Raad van de
Europese Unie

Brussel, 27 mei 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	

BEGELEIDENDE NOTA

van:	de secretaris-generaal van de Europese Commissie, ondertekend door mevrouw Martine DEPREZ, directeur
ingekomen:	25 mei 2022
aan:	het secretariaat-generaal van de Raad
nr. Comdoc.:	COM(2022) 252 final
Betreft:	MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD over het vierde voortgangsverslag over de uitvoering van de EU-strategie voor de veiligheidsunie

Hierbij gaat voor de delegaties document COM(2022) 252 final.

Bijlage: COM(2022) 252 final

EUROPESE
COMMISSIE

Brussel, 25.5.2022
COM(2022) 252 final

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD

over het vierde voortgangsverslag over de uitvoering van de EU-strategie voor de veiligheidsunie

I. INLEIDING

De Russische aanvalsoorlog tegen Oekraïne domineert vandaag de dag de veiligheidsagenda van de EU. De oorlog bedreigt niet alleen Oekraïne, maar ook de stabiliteit en veiligheid in de wereld. Binnen de EU brengt het een reeks risico's voor de veiligheid van de burgers met zich mee. Er zijn nieuwe onzekerheden over de levering van energie en andere grondstoffen, en kritieke infrastructuur kan het doelwit worden van cyberaanvallen. De interne veiligheid en beveiliging van de EU worden in gevaar gebracht door mogelijke aanslagen of ongelukken met chemische, biologische, radiologische of chemische strijdmiddelen in het oorlogsgebied. De kwetsbaarheid van miljoenen mensen die de oorlog zijn ontvlucht, kan snel worden uitgebuit door de georganiseerde misdaad, via de handel in vrouwen en kinderen, die bijzonder kwetsbaar zijn.

In het licht van deze nieuwe en potentiële bedreigingen is de EU vastberaden en eensgezind gebleven. Hoewel de gevolgen van de oorlog tot dusver hoofdzakelijk beperkt zijn gebleven tot het grondgebied van Oekraïne, heeft de EU haar *waakzaamheid en coördinatie* opgevoerd door het dreigingslandschap nauwlettender te monitoren, en gewerkt aan de versterking van de eigen veerkracht om *paraatheid* te garanderen.

In de Verklaring van Versailles van 10 en 11 maart 2022[1] benadrukten de Europese leiders dat we ons moeten voorbereiden op snel opkomende uitdagingen, onder meer door "onszelf te beschermen tegen toenemende hybride oorlogvoering, onze cyberveerkracht te verhogen, onze infrastructuur – en met name onze kritieke infrastructuur – te beschermen, en desinformatie tegen te gaan".

Het kader van de veiligheidsunie staat centraal bij het waarborgen van de veiligheid in de gehele EU. De vier strategische prioriteiten die in de strategie voor de veiligheidsunie zijn vastgesteld[2] blijven in de huidige geopolitieke context van rechtstreeks belang voor deze taak: i) een toekomstbestendige veiligheidsomgeving; ii) een aanpak van veranderende dreigingen; iii) bescherming van Europeanen tegen terrorisme en georganiseerde misdaad; en iv) een krachtig Europees veiligheidsecosysteem. De oorlog heeft onderstreept dat de EU en haar lidstaten ten volle gebruik moeten maken van de wetgevings- en beleidsinstrumenten die reeds beschikbaar zijn in het kader van de strategie voor de veiligheidsunie en die de basis vormen voor gecoördineerde EU-steun aan de lidstaten met betrekking tot kwesties van georganiseerde misdaad en terrorisme tot cyberveiligheid en hybride dreigingen.

Ook de Europese agentschappen op het gebied van justitie en binnenlandse zaken hebben hun inspanningen opgevoerd in reactie op de oorlog in Oekraïne, en spelen een sleutelrol bij het beoordelen van dreigingen en het ondersteunen van operationele reacties[3]. De voortdurende versterking van de operationele praktijk en de governance van het Schengengebied is een andere belangrijke factor.

Dit vierde voortgangsverslag over de veiligheidsunie gaat over de ontwikkelingen in de afgelopen maanden sinds de Russische aanvalsoorlog tegen Oekraïne. Het verslag geeft een overzicht van de acties die op alle onderdelen van de veiligheidsunie zijn ondernomen, en gaat in op de paraatheidsbehoeften in verband met mogelijke veiligheidsdreigingen als

[1] https://www.consilium.europa.eu/media/54788/20220311-versailles-declaration-nl.pdf
[2] COM(2020) 605.
[3] Gezamenlijke verklaring van de EU-agentschappen voor justitie en binnenlandse zaken over Oekraïne |Asielagentschap van de Europese Unie (europa.eu)

gevolg van de oorlog in Oekraïne. De vorderingen met betrekking tot andere dossiers van de veiligheidsunie zijn opgenomen in de bijlage.

II. CYBERBEVEILIGING EN KRITIEKE INFRASTRUCTUUR

Sinds het uitbreken van de oorlog hebben particuliere actoren en criminele operaties publiekelijk bekendgemaakt dat zij cyberactiviteiten ontplooien ter ondersteuning van deze of gene partij. Hacktivisme[4] vormt een bedreiging vanwege het risico van overloopeffecten in de EU tegen kritieke diensten, het risico dat aanvallen afkomstig zijn van officiële netwerken of andere onvoorziene overloopeffecten. Hoewel de oorlog tot dusver grotendeels met conventionele middelen is gevoerd, met slechts beperkte overloopeffecten, is het risico van escalatie op dit gebied reëel.

De EU heeft daarom haar coördinatie en paraatheid opgevoerd. De dreigingen die uit de oorlog voortvloeien, onderstrepen de noodzaak om een cultuur op te bouwen waarin informatie en deskundigheid worden gedeeld tussen de EU, de lidstaten en de verschillende cyberbeveiligingsgemeenschappen. Dit omvat het opbouwen van een geïntegreerd situationeel bewustzijn, gedeeld door de instellingen, organen en agentschappen van de EU en de lidstaten, met name ten aanzien van de kritieke infrastructuur waarvan de soepele werking van de interne markt afhangt.

Toeschrijving van cyberaanvallen op Oekraïne

Cyberaanvallen op Oekraïne zelf begonnen al vóór de Russische agressie en waren, in de eerste dagen van de oorlog[5], gericht op het compromitteren van gebruikersaccounts van Oekraïens militair personeel en het verstoren van de essentiële diensten, waaronder grenscontrole en telecommunicatie.

Op 14 januari 2022 heeft de hoge vertegenwoordiger namens de Europese Unie een verklaring afgelegd[6] waarin de cyberaanvallen op Oekraïne werden veroordeeld en de ondubbelzinnige steun van de EU aan Oekraïne opnieuw werd bevestigd.

Op 10 mei hebben de Europese Unie en haar lidstaten, samen met internationale partners de kwaadwillige cyberactiviteiten tegen Oekraïne van 24 februari krachtig veroordeeld[7], die gericht waren tegen het satellietnetwerk KA-SAT, dat eigendom is van Viasat, en de aanval rechtstreeks toegeschreven aan de Russische Federatie. Deze cyberaanval had een aanzienlijke impact en veroorzaakte willekeurige communicatiestoringen en -onderbrekingen

[4] Een recent voorbeeld van hacktivisme is het gebruik van "protestware" om malware via populair opensourcesoftware te verspreiden naar Russische IP-adressen, wat kan leiden tot risico's voor de toeleveringsketen en verlies van vertrouwen in de opensourcegemeenschap. De Commissie heeft duidelijk gemaakt dat (zelfs goedbedoelde) cyberaanvallen op Rusland illegaal zijn.

[5] Microsoft, Special Report: An overview of Russia's cyberattack activity in Ukraine (Speciaal rapport: een overzicht van de cyberaanvallen door Rusland in Oekraïne); The hybrid war in Ukraine - Microsoft On the Issues (De hybride oorlog in Oekraïne – Microsoft On the Issues)

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

[7] Russische cyberoperaties tegen Oekraïne:verklaring van de hoge vertegenwoordiger namens de EU (europa.eu)

bij verschillende overheidsinstanties, bedrijven en gebruikers in Oekraïne. Ook verschillende EU-lidstaten werden getroffen.

Waakzaamheid en coördinatie

Sinds de Russische aanvalsoorlog tegen Oekraïne wordt de cyberbeveiligingssituatie in de lidstaten en de EU-instellingen nauwgezetter gemonitord. Enisa, het agentschap van de Europese Unie voor cyberbeveiliging, het Europees Centrum voor de bestrijding van cybercriminaliteit van Europol en CERT-EU, het computercrisisresponsteam voor de instellingen, organen en instanties van de Europese Unie en het Inlichtingen- en situatiecentrum van de Europese Unie (EU Intcen), dragen allemaal bij tot het gedeelde situationele bewustzijn van de EU, bijvoorbeeld door te zorgen voor regelmatige monitoring van verdachte cyberactiviteiten, onder meer in specifieke sectoren zoals energie, vervoer en luchtvaart, en leveren beoordelingen die als uitgangspunt dienen voor preventieve maatregelen.

