste immédiate ne se soit encore manifestée dans l'UE en lien avec l'invasion russe de l'Ukraine, il est à l'évidence nécessaire de faire preuve de vigilance.

Les risques accrus d'activités criminelles et terroristes soulignent l'importance pour les États membres d'avoir recours aux bases de données pertinentes de l'UE, comme le système d'information Schengen, d'y encoder des données si nécessaire et de les consulter lors des contrôles des personnes entrant dans l'UE. Cela contribuera à l'identification, aux frontières extérieures, des personnes qui représentent une menace pour la sécurité intérieure de l'UE. L'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA) continue de garantir la disponibilité absolue et l'efficacité des systèmes de gestion des frontières de l'UE. Les orientations[28] destinées aux États membres expliquent comment trouver un équilibre entre la nécessité d'assurer un traitement fluide des arrivées aux frontières extérieures et la poursuite des contrôles de sécurité nécessaires.

[27] Le groupe d'analyse des menaces de Google a observé un nombre croissant d'acteurs représentant une menace, qui utilisent la guerre en Ukraine comme un leurre dans leurs campagnes d'hameçonnage et de diffusion de logiciels malveillants. Les chercheurs de la société de sécurité internet Cyren font état d'une augmentation du nombre d'escroqueries aux cryptomonnaies tirant parti du conflit grâce à l'utilisation de faux sites web de dons.

[28] Communication de la Commission fournissant des lignes directrices opérationnelles pour la gestion des frontières extérieures afin de faciliter le franchissement des frontières entre l'UE et l'Ukraine (2022/C 104 I/01).

***Préparation***

En plus des orientations et de la coordination, la préparation de l'UE a été renforcée par le déploiement du personnel des agences de l'UE.

**Europol** a déployé des équipes opérationnelles dans les États membres voisins de l'Ukraine. Ces équipes étaient composées d'agents invités d'Europol provenant des États membres et d'experts d'Europol, déployés en Hongrie, en Lituanie, en Pologne, en Roumanie et en Slovaquie, ainsi qu'en Moldavie[29]. Les agents invités d'Europol aident les autorités nationales à effectuer des contrôles de sécurité de deuxième ligne aux frontières extérieures de l'UE. Les experts d'Europol apportent leur soutien en collectant et en évaluant des informations en vue de détecter des menaces terroristes et criminelles, d'appuyer les enquêtes et d'identifier les individus représentant un risque en tentant d'entrer dans l'UE. Ces équipes opérationnelles collectent des informations destinées à alimenter les évaluations de la menace criminelle qui sont à la disposition des États membres. Une telle activité de collecte de renseignements permet à Europol d'anticiper l'évolution de la situation et de coordonner les activités opérationnelles avec les États membres de l'UE en réaction aux activités de groupes criminels cherchant à tirer parti de la guerre en Ukraine, et de s'appuyer sur son dialogue actif avec les services répressifs ukrainiens par l'intermédiaire de l'officier de liaison ukrainien présent au siège d'Europol aux Pays-Bas.

L'**Agence européenne de garde-frontières et de garde-côtes** (**Frontex**) est également présente dans les États membres et les pays voisins de l'UE pour soutenir les opérations de contrôle aux frontières: plus de 2 100 garde-frontières sont actuellement déployés dans l'ensemble de l'UE, dans les Balkans occidentaux et en Moldavie. **L'Agence de l'Union européenne pour l'asile (EUAA)** a déployé près de 750 membres du personnel dans les États membres méridionaux de l'UE et en Lituanie afin de soutenir les activités opérationnelles, de renforcer les capacités d'accueil et d'apporter une aide dans les procédures d'asile.

Sur la base de l'actuelle **décision Prüm**[30], qui prévoit un cadre permettant aux États membres de déployer des agents des services répressifs pour des opérations conjointes comme des patrouilles communes, la Commission et la présidence française du Conseil de l'Union européenne ont adressé une lettre conjointe à tous les États membres en vue de recenser les besoins et de demander le déploiement d'agents de police, afin de lancer des patrouilles communes dans les États membres de première ligne de l'UE les plus touchés par les franchissements en masse de frontières résultant de la guerre. La Commission financera ces déploiements par l'intermédiaire du Fonds pour la sécurité intérieure – Police.

**Lutte contre la traite des êtres humains**

L'UE est en alerte depuis les premiers jours de la guerre en ce qui concerne les risques liés à un domaine particulier d'activité criminelle qui pourrait bénéficier des mouvements massifs de personnes cherchant à se mettre en sécurité dans l'UE. Il est essentiel d'empêcher les trafiquants d'êtres humains de cibler les personnes vulnérables en déplacement, qui sont

[29] Au 3 mai, Europol avait déployé un de ses agents et 3 agents invités en Slovaquie, un de ses agents en Pologne, un de ses agents et 4 agents invités en Roumanie, et 2 agents invités en Hongrie. Un agent d'Europol et 2 agents invités sont déployés en Moldavie.