Ook de coördinatie en de uitwisseling van informatie met cyberbeveiligingsnetwerken, zoals het Europees Netwerk van verbindingsorganisaties voor cybercrises (CyCLONe), dat bestaat uit nationale cyberbeveiligingsagentschappen, de Commissie en Enisa, is geïntensiveerd. Om deze aanpak intern in de EU-instellingen te weerspiegelen, maakt een coördinatiemechanisme, de Taskforce Cybercrisis (*Cyber Crisis Task Force*), het mogelijk informatie te delen tussen alle betrokken diensten, organen en agentschappen, waaronder Enisa, het Europees Centrum voor de bestrijding van cybercriminaliteit van Europol en CERT-EU. Er zijn voortdurende inspanningen nodig om te zorgen voor communicatiekanalen tussen het politieke, het operationele en het technische niveau, alsmede om de samenwerking met het netwerk van Computer Security Incident Response Teams (CSIRT) te verbeteren.

Europol heeft ook het EU-noodhulpprotocol voor rechtshandhaving in werking gesteld, dat versterkte monitoring van cyberdreigingen en informatie-uitwisseling tussen een breed scala van belanghebbenden mogelijk maakt om een alomvattend inlichtingenbeeld van de cyberdreigingen op te bouwen.

Afgezien van cyberdreigingen zijn de lidstaten, de EDEO en de diensten van de Commissie waakzamer geworden wat betreft de blootstelling van kritieke infrastructuur aan andere niet-digitale, maar fysieke dreigingen. Kritieke infrastructuur en de entiteiten die deze exploiteren kunnen worden blootgesteld aan fysieke risico's, zoals sabotage door de staat of door door de staat gesteunde actoren als onderdeel van mogelijke vergeldingsmaatregelen tegen de EU.

Paraatheid

Paraatheid op het gebied van cyberbeveiliging en de beveiliging van kritieke infrastructuur is meer dan ooit van essentieel belang, gelet op de toegenomen blootstelling van Europa aan een opeenstapeling van dreigingen als gevolg van de oorlog. De inspanningen om de paraatheid te verhogen omvatten een aantal directe acties, waaronder enkele die al waren gepland vóór de Russische agressie tegen Oekraïne. Het gaat hierbij onder meer om oefeningen, richtsnoeren, wetgevingsmaatregelen, het vergroten van de veerkracht in kritieke sectoren, en samenwerking met partners.

Het Franse voorzitterschap van de Raad van de Europese Unie heeft begin 2022 samen met de Europese Dienst voor extern optreden (EDEO) en het agentschap van de Europese Unie voor cyberbeveiliging (Enisa) een op scenario's gebaseerde oefening georganiseerd, EU CyCLES (*Cyber Crisis Linking Exercise on Solidarity*) genoemd, die als doel had het bewustzijn op politiek niveau te vergroten en de samenwerking tussen het operationele en het politieke niveau te versterken in geval van een grootschalige cyberaanval.

Enisa en CERT-EU hebben in februari **richtsnoeren** gepubliceerd over hoe de veerkracht en de paraatheid in de EU kunnen worden versterkt[8]. Deze richtsnoeren moedigen alle organisaties in de publieke en private sector in de EU aan een minimumpakket van beste praktijken op het gebied van cyberbeveiliging vast te stellen om de cyberbeveiligingscultuur aanzienlijk te verbeteren. In maart heeft CERT-EU met de steun van Enisa aanvullende technische richtsnoeren gepubliceerd[9], alsmede een beveiligingshandleiding voor het versterken van de configuratie van Signal-apps[10] met een aantal praktische aanbevelingen aan organisaties om hun cyberbeveiligingspositie te verbeteren.

Wetgevingsinitiatieven

De huidige situatie onderstreept de noodzaak om **bestaande wetgeving uit te voeren** en **de goedkeuring van hangende initiatieven** te bespoedigen.

De Commissie ondersteunt de lidstaten bij de uitvoering van de **richtlijn netwerk- en informatiebeveiliging (de "NIB-richtlijn")**[11], die vereist dat de lidstaten naar behoren zijn uitgerust, bijvoorbeeld door een *Computer Security Incident Response Team* (CSIRT) op te zetten en bevoegde autoriteiten aan te wijzen. Het fungeert als basis voor doeltreffende samenwerking tussen de lidstaten. Het door de medewetgevers bereikte politieke akkoord over de **NIB 2-richtlijn**[12] is een verdere doorbraak in de totstandbrenging van een robuust EU-kader voor paraatheid.

NIB 2: verdere versterking van de paraatheid

- De nieuwe richtlijn netwerk- en informatiesystemen zal de tekortkomingen van de vorige NIB-richtlijn aanpakken, en deze aanpassen aan de huidige behoeften en toekomstbestendig maken. De richtlijn bevat minimumvoorschriften voor een regelgevingskader en voorziet in mechanismen voor doeltreffende samenwerking tussen de betrokken autoriteiten in elke lidstaat.
- Het toepassingsgebied van de regels wordt verruimd en er worden nieuwe sectoren toegevoegd die van cruciaal belang zijn voor de economie en de samenleving (bv. de farmaceutische sector en de sector medische hulpmiddelen of de

[8] Boosting your Organisation's Cyber Resilience (De cyberbestendigheid van uw organisatie verbeteren) (gezamenlijke publicatie), 14.02.2022.

[9] CERT-EU, Security Guidance 22-001 – Cybersecurity mitigation measures against critical threats (Beveiligingsrichtsnoer 22-001 – Mitigatiemaatregelen in de strijd tegen kritieke dreigingen op het gebied van cyberbeveiliging).

[10] CERT-EU, Security Guidance 22-002 – Hardening Signal (Beveiligingsrichtsnoer 22-002 – Versterking van Signal).

[11] Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.

[12] COM(2020) 823.

levensmiddelenindustrie). Alle middelgrote en grote entiteiten die actief zijn in de sectoren of diensten verlenen die onder de richtlijn vallen, zullen onder het toepassingsgebied ervan vallen. Openbare bestuurslichamen van centrale overheden (met uitzondering van de rechterlijke macht, parlementen en centrale banken) en op regionaal niveau vallen eveneens onder de richtlijn. Bovendien kunnen de lidstaten besluiten dat de richtlijn van toepassing is op dergelijke entiteiten op lokaal niveau.

- De NIB 2-richtlijn zal de basis vormen voor risicobeheersmaatregelen op het gebied van cyberbeveiliging en formeel het Europees Netwerk van verbindingsorganisaties voor cybercrises, EU-CyCLONe, oprichten, dat het gecoördineerde beheer van grootschalige incidenten op het gebied van cyberbeveiliging zal ondersteunen.
- Het voorstel bevat ook preciezere bepalingen over de procedure voor het melden van incidenten, de inhoud van de meldingen en de tijdlijnen, en voorziet in rechtsmiddelen en sancties om de handhaving te garanderen.
- De lidstaten hebben vanaf de inwerkingtreding van de richtlijn 21 maanden de tijd om de bepalingen in hun nationale recht om te zetten.

De voortgang met betrekking tot de NIB 2-richtlijn moet zo spoedig mogelijk worden gevolgd door de afronding van de onderhandelingen over de voorgestelde **richtlijn betreffende de veerkracht van kritieke entiteiten**[13] (de "VKE-richtlijn"), die, zodra zij zijn aangenomen en uitgevoerd, kritieke entiteiten beter bestand moeten maken tegen een reeks bedreigingen, waaronder terroristische aanslagen, dreiging van binnenuit of sabotage. Het is tevens van essentieel belang dat het ambitieniveau van de VKE-richtlijn overeenstemt met dat van het voorstel van de Commissie, en dat de samenhang met het politieke compromis dat over de NIB 2-richtlijn is bereikt, behouden blijft. Samen zullen deze maatregelen de veerkracht en de paraatheid vergroten door een coherenter en robuuster systeem op te zetten, onder meer via nationale rampen- en crisisbestrijdingsplannen. Deze maakten ook deel uit van de aanbeveling van de Commissie van vorig jaar[14] betreffende de opbouw van een **gemeenschappelijke cybereenheid**, waarin is bepaald hoe de verschillende actoren van het cyberbeveiligingsecosysteem (diplomaten, politie, civiele instanties en, in voorkomend geval, defensie) op operationeel niveau moeten samenwerken. Het huidige dreigingslandschap onderstreept de waarde van een dergelijke doeltreffende samenwerking tussen de belangrijkste spelers.

De Commissie blijft toezien op de uitvoering van het instrumentarium voor cyberbeveiliging van **5G**[15]. In dit verband heeft de NIB-samenwerkingsgroep op 11 mei een verslag vastgesteld over de veiligheid van Open RAN[16]. De groep blijft ook samenwerken met de lidstaten om het Europees centrum voor deskundigheid op het gebied van cyberbeveiliging volledig operationeel te maken.

Op 22 maart 2022 heeft de Commissie **nieuwe regels voorgesteld betreffende gemeenschappelijke maatregelen op het gebied van cyberbeveiliging en**

[13] COM(2020) 829.

[14] Aanbeveling van de Commissie van 23 juni 2021 betreffende de opbouw van een gezamenlijke cybereenheid;De digitale toekomst van Europa vormgeven (europa.eu).

[15] https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

[16] NIB-samenwerkingsgroep, Report on the cybersecurity of Open RAN, 11 mei 2022 (Verslag over de cyberbeveiliging van Open RAN).

informatiebeveiliging binnen de instellingen, organen en instanties van de Unie. Deze regels zullen de veerkracht van de EU-administratie en haar vermogen om te reageren op cyberdreigingen en -incidenten versterken. Door deze activiteiten in een gemeenschappelijk kader onder te brengen wordt de interinstitutionele samenwerking versterkt en de blootstelling aan risico's geminimaliseerd. De voorgestelde **verordening voor cyberbeveiliging in de instellingen, organen en instanties van de Unie**[17] zal het mandaat van CERT-EU versterken en leiden tot de oprichting van een nieuwe interinstitutionele raad voor cyberbeveiliging, de capaciteiten voor cyberbeveiliging versterken en regelmatige maturiteitsbeoordelingen en een betere cyberhygiëne stimuleren. De voorgestelde **richtlijn betreffende informatiebeveiliging**[18] schept minimumregels inzake informatiebeveiliging en normen voor het veilig verwerken en uitwisselen van informatie voor alle instellingen, organen en instanties van de Unie, om te zorgen voor een betere en consistente bescherming tegen de zich ontwikkelende dreigingen voor hun informatie. De Commissie roept het Europees Parlement en de Raad op deze maatregelen snel te bekrachtigen.

De Commissie heeft de openbare raadpleging over maatregelen om de **cyberweerbaarheid** van digitale producten te verbeteren, afgerond en werkt aan een voorstel dat dit najaar zal worden gepubliceerd[19]. Dit zal een antwoord bieden op de kwetsbaarheden van digitale producten en ondersteunende diensten die weliswaar kansen creëren voor de economieën en samenlevingen van de EU, maar ook tot nieuwe uitdagingen leiden, aangezien hoe meer alles met elkaar verbonden is, hoe gemakkelijker een incident op het gebied van cyberbeveiliging een volledig systeem kan treffen en zo de economische en sociale activiteiten kan verstoren.

Op 9 maart 2022 hebben de EU-ministers voor telecommunicatie unaniem de oproep van Nevers aangenomen om de EU-capaciteiten op het gebied van cyberbeveiliging te versterken, die onder meer voorziet in "de invoering van een nieuw noodfonds voor cyberbeveiliging dat door de Commissie moet worden opgericht"[20]. De Commissie beraadt zich over het beste gebruik van bestaande middelen ter ondersteuning van preventieve en responsmaatregelen.

Kritieke sectoren

De continuïteit van de **energievoorziening** van de EU is van cruciaal belang voor het welzijn van de burgers en voor de goede werking van onze economieën. De huidige situatie heeft duidelijk gemaakt dat er behoefte is aan duidelijke regels inzake cyberbeveiliging in deze sector. De Commissie werkt aan een netcode inzake cyberbeveiliging voor grensoverschrijdende elektriciteitsstromen, zoals vereist bij de elektriciteitsverordening[21], om regels vast te stellen voor risicobeoordelingen, gemeenschappelijke minimumeisen, planning, toezicht, verslaglegging en crisisbeheersing. Sinds de Russische aanvalsoorlog tegen Oekraïne zijn de voor de netcode beoogde doelstellingen inzake cyberbeveiliging nog relevanter. De Commissie heeft ook de aanzet gegeven tot een structurele samenwerking

[17] COM(2022) 122.
[18] COM(2022) 119.
[19] Wet inzake cyberweerbaarheid – nieuwe cyberbeveiligingsregels voor digitale producten en ondersteunende diensten
[20] Salle de Presse, Ministère des Finances, Déclaration conjointe des ministres de l'Union européenne chargés du numérique et des communications électroniques adressée au secteur numérique, 08.03.2022 (economie.gouv.fr).
[21] Verordening (EU) 2019/943 van het Europees Parlement en de Raad van 5 juni 2019 betreffende de interne markt voor elektriciteit (PB L 158 van 14.6.2019, blz. 54). Momenteel wordt een voorstel bestudeerd door het Agentschap voor de samenwerking tussen energieregulatoren (ACER).

tussen Enisa, ENTSB-E[22], ENTSB-G[23] en de Energiegemeenschap bij het regelmatig monitoren van de cyberbeveiligingssituatie in de energiesector.

De EU heeft zich ingespannen om de veiligheid van haar partners te beschermen zonder voor zichzelf nieuwe risico's te creëren. De noodsynchronisatie van de elektriciteitsnetten van Oekraïne en Moldavië met het net van continentaal Europa vond plaats in maart 2022, na de vaststelling van risicobeperkende maatregelen, met name op het gebied van cyberbeveiliging.

De oorlog en de sancties hebben ook voor het **vervoer** in de EU veel problemen veroorzaakt, van veiligheidsrisico's voor de burgerluchtvaart in de EU en vrachtwagenchauffeurs die vastzitten in conflictgebieden, tot de vernietiging van de vervoersinfrastructuur in Oekraïne, waardoor bevoorradingsketens worden afgesneden en de voedselzekerheid wereldwijd in gevaar komt. Het Europees Agentschap voor de veiligheid van de luchtvaart heeft, in nauwe samenwerking met de Commissie en Eurocontrol, de Europese Organisatie voor de veiligheid van de luchtvaart, de exploitanten sinds het begin van de oorlog geadviseerd het luchtruim van Oekraïne en het luchtruim binnen 100 zeemijlen van de grens tussen Wit-Rusland en Rusland/Oekraïne te mijden.

De Commissie heeft zich ook ingespannen om de paraatheid en de veerkracht van de Europese vervoerssector te versterken. Met name een nieuw noodplan voor vervoer[24], dat op 23 mei is vastgesteld, trekt lering uit zowel de COVID-19-pandemie als de militaire agressie van Rusland tegen Oekraïne. In het plan wordt een instrumentarium met 10 acties voorgesteld die de EU en haar lidstaten als leidraad kunnen gebruiken bij de invoering van crisisbestrijdingsmaatregelen, waaronder het waarborgen van een minimale connectiviteit, het opbouwen van veerkracht tegen cyber- en hybride dreigingen en het verbeteren van de samenwerking met internationale partners op het gebied van crisisparaatheid en crisisrespons. Ook wordt gewezen op het belang van regelmatige weerbaarheidstests voor verschillende crisisscenario's, waarbij relevante EU-agentschappen of andere actoren worden samengebracht, en wordt voortgebouwd op bestaande processen.

Krachtens het **EU-kader voor gezondheid en veiligheid** moet de uitwisseling van informatie op basis van het systeem voor vroegtijdige waarschuwing en maatregelen, met inbegrip van steun voor medische evacuaties uit Oekraïne, worden beschermd tegen cyberaanvallen; daarom wordt de beveiliging van het systeem versterkt.

Samenwerking met partners

De EU blijft met haar internationale partners samenwerken om kwaadwillig gedrag in cyberspace te voorkomen, te ontmoedigen, af te schrikken en aan te pakken. Door de Russische aanvalsoorlog tegen Oekraïne is samenwerking op dit gebied belangrijker dan ooit geworden. In dit verband heeft de EDEO gewerkt aan de uitwisseling van situationeel bewustzijn en de coördinatie van de respons op kwaadaardige cyberactiviteiten die gericht zijn tegen Oekraïne, alsook aan steun aan Oekraïne en andere landen in de regio, door samen te werken met partners, waaronder de VS en de NAVO, teneinde complementariteit te waarborgen en overlappingen te voorkomen.

[22] Europees netwerk van transmissiesysteembeheerders voor elektriciteit.
[23] Europees netwerk van transmissiesysteembeheerders voor gas.
[24] COM(2022) 211.

De nauwe samenwerking met de VS is ook geïntensiveerd in het kader van de Handels- en Technologieraad EU-VS (TTC). In de gezamenlijke verklaring[25] na de ministeriële bijeenkomst in Parijs in mei werd de centrale rol van de TTC voor het hernieuwde trans-Atlantische partnerschap benadrukt, dat dient om de gezamenlijke maatregelen van de EU en de VS ten aanzien van de Russische agressie tegen Oekraïne te coördineren. Beide partijen waren het erover eens dat nauwe samenwerking om de veerkracht van de toeleveringsketens te vergroten, belangrijker is dan ooit. Daarnaast werd een specifieke taskforce voor overheidsfinanciering voor een veilige en veerkrachtige digitale infrastructuur in derde landen opgezet om de weg vrij te maken voor gezamenlijke overheidsfinanciering van digitale projecten in derde landen door de VS en de EU, op basis van een reeks gemeenschappelijke overkoepelende beginselen.

Het in maart 2022 goedgekeurde strategisch kompas (zie punt VII) zal het EU-instrumentarium voor cyberdiplomatie verder versterken en het EU-beleid inzake cyberdefensie ontwikkelen om beter voorbereid te zijn op en beter te kunnen reageren op cyberaanvallen, als onderdeel van een bredere strategie om het vermogen van de EU om op te treden in crisissituaties en haar belangen te verdedigen, te versterken.

Steun bij cyberbeveiliging voor Oekraïne en de buurlanden

De EU ondersteunde de cyberveerkracht van Oekraïne al voor de oorlog. Reeds in juni 2021 hielden de EU en Oekraïne een eerste cyberdialoog, en de EU verleende via het programma EU4Digital 25 miljoen euro aan steun voor cyberbeveiliging en een veerkrachtige digitale transformatie aan Oekraïne. Een aanvullend associatieprogramma ter waarde van 1,5 miljoen euro zal de Oekraïense instanties op het gebied van cyberbeveiliging helpen zich aan te sluiten bij de EU-normen.

Sinds het uitbreken van de oorlog bevordert de EU de samenwerking tussen cyberdeskundigen uit de EU en Oekraïne, en coördineert zij de levering van technische bijstand, apparatuur, software en relevante diensten, om de cyberveerkracht en de cyberdefensie van Oekraïne te versterken.