[30] 2008/615/JAI, 2008/616/JAI.

principalement des **femmes et des enfants**, en utilisant, par exemple, de fausses offres de transport ou de logement.

En mars, Europol et Eurojust ont adressé des avis d'alerte précoce aux autorités nationales compétentes concernant la traite potentielle d'êtres humains et l'exploitation des victimes en provenance d'Ukraine. Eurojust contribue à améliorer l'échange d'informations et à accélérer la coopération judiciaire, notamment avec l'Ukraine, et des enquêtes sur la traite des êtres humains ont été renvoyées à l'agence à des fins de coordination.

Le coordinateur de l'UE pour la lutte contre la traite des êtres humains a tenu des réunions avec le réseau européen de rapporteurs nationaux ou de mécanismes équivalents, les agences chargées de la justice et des affaires intérieures et la plateforme de la société civile de l'UE pour la lutte contre la traite des êtres humains afin d'échanger sur les mesures nécessaires pour prévenir et combattre les abus et protéger les victimes. Des enquêtes ont été ouvertes dans plusieurs États membres sur les cas potentiels.

L'UE a été rapide et dynamique pour apporter une réponse coordonnée à cette menace réelle pour les personnes ayant besoin de son aide. Des lignes directrices opérationnelles[31], notamment sur la question de la traite des êtres humains, ont été rapidement proposées aux États membres mettant en œuvre la directive relative à la protection temporaire des personnes fuyant la guerre en Ukraine. Dans le cadre du plan en dix points pour une coordination européenne plus étroite en matière d'accueil des personnes fuyant la guerre en Ukraine[32], présenté lors du Conseil «Justice et affaires intérieures» du 28 mars 2022, un plan commun de lutte contre la traite des êtres humains[33] visant à prévenir la traite des êtres humains et à aider les victimes a été élaboré par le coordinateur de l'UE pour la lutte contre la traite des êtres humains en coopération avec les agences de l'UE et les États membres. L'accent est placé en particulier sur l'enregistrement des entités et des personnes (y compris les volontaires) qui souhaitent fournir un hébergement, un transport et d'autres types d'assistance, ainsi que sur la vérification des antécédents. La Commission a également établi des contacts avec l'EUAA afin de soutenir la détection des victimes de la traite des êtres humains lorsque des évaluations de santé sont prévues dans les centres d'accueil. Les enfants non accompagnés ou séparés sont particulièrement exposés au risque d'abus, d'exploitation sexuelle ou de criminalité forcée. Les lignes directrices opérationnelles susmentionnées fournissent également des orientations pour aider les États membres à gérer l'arrivée, l'accueil et le soutien des enfants, et en particulier des mineurs non accompagnés. Afin de sensibiliser les personnes à risque, la Commission a également lancé un site web spécifique comportant une section dans laquelle figurent des conseils pratiques sur la manière d'éviter les trafiquants.

Si certaines mesures visant à renforcer la préparation ont été prises spécifiquement en réaction aux nouvelles conditions résultant de la guerre, d'autres mesures clés découlent d'**initiatives législatives** qui étaient déjà en préparation avant la guerre d'agression menée par la Russie contre l'Ukraine.

[31] C/2022/1806, EUR-Lex - 52022XC0321(03) - FR - EUR-Lex (europa.eu).

[32] https://ec.europa.eu/home-affairs/10-point-plan-stronger-european-coordination-welcoming-people-fleeing-war-ukraine_en

[33] https://ec.europa.eu/home-affairs/news/new-anti-trafficking-plan-protect-people-fleeing-war-ukraine-2022-05-11_en

La Commission salue l'accord de février 2022 sur le mandat révisé d'**Europol**[34], qui, une fois mis en œuvre, permettra à cette dernière de mieux soutenir les États membres dans la lutte contre la criminalité organisée et le terrorisme. L'agence disposera alors des garanties et outils adéquats pour aider les forces de police à analyser les mégadonnées afin d'enquêter sur la criminalité et à mettre au point des méthodes novatrices pour lutter contre la cybercriminalité. a d'un renforcement du cadre de protection des données ainsi que du contrôle parlementaire et de la responsabilité.

Le paquet sur la **coopération policière** présenté par la Commission le 8 décembre 2021[35] et actuellement en cours de négociation renforcera la coopération entre les agents des services répressifs dans les États membres en rendant l'échange de données plus rapide, plus facile et plus sûr, ainsi qu'en renforçant et en rendant plus efficace la coopération policière opérationnelle sur le terrain. La Commission invite le Parlement européen et le Conseil à adopter rapidement ce paquet.

Une fois adoptées et mises en œuvre, ces propositions législatives soutiendront les services répressifs dans la lutte contre la criminalité organisée transfrontière. Cela sera particulièrement important dans un contexte où des organisations criminelles ukrainiennes pourraient essayer de se déplacer en raison de la situation actuelle et de poursuivre leurs activités dans l'UE.

La **mission de conseil de l'UE en Ukraine** soutient la réforme des services répressifs et des institutions chargées de faire respecter l'état de droit dans le pays depuis 2014. En mars 2022, le mandat de la mission a été révisé afin de permettre un soutien aux points de passage frontaliers entre l'Ukraine, d'une part, et la Pologne, la Roumanie et la Slovaquie, de l'autre, ce qui a contribué à la connaissance de la situation en ce qui concerne les activités criminelles transfrontières, y compris la traite des êtres humains, et l'acheminement de biens humanitaires vers l'Ukraine.

## IV. ARMES, MATIÈRES DANGEREUSES ET INCIDENTS CRITIQUES

La guerre a fortement augmenté la circulation des armes à feu et d'autres armes en Ukraine même, ce qui fait peser de nouveaux risques sur l'UE et d'autres États voisins de l'Ukraine.

### *Vigilance et coordination*

Les lignes directrices opérationnelles publiées en mars ont fourni aux États membres des conseils sur la manière de relever le défi que représente la circulation accrue des armes à feu à un moment où se produisent des arrivées massives aux frontières extérieures de l'UE[36]. Ces lignes directrices soulignent que la présence d'armes à feu devrait constamment faire l'objet de vérifications et qu'à défaut d'autorisation, personne ne devrait être admis dans l'UE avec une telle arme. Lorsque des armes à feu sont signalées comme manquantes par les autorités ukrainiennes, les États membres devraient les signaler dans le système d'information Schengen.

[34] COM(2020) 796.
[35] COM(2021) 780, COM(2021) 782, COM(2021) 784.
[36] Communication de la Commission fournissant des lignes directrices opérationnelles pour la gestion des frontières extérieures afin de faciliter le franchissement des frontières entre l'UE et l'Ukraine (2022/C 104 I/01).

Il est essentiel que toutes les expéditions d'armes à feu vers l'Ukraine soient dûment enregistrées, avec toutes les informations pertinentes (notamment le type, le pays et l'année de fabrication, la marque, le modèle, le calibre et le numéro de série) afin de faciliter la traçabilité des armes à feu concernées, tant en Ukraine que dans l'UE.

L'UE a publiquement déploré les attaques militaires inconsidérées menées par la Russie sur le site et dans les environs immédiats d'installations nucléaires, biologiques et chimiques civiles, ainsi que tout acte compromettant la sûreté de ces installations. La Commission suit la situation en Ukraine, en accordant une attention particulière à la menace radiologique, qui est la plus préoccupante du point de vue de la sécurité intérieure de l'UE[37]. La Commission surveille également les menaces chimiques potentielles et a mis en place un mécanisme de coordination interne pour le cas où une évaluation rapide des risques serait nécessaire.

***Préparation***

L'Ukraine est déjà mentionnée dans le plan d'action de l'UE en matière de lutte contre le trafic d'armes à feu pour la période 2020-2025 parmi les pays prioritaires pour la mise en œuvre d'actions spécifiques sur le plan extérieur. Il existe également une action opérationnelle spécifique menée dans la région, y compris en Ukraine, dans le cadre du volet «armes à feu» de l'EMPACT. Toutefois, compte tenu des risques de détournement d'armes à feu, des projets spécifiques financés par l'UE seront nécessaires, ainsi qu'une coopération opérationnelle avec Europol, Frontex et le volet «armes à feu» de l'EMPACT. La Commission présentera prochainement une proposition de révision du règlement sur les armes à feu[38] , qui concerne les exportations, les importations et le transit d'armes à feu à usage civil et s'inscrit dans le cadre juridique et opérationnel global visant à prévenir et détecter le trafic d'armes à feu, ainsi qu'à mener des enquêtes et engager des poursuites en la matière.

Afin d'améliorer la préparation et la réaction de l'UE aux risques pour la santé publique tels que les menaces CBRN, la Commission constitue actuellement des réserves stratégiques de capacités de réaction par l'intermédiaire du mécanisme de protection civile de l'UE (MPCU), financé par l'Autorité européenne de préparation et de réaction en cas d'urgence sanitaire (HERA)[39]. Les services de la Commission coopèrent à la constitution d'une réserve stratégique rescEU pour un montant de 540 500 000 EUR. Cette réserve comprendra des équipements et des médicaments, des vaccins et d'autres traitements pour les patients exposés à des agents CBRN constituant une situation d'urgence, ainsi qu'une réserve rescEU de décontamination composée d'équipements de décontamination et d'équipes d'intervention spécialisées. À titre de première mesure immédiate, l'UE a mobilisé sa réserve médicale rescEU pour fournir des comprimés d'iodure de potassium offrant une protection contre les effets nocifs de radiations, ainsi que d'autres produits dont il y a un besoin urgent en Ukraine. Près de 3 millions de comprimés d'iode ont déjà été livrés à l'Ukraine par l'intermédiaire du MPCU, avec l'aide de la France et de l'Espagne.