Daarnaast werkt de EU aan een evaluatie van mogelijke steun op middellange termijn aan Moldavië, Georgië en de Westelijke Balkan. Op 3 en 4 maart 2022 heeft een gezamenlijke beoordelingsmissie naar Moldavië over de cyberbeveiligingsbehoeften plaatsgevonden, die heeft geleid tot de vaststelling van een specifieke crisisbestrijdingsmaatregel om de cyberbeveiliging in het land snel op te voeren. Vergelijkbare snellereactiesteun wordt voorbereid voor een aantal landen in de Westelijke Balkan die mogelijk een bijzonder risico lopen doordat zij achter de EU-sancties staan. Mogelijke aanvullende bijstand aan Moldavië via de Europese Vredesfaciliteit wordt eveneens onderzocht.

III. GEORGANISEERDE MISDAAD EN TERRORISME

De Russische aanvalsoorlog tegen Oekraïne heeft miljoenen mensen gedwongen hun huizen te verlaten, waardoor het aantal bewegingen over de buitengrens van de EU enorm is toegenomen. Op 18 mei waren bijna 6 miljoen mensen uit Oekraïne en Moldavië naar de EU gekomen, en tot nu toe hebben 2,8 miljoen mensen zich voor tijdelijke bescherming in de EU

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

laten registreren. De EU heeft getracht de snelste en meest flexibele opvang te bieden aan burgers die de oorlog ontvluchten, zonder de veiligheid aan de buitengrens van de EU in gevaar te brengen. De EU heeft ongekende maatregelen genomen om burgers die de oorlog ontvluchten tijdelijke bescherming te bieden, en heeft zich ertoe verbonden alle nieuwkomers zonder onderscheid te behandelen. Tegelijkertijd mogen de potentiële risico's die kunnen voortvloeien uit het feit dat zoveel mensen onderweg zijn, niet worden genegeerd, en blijft de EU, met de krachtige steun van de bevoegde EU-agentschappen, waakzaam voor nieuwe ontwikkelingen op het gebied van georganiseerde misdaad en terrorisme.

Een sterk Schengen in tijden van toenemende dreiging

Het waarborgen van een hoog niveau van veiligheid in het **Schengengebied** en binnen de EU is nog nooit zo belangrijk geweest als in een klimaat van verhoogde dreiging als gevolg van de oorlog net over de buitengrenzen van de EU.

Met het oog op de ambitieuze agenda voor het Schengengebied in de strategie van juni 2021, heeft de Commissie in mei het eerste verslag over de staat van Schengen vastgesteld[26]. De jaarlijkse Schengencyclus biedt een nieuw governancemodel voor het Schengengebied, met een regelmatige check-up van de staat van Schengen. Dit zal bijdragen tot een snelle opsporing van tekortkomingen en efficiënte follow-upprocedures, teneinde het Schengengebied sterker en veerkrachtiger te maken.

In dit eerste verslag wordt erkend dat de inspanningen ter uitvoering van belangrijke initiatieven op EU-niveau, waaronder systematische controles aan de buitengrenzen van alle reizigers, moeten worden opgevoerd, waarbij ten volle gebruik moet worden gemaakt van de mandaten van Frontex en Europol, alsook van de voorgestelde en beschikbare instrumenten voor grensoverschrijdende politiesamenwerking.

Met name de nieuwe architectuur voor EU-informatiesystemen voor grenzen, migratie en veiligheid, en de interoperabiliteit daarvan, vormt de hoeksteen van de inspanningen om de interne veiligheid en het grensbeheer te verbeteren. Het zal van cruciaal belang zijn dat alle elementen van het interoperabiliteitskader effectief en volgens de overeengekomen tijdschema's worden uitgevoerd.

Waakzaamheid en coördinatie

Een sterkere samenwerking tussen de lidstaten en met derde landen op het gebied van rechtshandhaving is van essentieel belang om ervoor te zorgen dat men zich bewust is van opkomende criminele en terroristische dreigingen, en ook moet worden opgetreden tegen criminele netwerken en individuen die wellicht proberen te profiteren van de oorlog tegen Oekraïne. De lidstaten en operationele partners delen actief relevante beschikbare informatie en criminele inlichtingen met Europol, dat de informatie controleert, analyseert en omzet in bruikbare operationele inlichtingen, zoals vroegtijdige waarschuwingen en dreigingsanalyses, die met de partners worden gedeeld.

[26] COM(2022) 301.

Georganiseerde misdaad

De georganiseerde misdaad vindt nu al manieren om de huidige situatie uit te buiten. Bij een eerste inlichtingenanalyse werden misdaadpatronen op een aantal gebieden vastgesteld, waaronder mensenhandel, valse aangiften van in- en uitgevoerde goederen, onlinefraude, cybercriminaliteit en handel in vuurwapens. Er zijn ook aanwijzingen dat cybercriminelen zich voordoen als fondsenwervers voor Oekraïne om geld en cryptovaluta te stelen[27]. Misdaadorganisaties uit Oekraïne zullen wellicht proberen zich als gevolg van de huidige situatie elders te vestigen en hun activiteiten in de EU voort te zetten.

De Commissie en het Franse voorzitterschap van de Raad hebben samen met de JBZ-instanties van de EU, met name Europol, het Europees multidisciplinair platform tegen criminaliteitsdreiging (**EMPACT**) in het leven geroepen om bestaande of opkomende dreigingen van zware en georganiseerde misdaad te beoordelen, erop te anticiperen, te voorkomen en te bestrijden. Op 7 april 2022 organiseerde Europol een EMPACT-bijeenkomst met vertegenwoordigers van en deskundigen uit de EU-lidstaten en de Europese veiligheidsgemeenschap om zich te buigen over de dreigingen van zware en georganiseerde misdaad die zijn ontstaan als gevolg van de oorlog in Oekraïne. Tot de concrete stappen die zijn besproken, behoorden het verzamelen van meer inlichtingen, het nemen van operationele noodmaatregelen en het bijsturen van bestaande maatregelen, alsmede gezamenlijke ad-hoc-actiedagen.

CELBET (*Customs Eastern and South-Eastern Land Border Expert Team*, team van douane-experts voor de oostelijke en zuidoostelijke landgrenzen) – een door de Europese Commissie gefinancierd samenwerkingsproject, volgt de ontwikkelingen aan de grens als onderdeel van zijn opdracht om operationele steun en begeleiding te verlenen aan de douanebeambten en houdt toezicht op beslag bij de invoer aan de grensovergangen aan de EU-grens (Polen, Slowakije, Hongarije en Roemenië) met Oekraïne.

Criminele en terroristische activiteiten

Hoewel zich in de EU nog geen onmiddellijke terroristische dreiging heeft voorgedaan in verband met de Russische inval in Oekraïne, is het duidelijk dat waakzaamheid geboden is.

De verhoogde risico's op criminele en terroristische activiteiten onderstrepen hoe belangrijk het is dat de lidstaten gebruikmaken van de relevante EU-databanken, zoals het Schengeninformatiesysteem, daar zo nodig gegevens in invoeren en deze raadplegen tijdens controles van personen die de EU binnenkomen. Dit zal ertoe bijdragen dat personen die een bedreiging vormen voor de interne veiligheid van de EU, aan de buitengrenzen worden geïdentificeerd. eu-LISA, het Agentschap van de Europese Unie voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht, blijft ervoor zorgen dat de grensbeheersystemen van de EU volledig beschikbaar en efficiënt zijn. In de

[27] De Threat Analysis Group van Google heeft een groeiend aantal dreigingsactoren waargenomen die de oorlog in Oekraïne gebruiken als lokmiddel in phishing- en malwarecampagnes. Onderzoekers van het internetbeveiligingsbedrijf Cyren melden een toename van cryptozwendel waarbij misbruik wordt gemaakt van het conflict door het gebruik van nagebootste donatiewebsites.

richtsnoeren[28] aan de lidstaten is verduidelijkt hoe een evenwicht kan worden gevonden tussen de noodzaak om te zorgen voor een vlotte afhandeling van de aankomsten aan de buitengrens en de uitvoering van de nodige veiligheidscontroles.

Paraatheid

Naast begeleiding en coördinatie is de paraatheid van de EU versterkt door de inzet van personeel van de EU-agentschappen.

Europol heeft operationele teams ingezet in de EU-lidstaten die aan Oekraïne grenzen. Deze teams bestonden uit uitgezonden Europol-functionarissen uit de lidstaten en Europol-deskundigen in Hongarije, Litouwen, Polen, Roemenië en Slowakije, alsook in Moldavië[29]. De uitgezonden Europol-functionarissen ondersteunen de nationale autoriteiten met tweedelijnsveiligheidscontroles aan de buitengrenzen van de EU. Europol-deskundigen bieden ondersteuning door informatie te verzamelen en te beoordelen om terroristische en criminele dreigingen op te sporen, onderzoeken te ondersteunen en personen te identificeren die een risico vormen door te proberen de EU binnen te komen. Deze operationele teams verzamelen informatie die wordt gebruikt bij de beoordeling van misdaaddreigingen waarover de lidstaten beschikken. Door het verzamelen van dergelijke inlichtingen kan Europol anticiperen op ontwikkelingen en operationele activiteiten coördineren met de EU-lidstaten om te reageren op de activiteiten van criminele groepen die proberen te profiteren van de oorlog in Oekraïne, en voortbouwen op de actieve betrokkenheid van Europol bij de Oekraïense rechtshandhaving via de Oekraïense verbindingsfunctionaris die aanwezig is op het hoofdkwartier van Europol in Nederland.

Het **Europees Grens- en kustwachtagentschap** (**Frontex**) is ook aanwezig in de lidstaten en de buurlanden van de EU ter ondersteuning van grenscontroleoperaties: momenteel zijn er meer dan 2 100 grenswachten gestationeerd in de gehele EU, in de Westelijke Balkan en in Moldavië. **Het Asielagentschap van de Europese Unie** (**EUAA**) heeft bijna 750 medewerkers ingezet in de zuidelijke EU-lidstaten en in Litouwen om operationele activiteiten te ondersteunen, de opvangcapaciteit te versterken en te helpen bij asielprocedures.

Voortbouwend op het huidige **Prümbesluit**[30], dat de lidstaten een kader biedt om rechtshandhavingsfunctionarissen in te zetten voor gezamenlijke operaties zoals gezamenlijke patrouilles, hebben de Commissie en het Franse voorzitterschap van de Raad van de Europese Unie alle lidstaten een gezamenlijke brief gestuurd om de behoeften te inventariseren en te verzoeken om politiemensen in te zetten voor gezamenlijke patrouilles in de lidstaten aan de EU-grenzen die het meest te maken hebben met massale grensoverschrijdingen als gevolg van de oorlog. De Commissie zal deze inzet financieren uit het fonds voor interne veiligheid/politie.

---

[28] Mededeling van de Commissie met operationele richtsnoeren voor het beheer van de buitengrenzen om grensoverschrijdingen aan de grenzen tussen de EU en Oekraïne te faciliteren (C(2022) 104 I/01).

[29] Sinds 3 mei heeft Europol 1 Europol-medewerker en 3 uitgezonden functionarissen ingezet in Slowakije, 1 Europol-medewerker in Polen, 1 Europol-medewerker en 4 uitgezonden functionarissen in Roemenië, en 2 uitgezonden functionarissen in Hongarije. 1 Europol-medewerker en 2 uitgezonden functionarissen zijn in Moldavië ingezet.

[30] 2008/615/JBZ en 2008/616/JBZ.

Aanpak van mensenhandel

De EU is vanaf de eerste dagen van de oorlog alert geweest op de risico's van één bepaalde vorm van criminele activiteit die zou kunnen profiteren van de massale bewegingen van mensen die veiligheid zoeken in de EU. Het is van essentieel belang geweest te voorkomen dat mensenhandelaars zich richten op kwetsbare mensen die onderweg zijn, meestal **vrouwen en kinderen**, en daarbij bijvoorbeeld gebruikmaken van valse aanbiedingen van vervoer of onderdak.

In maart hebben Europol en Eurojust de bevoegde nationale autoriteiten vroegtijdige waarschuwingen gestuurd over de mogelijkheid van mensenhandel en de uitbuiting van slachtoffers die uit Oekraïne komen. Eurojust helpt de uitwisseling van informatie te verbeteren en de justitiële samenwerking te versnellen, ook met Oekraïne, en onderzoeken naar mensenhandel zijn voor coördinatie naar het agentschap doorverwezen.

De EU-coördinator voor de bestrijding van mensenhandel heeft overleg gevoerd met het EU-netwerk van nationale rapporteurs en gelijkwaardige mechanismen, de agentschappen voor justitie en binnenlandse zaken en het EU-platform van het maatschappelijk middenveld tegen mensenhandel, om van gedachten te wisselen over de maatregelen die nodig zijn om misbruik te voorkomen en te bestrijden en om slachtoffers te beschermen. In verschillende lidstaten zijn er onderzoeken naar mogelijke gevallen ingesteld.

De EU heeft snel en energiek gezorgd voor een gecoördineerde reactie op deze reële bedreiging voor mensen die de hulp van de EU nodig hebben. Operationele richtsnoeren[31], onder meer over het probleem van de mensenhandel, werden snel aangeboden aan de lidstaten die de richtlijn tijdelijke bescherming uitvoeren, ter ondersteuning van burgers die de oorlog in Oekraïne ontvluchten. Als onderdeel van het 10-puntenplan voor een betere Europese coördinatie van de opvang van mensen die de oorlog in Oekraïne ontvluchten[32], dat werd gepresenteerd tijdens de Raad Justitie en Binnenlandse Zaken van 28 maart 2022, is een gemeenschappelijk plan ter bestrijding van mensenhandel[33], over het voorkomen van mensenhandel en het helpen van slachtoffers, ontwikkeld door de EU-coördinator voor de bestrijding van mensenhandel, in samenwerking met de EU-agentschappen en de lidstaten. Bijzondere aandacht gaat uit naar de registratie van entiteiten en personen (waaronder vrijwilligers) die accommodatie, vervoer en andere vormen van bijstand willen verlenen, en naar het verrichten van achtergrondcontroles. De Commissie heeft ook samengewerkt met het EUAA om de opsporing van slachtoffers van mensenhandel te ondersteunen wanneer in opvangcentra medische controles worden uitgevoerd. Alleenreizende of van hun familie gescheiden kinderen lopen een bijzonder risico op misbruik, seksuele uitbuiting of gedwongen criminaliteit. De bovengenoemde operationele richtsnoeren bevatten ook richtlijnen om de lidstaten te helpen bij de aankomst en opvang van en de steun aan kinderen, en alleenreizende minderjarigen in het bijzonder. Om risicogroepen bewuster te maken van de problematiek, heeft de Commissie ook een speciale website opgezet met praktische adviezen over hoe mensenhandelaars kunnen worden vermeden.

[31] C(2022) 1806, EUR-Lex – 52022XC0321(03) (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

Sommige maatregelen om de paraatheid te verhogen zijn specifiek genomen in reactie op de nieuwe omstandigheden die door de oorlog zijn ontstaan, maar andere belangrijke maatregelen vloeien voort uit **wetgevingsinitiatieven** die al in de pijplijn zaten vóór de Russische aanvalsoorlog tegen Oekraïne.

De Commissie is verheugd dat in februari 2022 overeenstemming is bereikt over het herziene mandaat van **Europol**[34], dat Europol na uitvoering in staat zal stellen de lidstaten beter te ondersteunen in de strijd tegen georganiseerde misdaad en terrorisme. Het agentschap zal dan over de juiste instrumenten en waarborgen beschikken om de politiediensten te ondersteunen bij het analyseren van big data om misdaad te onderzoeken en bij het ontwikkelen van vernieuwende methoden om cybercriminaliteit aan te pakken. Deze veranderingen gaan gepaard met een versterkt kader voor gegevensbescherming en een sterker parlementair toezicht en betere controleerbaarheid.

Het pakket over **politiesamenwerking** dat op 8 december 2021[35] door de Commissie werd gepresenteerd en waarover momenteel wordt onderhandeld, zal de samenwerking tussen rechtshandhavingsfunctionarissen in de lidstaten versterken door de uitwisseling van gegevens sneller, gemakkelijker en veiliger te maken, en door de operationele politiesamenwerking ter plekke te verbeteren en efficiënter te maken. De Commissie roept het Europees Parlement en de Raad op dit pakket snel te bekrachtigen.

Zodra deze wetgevingsvoorstellen zijn aangenomen en uitgevoerd, zullen zij de rechtshandhaving ondersteunen in de strijd tegen de grensoverschrijdende georganiseerde misdaad. Dit zal met name van belang zijn tegen een achtergrond waarin misdaadorganisaties uit Oekraïne vanwege de huidige situatie wellicht zullen proberen zich elders te vestigen en hun activiteiten in de EU voort te zetten.

De **EU-adviesmissie in Oekraïne** ondersteunt de hervorming van de instellingen voor rechtshandhaving en de rechtsstaat in het land al sinds 2014. In maart 2022 is het mandaat van de missie herzien om steun mogelijk te maken aan de Oekraïense grensovergangen met Polen, Roemenië en Slowakije, om bij te dragen tot het situationeel bewustzijn van grensoverschrijdende criminele activiteiten, waaronder mensensmokkel, en om de stroom van humanitaire goederen naar Oekraïne te verbeteren.

IV. WAPENS, GEVAARLIJKE MATERIALEN EN KRITIEKE INCIDENTEN

De oorlog heeft het verkeer van vuurwapens en andere wapens in Oekraïne zelf enorm doen toenemen, wat nieuwe risico's inhoudt voor de EU en andere staten die aan Oekraïne grenzen.

Waakzaamheid en coördinatie

De in maart gepubliceerde operationele richtsnoeren geven de lidstaten advies over de aanpak van het toegenomen verkeer van vuurwapens in een tijd van massale aankomsten aan de

[34] COM(2020) 796.
[35] COM(2021) 780, COM(2021) 782, COM(2021) 784.

buitengrens van de EU[36]. In deze richtsnoeren wordt onderstreept dat de aanwezigheid van vuurwapens voortdurend moet worden gecontroleerd en dat niemand zonder vergunning de EU mag binnenkomen met een vuurwapen. Wanneer deze vuurwapens door de Oekraïense autoriteiten als vermist worden opgegeven, dienen de lidstaten ze in het Schengeninformatiesysteem op te nemen.