---

[37] La Commission organisera, en coopération avec ses partenaires américains, un atelier axé sur les risques liés aux matières radiologiques qui se trouvent dans des hôpitaux et échappent au contrôle réglementaire.

[38] Règlement (UE) nº 258/2012 du Parlement européen et du Conseil du 14 mars 2012 portant application de l'article 10 du protocole des Nations unies contre la fabrication et le trafic illicites d'armes à feu, de leurs pièces, éléments et munitions, additionnel à la convention des Nations unies contre la criminalité transnationale organisée (protocole relatif aux armes à feu) et instaurant des autorisations d'exportation, ainsi que des mesures concernant l'importation et le transit d'armes à feu, de leurs pièces, éléments et munitions.

[39] Plan de travail 2022 de l'HERA (europa.eu)

## V. ACTION COORDONNÉE POUR DEMANDER DES COMPTES FACE À L'AGRESSION RUSSE

L'UE joue un rôle décisif dans les actions menées par la communauté internationale afin de faire pression sur la Russie pour qu'elle mette fin à son agression contre l'État ukrainien et contre les civils prisonniers du conflit, agression qui est inacceptable et contraire au droit international. Cette pression comprend notamment des mesures visant à faire connaître les conséquences, y compris les sanctions sévères, encourues par les auteurs, ainsi que des actions destinées à recenser les crimes de guerre et à faciliter les poursuites contre ceux-ci.

*Mesures restrictives et confiscations*

Depuis la reconnaissance par la Russie, le 21 février 2022, des zones non contrôlées par le gouvernement des oblasts de Donetsk et de Louhansk en Ukraine et l'invasion de l'Ukraine le 24 février 2022, l'UE a imposé une série de mesures restrictives d'une ampleur inédite à l'encontre de la Russie. À ce jour, cinq trains de sanctions ont été adoptés. Les mesures se concentrent sur des secteurs essentiels, notamment les finances, le commerce, les transports, la défense et les médias, et visent les élites politiques et militaires, ainsi que des oligarques russes et biélorusses de premier plan. Les listes comprennent déjà plus de 1 000 personnes physiques et 80 personnes morales. Un sixième train de sanctions est en cours d'examen au Conseil.

Les mesures restrictives actuelles et antérieures visant des particuliers et des entreprises russes et biélorusses produiront des effets dont la force sera à la mesure de celle de leur mise en œuvre. La coordination au niveau de l'UE peut contribuer de manière significative à combler les lacunes potentielles, et la Commission a fourni un appui important aux parties prenantes, au moyen d'orientations écrites, de réunions des parties prenantes et d'un groupe d'experts spécialisé, ainsi que de toute une série de ressources destinées à faciliter le respect des mesures.

En outre, la Commission a mis en place un groupe de travail «Gel et confiscation» réunissant des services de la Commission, les États membres, Eurojust et Europol. Jusqu'à présent, les États membres ont déclaré avoir gelé des avoirs d'une valeur de 9 890 000 000 EUR[40]. Le 11 avril, Europol, conjointement avec les États membres, Eurojust et Frontex, a lancé l'opération Oscar afin de soutenir les enquêtes financières et pénales ciblant les avoirs d'origine criminelle détenus par des personnes physiques ou morales faisant l'objet de sanctions de l'UE liées à la guerre menée par la Russie contre l'Ukraine. Le groupe de travail «Gel et confiscation» de l'UE collabore étroitement avec le groupe de travail «Russian Elites, Proxies, and Oligarchs (REPO)» («Élites, mandataires et oligarques russes») mis en place par les pays du G7 (Allemagne, Canada, États-Unis, France, Italie, Japon et Royaume-Uni) et des partenaires partageant les mêmes valeurs tels que l'Australie, ainsi qu'avec le groupe de travail «KleptoCapture» des États-Unis et le groupe de travail ukrainien.

Le groupe de travail «Gel et confiscation» sert de plateforme pour coordonner et faciliter l'échange d'informations et d'expériences entre les États membres, fournir des orientations sur la mise en œuvre des sanctions, et faciliter l'échange de bonnes pratiques en matière d'enquêtes pénales et de confiscations. En particulier, il importe que les autorités répressives soient vigilantes et proactives en ce qui concerne les infractions susceptibles d'être commises

[40] En outre, des actifs de la banque centrale russe, d'un montant d'environ 23 000 000 000 EUR ont été bloqués.

par les personnes physiques et morales sanctionnées. Le groupe de travail a également pour objet de faire avancer les discussions sur un éventuel déploiement des fonds confisqués, par exemple à des fins de contribution à la reconstruction de l'Ukraine.

La Commission adopte aujourd'hui un train de mesures concernant **le recouvrement et la confiscation d'avoirs**[41], qui tient compte des enseignements tirés de la mise en œuvre des mesures restrictives de l'Union visant des personnes physiques et morales russes et biélorusses. Ce train de mesures facilitera la mise en œuvre effective des mesures restrictives de l'UE dans l'ensemble de l'Union en permettant le dépistage et l'identification rapides des biens détenus ou contrôlés par des personnes physiques ou morales faisant l'objet de ces mesures. Le cadre renforcé en matière de recouvrement et de confiscation d'avoirs s'appliquera également à la violation des mesures restrictives et garantira ainsi l'efficacité du dépistage, du gel, de la gestion et de la confiscation des produits tirés de la violation des mesures restrictives. Afin de garantir que les avoirs des personnes physiques et morales qui enfreignent les mesures restrictives puissent réellement être confisqués, la Commission adopte également aujourd'hui une proposition de décision du Conseil prévoyant d'ajouter la violation des sanctions à la liste des infractions pénales de l'UE établie à l'article 83, paragraphe 1, du TFUE[42], proposition accompagnée d'une communication[43] dans laquelle il est envisagé de proposer une directive visant à rapprocher les définitions des infractions et des sanctions pénales applicables en cas de violation des mesures restrictives.

De manière plus générale, ce train de mesures marque une étape cruciale dans la lutte contre la criminalité organisée. Il fait suite aux engagements pris par la Commission dans le cadre de la stratégie pour l'union de la sécurité et de la stratégie visant à lutter contre la criminalité organisée 2020-2025[44]. Il prévoit la révision de la directive de 2014 relative à la confiscation, de la décision du Conseil de 2007 relative aux bureaux de recouvrement des avoirs et de la décision-cadre de 2005 relative à la confiscation des produits, des instruments et des biens en rapport avec le crime, afin de renforcer les capacités de dépistage, d'identification et, enfin, de confiscation des gains illicites et de remédier ainsi aux taux de confiscation très faibles constatés dans l'UE[45]. Le train de mesures élargit le champ des infractions pénales couvertes et étend les règles en matière de confiscation aux cas où une condamnation pénale pour une infraction donnée n'est pas possible mais où les avoirs proviennent clairement d'activités criminelles. La révision renforce également l'efficacité de la gestion des avoirs gelés et confisqués ainsi que la capacité des bureaux de recouvrement des avoirs à dépister et à identifier les avoirs illicites. Le nouveau cadre de l'UE en matière de recouvrement des avoirs est conçu pour s'attaquer au mode opératoire complexe des organisations criminelles, qui opèrent souvent par-delà les frontières et utilisent différentes méthodes pour dissimuler leurs avoirs, y compris au moyen de crypto-actifs.

---

41 COM(2022) 245.
42 COM(2022) 247.
43 COM(2022) 249.
44 COM(2021) 170.
45 Selon les estimations d'Europol, seuls 2 % des avoirs d'origine criminelle (soit 2 400 000 000 EUR) sont gelés et 1 % (soit un montant de 1 200 000 000 EUR) est confisqué, tandis que les recettes d'origine criminelle dans les principaux marchés criminels s'élevaient à 139 000 000 000 EUR en 2019 (ce qui représente 1 % du PIB de l'UE).

*Une réponse judiciaire coordonnée*

Des travaux sont également en cours au niveau de l'UE pour garantir une réponse judiciaire coordonnée aux **crimes internationaux** présumés commis en Ukraine, afin de permettre que leurs auteurs répondent de leurs actes.

Une équipe commune d'enquête (ECE) a été constituée par deux États membres et l'Ukraine pour enquêter sur les crimes de guerre, les crimes contre l'humanité et d'autres crimes internationaux qui sont présumés avoir été commis sur le territoire ukrainien. Eurojust apporte un soutien juridique, analytique, financier et logistique à cette ECE. Le 25 avril 2022, le bureau du procureur de la Cour pénale internationale s'est joint à l'ECE en tant que participant[46], et d'autres participants devraient y être intégrés prochainement.

Le 25 avril 2022, la Commission a présenté une proposition visant à modifier le règlement relatif à Eurojust[47] afin de permettre à cette dernière de conserver, d'analyser et de stocker des éléments de preuve relatifs aux principaux crimes internationaux. Eurojust et Europol continueront de collaborer étroitement tout au long de ce processus. Le réseau Génocide, dont le secrétariat est hébergé par Eurojust, joue également un rôle essentiel dans la coordination de la réponse judiciaire; il a élaboré un atlas des ONG actuellement actives en Ukraine et soutient les praticiens nationaux des États membres et d'Ukraine qui traitent les affaires en cours liées à la guerre.