Het is van cruciaal belang dat alle zendingen van vuurwapens naar Oekraïne naar behoren worden geregistreerd, met alle relevante informatie (waaronder type, land en jaar van vervaardiging, merk, kaliber, serienummer) teneinde de traceerbaarheid van die vuurwapens, zowel in Oekraïne als in de EU, te vergemakkelijken.

De EU heeft de roekeloze militaire aanvallen van Rusland op en in de directe omgeving van civiele nucleaire, biologische en chemische installaties in Oekraïne, alsmede alle acties die de veiligheid van deze installaties in gevaar brengen, publiekelijk betreurd. De Commissie volgt de situatie in Oekraïne en besteedt daarbij bijzondere aandacht aan de stralingsdreiging, die vanuit het oogpunt van de interne veiligheid van de EU de grootste bron van zorg is[37]. De Commissie houdt ook toezicht op potentiële chemische dreigingen en heeft een intern coördinatiemechanisme opgezet voor het geval een snelle risicobeoordeling nodig is.

Paraatheid

Oekraïne is reeds een van de landen die in het EU-actieplan 2020–2025 inzake illegale vuurwapenhandel zijn aangemerkt als sleutellanden voor specifieke acties op extern niveau. Er vindt ook een specifieke operationele actie plaats in de regio, waaronder in Oekraïne, in het kader van het onderdeel vuurwapens van EMPACT. Gezien het risico dat vuurwapens worden omgeleid, zullen er echter specifieke door de EU gefinancierde projecten nodig zijn, alsmede operationele samenwerking met Europol, Frontex en het onderdeel vuurwapens van EMPACT. De Commissie zal binnenkort een voorstel indienen tot herziening van de vuurwapenverordening[38] over de uitvoer, invoer en doorvoer van civiele vuurwapens, als onderdeel van het algemene wettelijke en operationele kader voor het voorkomen, opsporen, onderzoeken en vervolgen van de handel in vuurwapens.

Om de paraatheid en de reactie van de EU ten aanzien van risico's voor de volksgezondheid, zoals CBRN-dreigingen, te verbeteren, bouwt de Commissie strategische reserves van reactiecapaciteiten op via het Uniemechanisme voor civiele bescherming (UCPM), dat wordt gefinancierd door de Autoriteit voor paraatheid en respons inzake noodsituaties op gezondheidsgebied (HERA)[39]. De diensten van de Commissie werken samen aan de ontwikkeling van een strategische reserve van 540,5 miljoen euro voor de rescEU-voorraad. Deze voorraad zal bestaan uit uitrusting en geneesmiddelen, vaccins en andere therapeutische

---

[36] Mededeling van de Commissie met operationele richtsnoeren voor het beheer van de buitengrenzen om grensoverschrijdingen aan de grenzen tussen de EU en Oekraïne te faciliteren (C(2022) 104 I/01).

[37] De Commissie zal – in samenwerking met de partners in de VS – een workshop organiseren over de risico's die verbonden zijn aan radiologisch materiaal dat zich in ziekenhuizen bevindt en niet meer door regulatoren te controleren is.

[38] Verordening (EU) nr. 258/2012 van het Europees Parlement en de Raad van 14 maart 2012 tot uitvoering van artikel 10 van het Protocol van de Verenigde Naties tegen de illegale vervaardiging van en handel in vuurwapens, hun onderdelen, componenten en munitie, tot aanvulling van het Verdrag van de Verenigde Naties ter bestrijding van grensoverschrijdende georganiseerde misdaad (VN-protocol inzake vuurwapens), en tot vaststelling van uitvoervergunningen voor vuurwapens, hun onderdelen, componenten en munitie en maatregelen betreffende de invoer en doorvoer ervan.

[39] Werkprogramma van HERA voor 2022 (europa.eu)

middelen voor de behandeling van patiënten die zijn blootgesteld aan CBRN-stoffen, plus een rescEU-ontsmettingsreserve van ontsmettingsapparatuur en deskundige responsteams. Als onmiddellijke eerste stap heeft de EU haar medische rescEU-reserve gemobiliseerd om kaliumjodiumtabletten aan te schaffen die kunnen worden gebruikt om mensen te beschermen tegen de schadelijke effecten van straling, alsmede andere producten die in Oekraïne dringend nodig zijn. Via het UCPM werden, met de hulp van Frankrijk en Spanje, reeds bijna 3 miljoen jodidetabletten aan Oekraïne geleverd.

V. GECOÖRDINEERDE ACTIE OM DE VERANTWOORDENLIJKEN VOOR DE RUSSISCHE AGRESSIE TER VERANTWOORDING TE ROEPEN

De EU speelt een beslissende rol in de acties van de internationale gemeenschap om Rusland onder druk te zetten een einde te maken aan zijn agressie tegen de Oekraïense staat en de burgers die in het conflict verwikkeld zijn geraakt; deze agressie is onaanvaardbaar en in strijd met het internationale recht. Deze druk omvat maatregelen om de gevolgen voor de daders aan te geven, waaronder strenge sancties, en acties om oorlogsmisdaden op te sporen en de vervolging ervan te vergemakkelijken.

Beperkende maatregelen en confiscatie

Sinds Rusland op 21 februari 2022 de niet door de regering gecontroleerde gebieden van de oblasten Donetsk en Loehansk in Oekraïne heeft erkend, en sinds de invasie van Oekraïne op 24 februari 2022, heeft de EU de meest uitgebreide reeks beperkende maatregelen ooit tegen Rusland opgelegd. Tot dusver zijn vijf sanctiepakketten aangenomen. Deze maatregelen zijn gericht op sleutelsectoren, zoals financiën, handel, vervoer, defensie en de media, en zijn gericht tegen politieke en militaire elites, alsmede tegen prominente Russische en Wit-Russische oligarchen. Op de lijsten staan reeds meer dan 1 000 personen en 80 entiteiten. Een zesde pakket sancties wordt momenteel in de Raad behandeld.

Het effect van deze en eerdere beperkende maatregelen tegen Russische en Wit-Russische personen en bedrijven zal even groot zijn als de handhaving ervan. Gecoördineerd EU-optreden kan een belangrijke bijdrage leveren aan het dichten van mogelijke mazen in de wetgeving, en de Commissie heeft de belanghebbenden uitgebreide ondersteuning geboden in de vorm van schriftelijke richtsnoeren, overleg met belanghebbenden en een speciale deskundigengroep, en een reeks middelen om de naleving te vergemakkelijken.

Daarnaast heeft de Commissie een taskforce “Freeze and Seize” opgericht waarin de diensten van de Commissie, de lidstaten, Eurojust en Europol samenwerken. Tot dusver hebben de lidstaten naar verluidt tegoeden ter waarde van 9,89 miljard euro bevroren[40]. Op 11 april heeft Europol samen met de lidstaten, Eurojust en Frontex Operatie Oscar gelanceerd, ter ondersteuning van financiële en strafrechtelijke onderzoeken naar criminele vermogensbestanddelen die in handen zijn van personen en entiteiten die vallen onder de EU-sancties in verband met de oorlog van Rusland tegen Oekraïne. De EU-taskforce “Freeze and Seize” werkt nauw samen met de “REPO taskforce (*Russian Elites, Proxies, and Oligarchs*)”, die is opgezet door de landen van de G7 (Canada, Frankrijk, Duitsland, Italië, Japan, het Verenigd Koninkrijk en de Verenigde Staten) en gelijkgestemde partners zoals Australië, alsook met de KleptoCapture-taskforce van de VS en de taskforce “Oekraïne”.

[40] Er is ook een bedrag van ongeveer 23 miljard euro aan geblokkeerde activa van de Russische centrale bank.

De taskforce "Freeze and Seize" fungeert als platform om de uitwisseling van informatie en ervaringen tussen de lidstaten te coördineren en te vergemakkelijken, richtsnoeren te verstrekken voor de uitvoering van sancties, en de uitwisseling van beste praktijken op het gebied van strafrechtelijk onderzoek en confiscatie te vergemakkelijken. Het is met name van belang dat de rechtshandhavingsinstanties alert en proactief zijn met betrekking tot mogelijke strafbare feiten door de personen en entiteiten op de sanctielijsten. De taskforce wil ook besprekingen op gang brengen over de mogelijke aanwending van geconfisqueerde middelen, bijvoorbeeld om bij te dragen tot de wederopbouw van Oekraïne.

De Commissie keurt vandaag een pakket maatregelen inzake de **ontneming en confiscatie van vermogensbestanddelen** goed[41], waarin rekening wordt gehouden met de lessen die zijn getrokken uit de uitvoering van de beperkende maatregelen van de EU tegen Russische en Wit-Russische personen en entiteiten. Het zal de doeltreffende uitvoering van beperkende maatregelen van de EU in de gehele EU vergemakkelijken door een snelle opsporing en identificatie mogelijk te maken van goederen die eigendom zijn van of gecontroleerd worden door personen of entiteiten die aan dergelijke maatregelen zijn onderworpen. Het versterkte kader voor de ontneming en confiscatie van vermogensbestanddelen zal ook gelden voor de schending van beperkende maatregelen en zal er aldus voor zorgen dat de opbrengsten van de schending van beperkende maatregelen daadwerkelijk worden opgespoord, bevroren, beheerd en geconfisqueerd. Om ervoor te zorgen dat de vermogensbestanddelen van de personen en entiteiten die de beperkende maatregelen schenden, daadwerkelijk kunnen worden geconfisqueerd, keurt de Commissie vandaag ook voorstellen voor een besluit van de Raad goed om de schending van sancties toe te voegen aan de lijst van EU-misdrijven van artikel 83, lid 1, VWEU[42], vergezeld van een mededeling[43], met het oog op de indiening van een voorstel voor een richtlijn tot onderlinge afstemming van de definitie van de strafbare feiten en de sancties op schending van de beperkende maatregelen.