En avril 2022, le Conseil a procédé à une nouvelle révision du mandat de la **mission de conseil de l'UE en Ukraine**, ouvrant la voie à l'apport, par la mission, d'un soutien aux autorités ukrainiennes dans les enquêtes et les poursuites portant sur tout crime international commis dans le contexte de l'agression militaire menée par la Russie. La mission fournira aux autorités ukrainiennes des conseils stratégiques concernant les enquêtes et les poursuites portant sur les crimes internationaux, les modifications nécessaires de la législation ukrainienne et la stratégie de communication, ainsi qu'une formation sur les questions connexes. La mission s'inscrit dans un ensemble d'initiatives de coordination prises dans ce contexte et, conjointement avec la délégation de l'UE, fait partie du groupe consultatif États-Unis-UE sur les atrocités criminelles pour l'Ukraine.

## VI. ACTIVITÉS DE MANIPULATION DE L'INFORMATION ET D'INGÉRENCE MENÉES DEPUIS L'ÉTRANGER

Les évolutions géopolitiques actuelles ont mis en évidence les risques d'ingérence étrangère. L'agression militaire de la Russie contre l'Ukraine s'est accompagnée d'activités de **manipulation** de l'information et d'**ingérence**. Des allégations – sans fondement – de «nazisme» et de «génocide» contre le gouvernement ukrainien, des opérations sous fausse bannière et des accusations infondées contre l'OTAN et l'Occident ont été utilisées pour justifier des attaques brutales contre l'Ukraine, tandis qu'il a été mis fin à la liberté d'expression et à la diffusion d'informations indépendantes en Russie. Il existe un risque persistant que la Russie tente de se servir de matériel audiovisuel manipulé et d'éléments de désinformation pour justifier de nouvelles attaques militaires, pour affaiblir la détermination de la résistance ukrainienne, pour diviser la communauté internationale dans son opposition à la guerre ou pour semer le doute quant aux violations du droit international par la Russie.

[46] https://www.eurojust.europa.eu/eurojust-and-the- war-in-ukraine
[47] COM(2022) 187 final.

Dans le cadre de la boussole stratégique, l'UE s'est engagée à réagir fermement aux activités de manipulation de l'information et d'ingérence menées depuis l'étranger et à renforcer sa résilience face à de telles menaces ainsi que sa capacité à contrer ces dernières[48]. La manipulation du débat démocratique au sein de l'UE est au cœur du plan d'action pour la démocratie européenne, le plan coordonné de la Commission visant à lutter contre la désinformation et à renforcer la résilience démocratique[49].

***Vigilance et coordination***

L'Union européenne a réagi par une action résolue et coordonnée à la campagne de désinformation menée par la Russie dans le contexte de l'agression militaire contre l'Ukraine. L'UE a collaboré étroitement avec ses États membres par l'intermédiaire du système d'alerte rapide, ainsi qu'avec des partenaires internationaux tels que l'OTAN, les États-Unis, le Canada et le mécanisme de réaction rapide du G7, afin de partager des informations sur les tactiques de manipulation employées par le Kremlin et les évolutions observées à cet égard. Les travaux visant à déconstruire les manipulations du Kremlin se sont intensifiés, notamment par l'intermédiaire du site web EUvsDisinfo, qui diffuse des informations en anglais, en russe, en ukrainien et dans d'autres langues, afin de fournir des données factuelles au sein de l'UE, en Ukraine et dans la région, ainsi que sur le territoire russe. Le 2 mars, les activités de transmission et de diffusion des médias d'État russes RT et Sputnik dans l'UE ou à destination de l'UE ont été suspendues, dans le cadre des mesures restrictives adoptées par l'UE. Les plateformes en ligne, les principaux réseaux sociaux, les annonceurs et les acteurs du secteur de la publicité signataires du code de bonnes pratiques contre la désinformation[50] prennent des mesures urgentes pour limiter la désinformation relative à l'agression russe contre l'Ukraine. La Commission et le SEAE suivent ces efforts. Il ressort des informations fournies que les plateformes ont renforcé leurs outils de surveillance et d'intervention se rapportant à la guerre.

En outre, des actions sont rapidement mises en place pour aider les pays d'Asie centrale et les Balkans occidentaux à renforcer la résilience de l'information et à lutter contre les activités de manipulation de l'information et d'ingérence menées depuis l'étranger.

***Préparation***

Eu égard à l'existence manifeste d'activités de manipulation de l'information et d'ingérence menées depuis l'étranger, y compris la désinformation en tant qu'outil des menaces hybrides, il est devenu plus urgent de donner suite au plan d'action pour la démocratie européenne. Au cours de ces derniers mois, les institutions de l'UE ont aidé les États membres à lutter contre les activités de manipulation de l'information et d'ingérence menées depuis l'étranger, en particulier dans le cadre du système d'alerte rapide, en partageant des informations sur les tactiques utilisées par ceux qui se livrent à de telles activités et sur les stratégies de riposte. Des discussions sont en cours au sujet du renforcement de la réaction globale de l'UE aux activités de manipulation de l'information et d'ingérence menées depuis l'étranger, sur la base d'une note de synthèse présentée par le SEAE concernant l'élaboration d'une **boîte à outils** spécifique pour faire face à cette menace. Cette boîte à outils regroupera les mesures internes existantes et les nouveaux outils de l'UE relevant de la politique étrangère et de

[48] https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/fr/pdf
[49] COM(2020) 790.
[50] https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

sécurité commune. Elle bénéficiera également de l'intensification de l'action de la Commission et de la division Stratcom du Service européen pour l'action extérieure[51].