Meer in het algemeen betekent dit pakket een cruciale stap in de strijd tegen de georganiseerde misdaad. Het sluit aan bij de verbintenissen die de Commissie is aangegaan in de strategie voor de veiligheidsunie en de strategie 2020–2025 ter bestrijding van de georganiseerde misdaad[44]. De richtlijn herziet de confiscatierichtlijn van 2014, het Besluit van de Raad inzake de bureaus voor de ontneming van vermogensbestanddelen (BOV's) van 2007 en het Kaderbesluit inzake de confiscatie van opbrengsten van misdrijven, alsmede van de daarbij gebruikte hulpmiddelen en de door middel daarvan verkregen voorwerpen van 2005, teneinde de capaciteit voor het opsporen en identificeren en uiteindelijk het confisqueren van illegale opbrengsten te versterken en aldus het zeer lage percentage confiscaties in de EU aan te pakken[45]. Het pakket breidt het bereik van de bestreken strafbare feiten uit en breidt de regels inzake confiscatie uit tot gevallen waarin een strafrechtelijke veroordeling voor een specifiek misdrijf niet mogelijk is, maar waarin de vermogensbestanddelen duidelijk afkomstig zijn van criminele activiteiten. De herziening versterkt ook het effectieve beheer van bevroren en geconfisqueerde vermogensbestanddelen en vergroot de capaciteit van de BOV's om illegale vermogensbestanddelen op te sporen en

[41] COM(2022) 245.
[42] COM(2022) 247.
[43] COM(2022) 249.
[44] COM(2021) 170.
[45] Europol schat dat slechts 2 % van de criminele vermogensbestanddelen wordt bevroren (2,4 miljard euro) en 1 % wordt geconfisqueerd (1,2 miljard euro), terwijl de criminele inkomsten op de belangrijkste criminele Markten in de EU in 2019 139 miljard euro bedroegen (1 % van het bbp van de EU).

te identificeren. Het nieuwe EU-kader voor de ontneming van vermogensbestanddelen is bedoeld om de complexe modus operandi van misdaadorganisaties aan te pakken, die vaak grensoverschrijdend opereren en verschillende methoden gebruiken om hun vermogensbestanddelen te verbergen, onder meer door middel van cryptoactiva.

Gecoördineerde justitiële reactie

Ook op EU-niveau is gewerkt aan een gecoördineerde justitiële reactie op **internationale misdrijven** die in Oekraïne zouden zijn gepleegd, zodat de daders ter verantwoording kunnen worden geroepen.

Door twee lidstaten en Oekraïne is een gemeenschappelijk onderzoeksteam (GOT) ingesteld om onderzoek te doen naar oorlogsmisdaden, misdaden tegen de menselijkheid en andere internationale misdrijven die op Oekraïens grondgebied zouden zijn begaan. Eurojust verleent juridische, analytische, financiële en logistieke steun aan dit GOT. Op 25 april 2022 heeft het parket van de Aanklager van het Internationaal Strafhof (ICC) zich als deelnemer bij het GOT gevoegd[46] en verwacht wordt dat zich spoedig nog meer deelnemers zullen aansluiten.

Op 25 april 2022 heeft de Commissie een voorstel ingediend tot wijziging van de Eurojust-verordening[47] om Eurojust in staat te stellen bewijsmateriaal van ernstige internationale misdrijven veilig te stellen, te analyseren en te bewaren. Eurojust en Europol zullen gedurende dit proces nauw blijven samenwerken. Een cruciale rol bij de coördinatie van de justitiële reactie is ook weggelegd voor het Genocidenetwerk, waarvan Eurojust het secretariaat verzorgt, dat een atlas heeft opgesteld van ngo's die momenteel actief zijn in Oekraïne en nationale beroepsbeoefenaars uit de lidstaten en Oekraïne ondersteunt die actieve zaken in verband met de oorlog behandelen.

In april 2022 heeft de Raad het mandaat van de **EU-adviesmissie in Oekraïne** verder herzien, en aldus de weg geëffend voor steun van de missie aan de Oekraïense autoriteiten bij het onderzoek naar en de vervolging van internationale misdrijven die tegen de achtergrond van de militaire agressie van Rusland zijn gepleegd. De missie zal de Oekraïense autoriteiten strategisch advies verstrekken over onderzoek naar en vervolging van internationale misdrijven, noodzakelijke wijzigingen in de Oekraïense wetgeving, communicatiestrategie, alsmede opleiding over aanverwante aangelegenheden. De missie maakt deel uit van een aantal coördinatie-initiatieven in dit verband en maakt samen met de EU-delegatie deel uit van de Adviesgroep VS-EU inzake gruweldaden in Oekraïne.

VI. BUITENLANDSE INFORMATIEMANIPULATIE EN INMENGING

De huidige geopolitieke ontwikkelingen hebben de risico's van buitenlandse inmenging onderstreept. De militaire agressie van Rusland tegen Oekraïne is gepaard gegaan met **informatiemanipulatie- en inmengingsactiviteiten**. Ongegronde beschuldigingen van "nazisme" en "genocide" tegen de Oekraïense regering, "false flag"-operaties en ongegronde beschuldigingen aan het adres van de NAVO en het Westen zijn gebruikt om de brute aanvallen op Oekraïne te rechtvaardigen, terwijl de vrije meningsuiting en onafhankelijke berichtgeving in Rusland zijn onderdrukt. Er is een voortdurend risico van gemanipuleerd

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

audiovisueel materiaal en desinformatie dat Rusland kan proberen te gebruiken als voorwendsel voor extra militaire aanvallen, om de vastberadenheid van het Oekraïense verzet te verzwakken, om de internationale gemeenschap te verdelen in haar verzet tegen de oorlog, of om twijfel te zaaien over de schendingen door Rusland van het internationale recht. De EU heeft zich er in het Strategisch Kompas toe verbonden krachtig te reageren op buitenlandse informatiemanipulatie en inmenging, en haar veerkracht en vermogen om dergelijke dreigingen het hoofd te bieden, te vergroten[48]. Manipulatie van het democratisch debat binnen de EU is het onderwerp van het Europees actieplan voor democratie, het gecoördineerde plan van de Commissie om desinformatie aan te pakken en de democratische weerbaarheid te versterken[49].

Waakzaamheid en coördinatie

De Europese Unie heeft met een vastberaden en gecoördineerd optreden gereageerd op de desinformatiecampagne van Rusland in het kader van de militaire agressie tegen Oekraïne. De EU heeft nauw samengewerkt met haar lidstaten via het systeem voor snelle waarschuwingen, en met internationale partners zoals de NAVO, de VS, Canada en het snellereactiemechanisme van de G7, om inzichten te delen in de manipulatietendensen en -tactieken van het Kremlin. De activiteiten om de manipulatie van het Kremlin te deconstrueren zijn geïntensiveerd, met name via de website EUvsDisinfo, die in het Engels, Russisch, Oekraïens en andere talen uitzendt om feitelijke informatie te verstrekken binnen de EU, in Oekraïne en de regio, alsook binnen Rusland. Sinds 2 maart zijn de doorgifte en de uitzending van de kanalen van de Russische staatsmedia RT en Sputnik in de EU of gericht op de EU opgeschort, als gevolg van de beperkende maatregelen die de EU heeft genomen. Onlineplatforms, toonaangevende sociale netwerken, adverteerders en partijen uit de reclame-industrie die de gedragscode inzake desinformatie[50] hebben ondertekend, nemen urgent maatregelen om de desinformatie in verband met de Russische agressie tegen Oekraïne te beperken. De Commissie en de EDEO volgen deze inspanningen. Uit de verstrekte informatie blijkt dat de platforms hun toezichts- en interventie-instrumenten in verband met de oorlog hebben versterkt.

Daarnaast worden in hoog tempo acties opgezet om landen in Centraal-Azië en de Westelijke Balkan te ondersteunen bij het versterken van de informatieweerbaarheid en het tegengaan van buitenlandse informatiemanipulatie en desinformatie.

Paraatheid

Openlijke buitenlandse informatiemanipulatie en inmenging (FIMI), met inbegrip van desinformatie als een van de instrumenten van hybride dreigingen, heeft de follow-up van het Europees actieplan voor democratie extra urgent gemaakt. De afgelopen maanden hebben de EU-instellingen de lidstaten ondersteund bij het bestrijden van FIMI, met name in het kader van het systeem voor snelle waarschuwingen, door inzichten uit te wisselen over de tactieken van FIMI-actoren en over reactiestrategieën. Er zijn besprekingen gaande om de algehele reactie van de EU op FIMI verder te versterken, op basis van een door de EDEO gepresenteerde conceptnota over de ontwikkeling van een speciaal **instrumentarium** om deze dreiging het hoofd te bieden. Dit brengt bestaande interne maatregelen en nieuwe EU-

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

instrumenten in het kader van het gemeenschappelijk buitenlands en veiligheidsbeleid samen. Ook wordt een bijdrage geleverd door de EDEO, via intensievere werkzaamheden van haar afdeling Stratcom[51], alsook door de Commissie.