L'Observatoire européen des médias numériques (EDMO) a mis en place un groupe de travail sur la désinformation à la suite de l'éclatement de la guerre en Ukraine et coordonne les actions des vérificateurs de faits et des chercheurs au sein de son réseau. Il a analysé la manière dont les théoriciens du complot autour de la COVID-19 se sont rapidement tournés vers la diffusion de canulars («hoaxes») pro-russes, une évolution observée dans un certain nombre d'États membres[52].

La proposition de législation sur les services numériques vise à s'adapter à l'évolution rapide des technologies numériques et à ses effets sur les défis technologiques et démocratiques, tels que les discours de haine, la désinformation en ligne et les stratégies de déstabilisation. Des progrès notables dans les négociations entre le Parlement européen et le Conseil devraient permettre une adoption rapide du paquet.

## VII. UNE PLUS GRANDE PRÉPARATION

À l'heure où l'Europe connaît à nouveau la guerre et où des mutations géopolitiques majeures sont à l'œuvre, la coordination de la sécurité au sein de l'UE est passée à la vitesse supérieure, en s'appuyant sur des initiatives déjà en préparation avant la guerre d'agression menée par la Russie contre l'Ukraine. Les initiatives essentiellement axées sur la sécurité extérieure de l'UE ont de fortes répercussions sur le volet intérieur de l'union de la sécurité.

Le 15 février 2022, la Commission a présenté le **paquet «Défense»**[53], qui comprend un certain nombre d'initiatives dans des domaines essentiels pour la défense et la sécurité au sein de l'UE. Cette contribution de la Commission à la défense et à la sécurité européennes couvre l'ensemble des défis. Les initiatives proposées sont des mesures concrètes pour parvenir à un marché européen de la défense plus intégré et plus compétitif, notamment en renforçant la coopération au sein de l'UE et en réalisant des économies d'échelle. Elles comprennent également une feuille de route sur les technologies critiques pour la sécurité et la défense, afin de stimuler la recherche, le développement technologique et l'innovation dans ces secteurs et de réduire les dépendances dans les technologies critiques et les chaînes de valeur. Par ailleurs, le paquet vise à renforcer la dimension «défense» de l'espace au niveau de l'UE. En outre, il examine comment la Commission pourrait intensifier ses actions contre les menaces hybrides, y compris dans le cyberespace, renforcer la mobilité militaire à l'intérieur et à l'extérieur de l'Europe et continuer à relever les défis liés au changement climatique pour la défense. Afin de compléter ces travaux, la communication conjointe du 18 mai intitulée «**Defence Investment Gaps Analysis and way forward**» (Analyse des déficits

[51] La division «Communication stratégique, groupes de travail et analyse de l'information» du Service européen pour l'action extérieure apporte un soutien en matière de communication stratégique pour la mise en œuvre de la politique étrangère et de sécurité de l'UE dans les régions prioritaires concernées (voisinage méridional et oriental, Balkans occidentaux) en élaborant et en mettant en œuvre des actions de communication stratégique spécifiques axées sur la promotion des politiques, des valeurs, des objectifs et des intérêts de l'UE.

[52] https://edmo.eu/2022/03/30/how-covid-19-conspiracy-theorists-pivoted-to-pro-russian-hoaxes/

[53] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/contributing-european-defence_fr

d'investissement dans le domaine de la défense et voie à suivre)[54] examine les déficits industriels ainsi que les déficits en matière de capacités auxquels il y a lieu de remédier pour soutenir les États membres de l'UE les plus exposés et définir des mesures visant à atténuer les défaillances recensées.

La résilience de l'UE face à ces menaces implique également des approches axées sur les capacités dans tous les secteurs de la sécurité, comme le préconise la Commission dans son plan d'action sur les synergies entre les industries civile, spatiale et de la défense[55]. Des travaux sont en cours en vue de promouvoir des approches axées sur les capacités dans le domaine de la sécurité intérieure et des services répressifs.

Le 21 mars 2022, le Conseil a adopté la **boussole stratégique en matière de sécurité et de défense**[56], que le Conseil européen a approuvée peu après. La boussole stratégique définit un plan d'action ambitieux destiné à renforcer la politique de sécurité et de défense de l'UE d'ici 2030. L'objectif est de faire de l'UE une garante de la sécurité plus forte et aux capacités renforcées, qui protège ses citoyens et contribue à la paix et à la sécurité internationales. Le document contient des propositions concrètes, assorties d'un calendrier de mise en œuvre très précis, afin d'améliorer la capacité de l'UE à agir de manière décisive en cas de crise.