Het Europees Waarnemingscentrum voor digitale media (EDMO) heeft na het uitbreken van de oorlog in Oekraïne een taskforce voor desinformatie opgericht en coördineert acties van feitencontroleurs en onderzoekers in zijn netwerk. De taskforce heeft geanalyseerd hoe de aanhangers van samenzweringstheorieën rond COVID-19 snel zijn overgeschakeld op het verspreiden van pro-Russische hoaxen, een verschuiving die in een aantal lidstaten is waargenomen[52].

Het voorstel voor een wet digitale diensten beoogt een aanpassing aan de snel evoluerende digitale technologieën en aan wat dit betekent voor technologische en democratische uitdagingen, zoals haatzaaien, desinformatie online en destabiliseringsstrategieën. Aanzienlijke vooruitgang in de onderhandelingen door het Europees Parlement en de Raad moet een snelle goedkeuring van het pakket mogelijk maken.

VII. BREDERE PARAATHEID

Nu de oorlog in Europa is teruggekeerd en zich grote geopolitieke verschuivingen voordoen, is de veiligheidscoördinatie in de EU in een hogere versnelling gekomen, op basis van initiatieven die al in de pijplijn zaten vóór de Russische aanvalsoorlog tegen Oekraïne. Initiatieven die in de eerste plaats op de externe veiligheid van de EU zijn gericht, hebben grote gevolgen voor de interne agenda van de veiligheidsunie.

Op 15 februari 2022 heeft de Commissie het **defensiepakket**[53] ingediend, met een aantal initiatieven op gebieden die van cruciaal belang zijn voor defensie en veiligheid binnen de EU. Deze bijdrage van de Commissie aan de Europese defensie en veiligheid bestrijkt het volledige scala van uitdagingen. Er worden concrete stappen voorgesteld om tot een meer geïntegreerde en concurrerende Europese defensiemarkt te komen, met name door de samenwerking binnen de EU te verbeteren en schaalvoordelen tot stand te brengen. Het behelst tevens een routekaart inzake kritische technologieën voor veiligheid en defensie, teneinde onderzoek, technologische ontwikkeling en innovatie in deze sectoren te stimuleren en de afhankelijkheid van kritische technologieën en waardeketens te verminderen. Met het pakket wordt ook beoogd de defensiedimensie in de ruimte op EU-niveau te versterken. Daarnaast wordt nagegaan hoe de Commissie haar acties tegen hybride dreigingen kan opvoeren, onder meer in het cyberdomein, de militaire mobiliteit binnen en buiten Europa kan vergroten, en de uitdagingen in verband met klimaatverandering op defensiegebied verder kan aanpakken. Ter aanvulling van deze werkzaamheden wordt in de gezamenlijke mededeling **over de analyse van de lacunes op het gebied van defensie-investeringen en**

---

[51] De afdeling Strategische communicatie, taskforces en informatieanalyse van de Europese Dienst voor extern optreden biedt strategische communicatieondersteuning bij de uitvoering van het buitenlands en veiligheidsbeleid van de EU in de desbetreffende prioritaire regio's (zuidelijke en oostelijke buurlanden, de Westelijke Balkan) door specifieke strategische communicatieacties te ontwikkelen en uit te voeren die gericht zijn op het bevorderen van het beleid, de waarden, de doelstellingen en de belangen van de EU.

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

[53] https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52022JC0024&qid=1654803323980&from=NL

de te volgen koers[54] van 18 mei nagegaan welke lacunes er op capaciteits- en industrieel gebied moeten worden aangepakt om de meest blootgestelde EU-lidstaten te ondersteunen en welke maatregelen er moeten worden genomen om de geconstateerde tekortkomingen te verhelpen.

De veerkracht van de EU ten aanzien van deze bedreigingen impliceert ook een capaciteitsgestuurde aanpak in alle veiligheidssectoren, zoals bepleit in het actieplan van de Commissie voor synergieën tussen de civiele, defensie- en ruimtevaartindustrieën[55]. Er wordt gewerkt aan het bevorderen van een capaciteitsgestuurde aanpak op het gebied van interne veiligheid en rechtshandhaving.

De Raad heeft op 21 maart 2022 het **Strategisch Kompas voor veiligheid en defensie**[56] vastgesteld, dat kort daarna werd bekrachtigd door de Europese Raad. Het kompas bevat een ambitieus actieplan om het veiligheids- en defensiebeleid van de EU tegen 2030 te versterken. Doel is van de EU een sterkere en capabelere veiligheidsleverancier te maken, die haar burgers beschermt en bijdraagt tot internationale vrede en veiligheid. Het bevat concrete voorstellen, met een zeer precies tijdschema voor de uitvoering, om het vermogen van de EU om in crisissituaties doortastend op te treden, te verbeteren.

Een van de resultaten van het strategisch kompas is de ontwikkeling van een **EU-toolbox tegen hybride dreigingen** die een kader moet bieden voor een gecoördineerde reactie op hybride campagnes die de EU en haar lidstaten treffen, met inbegrip van interne en externe maatregelen. Na de vaststelling van sectorale referentieniveaus voor veerkracht begin 2022[57], zal er een analyse van lacunes en behoeften worden gemaakt. In dit kader zal de EU blijven werken aan paraatheid, veerkracht en reactievermogen ten aanzien van de dreigingen die uitgaan van de Russische agressie en van andere pogingen om democratieën en de op regels gebaseerde multilaterale orde te destabiliseren.

VIII. VOORUITBLIK

In de toekomst zal de EU uiterst waakzaam moeten blijven ten aanzien van zich ontwikkelende dreigingen, en **paraatheid en veerkracht moeten opbouwen voor alle eventualiteiten**. De gevolgen van de oorlog kunnen verschillende vormen aannemen, die nog niet allemaal kunnen worden ingeschat.

De omvang van de verplaatsing van de Oekraïense criminele netwerken is nog niet bekend. Uit eerdere dossiers van Eurojust blijkt een tendens van heroïnehandel van Afghanistan naar de EU via Oekraïne, zoals bevestigd door het Europees Waarnemingscentrum voor drugs en drugsverslaving[58]. Instabiliteit kan het moeilijker maken om op te treden tegen de

[54] JOIN(2022) 24.
[55] COM(2021) 70.
[56] Een strategisch kompas voor veiligheid en defensie – Voor een Europese Unie die haar burgers, waarden en belangen beschermt en bijdraagt aan de internationale vrede en veiligheid: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/nl/pdf
[57] SWD(2022) 21 final.
[58] Verslag over de drugs- en alcoholsituatie in Oekraïne voor 2020 (volgens de gegevens van 2019), OEDT, Stopzetting van de handel in een heroïnesurrogaat in Frankrijk, Polen en Oekraïne, met inbegrip van de planning en uitvoering van een gecontroleerde aflevering, 2021/00446, Eurojust, mei 2020.

heroïnehandel via deze route, met het risico van een mogelijke toename van de drugsstroom naar de EU.

Sommige risico's voor de EU zullen eerder toenemen aan het eind of tijdens mogelijke pauzes in de gevechten. Er zal bijzondere aandacht worden besteed aan het verkeer van vuurwapens, waarbij het risico toeneemt wanneer de gevechten in Oekraïne afnemen. Ervaringen uit het verleden wijzen ook op het risico dat de terugkeer van buitenlandse strijders die gevechtservaring hebben opgedaan en in contact kunnen zijn gekomen met extremistische groeperingen, in een later stadium tot terroristische acties in de EU kan leiden. Dit potentiële verschijnsel moet nauwlettend worden gevolgd, en de Commissie bevordert reeds besprekingen tussen de lidstaten over de problemen die ontstaan door de terugkeer van buitenlandse vrijwilligers met een gewelddadige extremistische achtergrond.

Gelet op deze mogelijke dreigingen is het van belang dat de uitvoering van de strategie voor de veiligheidsunie wordt voortgezet, onder meer met de uitvoering van belangrijke strategieën zoals de EU-cyberbeveiligingsstrategie, de EU-strategie voor de aanpak van georganiseerde criminaliteit (2020–2025), de terrorismebestrijdingsagenda voor de EU (2020–2025), het EU-actieplan inzake illegale vuurwapenhandel (2020–2025), de EU-strategie ter bestrijding van mensenhandel (2021–2025) en de EU-drugsstrategie (2021–2025).

De inspanningen om de EU van het nodige wetgevingskader te voorzien, zullen worden voortgezet. De Commissie bereidt bijvoorbeeld de effectbeoordeling voor van een voorstel dat het op de markt brengen en het gebruik van chemische stoffen met een hoog risico regelt.

IX. CONCLUSIES

De veiligheidsunie blijft haar rol spelen in de voorbereiding van de EU en haar lidstaten op de aanpak van bestaande en mogelijke dreigingen. De Russische aanvalsoorlog tegen Oekraïne heeft aangetoond hoe snel theoretische dreigingen werkelijkheid kunnen worden, en onderstreept het belang van waakzaamheid, coördinatie en paraatheid.

Dit vierde voortgangsverslag over de strategie voor de veiligheidsunie toont aan dat de EU in staat is zich aan te passen, zelfs in het licht van uitzonderlijke en onverwachte dreigingen, zoals de aanvalsoorlog van Rusland tegen Oekraïne. Een vastberaden uitvoering van de strategie voor de veiligheidsunie is belangrijker dan ooit.