L'un des résultats attendus de la boussole stratégique consiste en l'élaboration d'une **boîte à outils hybride de l'UE**, qui devrait fournir un cadre pour apporter une réponse coordonnée aux campagnes hybrides touchant l'UE et ses États membres, comprenant des mesures internes et externes. À la suite du recensement des exigences de base sectorielles en matière de résilience réalisé au début de l'année 2022[57], une analyse des lacunes et des besoins sera menée à bien. C'est dans ce cadre que l'UE continuera de renforcer la préparation, la résilience et la réaction face aux menaces résultant de l'agression russe et de toute autre tentative de déstabilisation des démocraties et de l'ordre multilatéral fondé sur des règles.

## VIII. PERSPECTIVES

Dans une perspective d'avenir, l'UE devra rester extrêmement vigilante face à des menaces en constante évolution, et renforcer **la préparation et la résilience pour tous les cas de figure**. Les répercussions de la guerre peuvent prendre différentes formes – il n'est pas encore possible de prendre la mesure de l'ensemble d'entre elles.

L'ampleur du déplacement des réseaux criminels ukrainiens n'est pas encore connue. Les dossiers traités précédemment par Eurojust indiquent une tendance au trafic d'héroïne depuis l'Afghanistan vers l'UE en passant par l'Ukraine, comme le confirme l'Observatoire européen des drogues et des toxicomanies (OEDT)[58]. L'instabilité est susceptible de rendre

---

54 JOIN(2022) 24.

55 COM(2021) 70.

56 Une boussole stratégique en matière de sécurité et de défense – Pour une Union européenne qui protège ses citoyens, ses valeurs et ses intérêts, et qui contribue à la paix et à la sécurité internationales (https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/fr/pdf)

57 SWD(2022) 21 final.

58 *Report on the drug and alcoholic situation in Ukraine for 2020 (according to 2019 data)* [Rapport 2020 sur la situation en matière de drogue et d'alcool en Ukraine (selon les données de 2019)], OEDT, *Stopping the trafficking of a heroin substitute in France, Poland and Ukraine, including the planning and execution of a*

plus difficile la lutte contre le commerce de l'héroïne par cette filière, ce qui risque d'entraîner une augmentation du flux de drogues vers l'UE.

Certains risques pour l'UE sont davantage susceptibles d'augmenter à la fin des hostilités ou au cours des pauses potentielles dans les combats. Une attention particulière sera accordée à la circulation des armes à feu, le risque étant appelé à croître lorsque les combats en Ukraine se calmeront. L'expérience passée montre également que le retour de combattants étrangers qui ont acquis une expérience de combat et qui ont pu entrer en contact avec des groupes extrémistes risque d'entraîner des actions terroristes dans l'UE à un stade ultérieur. Ce phénomène potentiel est à suivre de près, et la Commission facilite déjà les discussions entre les États membres concernant les défis posés par le retour des volontaires étrangers ayant des antécédents d'extrémisme violent.

Compte tenu de ces menaces possibles, il importe que la mise en œuvre de la stratégie pour l'union de la sécurité se poursuive, notamment par la réalisation de stratégies clés telles que la stratégie de cybersécurité de l'UE, la stratégie de l'UE visant à lutter contre la criminalité organisée (2020-2025), le programme de lutte antiterroriste pour l'UE (2020-2025), le plan d'action de l'UE en matière de lutte contre le trafic d'armes à feu (2020-2025), la stratégie de l'UE visant à lutter contre la traite des êtres humains (2021-2025) et la stratégie de l'UE en matière de drogue (2021-2025).

Les efforts destinés à doter l'UE du cadre législatif nécessaire seront maintenus. À titre d'exemple, la Commission est en train de préparer l'analyse d'impact relative à une proposition réglementant la commercialisation et l'utilisation des produits chimiques à haut risque.

## IX. CONCLUSION

L'union de la sécurité continue de jouer son rôle, pour ce qui est de préparer l'UE et ses États membres à faire face aux menaces existantes et potentielles. La guerre d'agression menée par la Russie contre l'Ukraine a montré à quelle vitesse des menaces théoriques pouvaient devenir une réalité. Elle met également en évidence l'importance de la vigilance, de la coordination et de la préparation.

Ce quatrième rapport sur l'état d'avancement de la stratégie pour l'union de la sécurité démontre la capacité de l'UE à s'adapter, même face à des menaces exceptionnelles et inattendues telles que la guerre d'agression menée par la Russie contre l'Ukraine. Il est plus important que jamais de mettre résolument en œuvre la stratégie pour l'union de la sécurité.

*controlled delivery* (Mettre fin au trafic d'un substitut de l'héroïne en France, en Pologne et en Ukraine, y compris la planification et l'exécution d'une livraison surveillée), 2021/00446, Eurojust, mai 2020.