Rådet for
Den Europæiske Union

Bruxelles, den 27. maj 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	

FØLGESKRIVELSE

fra:	Martine DEPREZ, direktør, på vegne af generalsekretæren for Europa-Kommissionen
modtaget:	25. maj 2022
til:	Generalsekretariatet for Rådet
Komm. dok. nr.:	COM(2022) 252 final
Vedr.:	MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET om den fjerde statusrapport om gennemførelsen af strategien for EU's sikkerhedsunion

Hermed følger til delegationerne dokument COM(2022) 252 final.

Bilag: COM(2022) 252 final

EUROPA-
KOMMISSIONEN

Bruxelles, den 25.5.2022
COM(2022) 252 final

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET

om den fjerde statusrapport om gennemførelsen af strategien for EU's sikkerhedsunion

I. INDLEDNING

Den russiske aggressionskrig mod Ukraine dominerer EU's aktuelle sikkerhedsdagsorden. Krigen truer ikke blot Ukraine, den har også til formål at skade den globale stabilitet og sikkerhed. Inden for EU indebærer det en række risici for borgernes sikkerhed. Der er opstået ny usikkerhed om forsyningen af energi og andre råstoffer, og kritisk infrastruktur kan blive mål for cyberangreb. EU's indre sikkerhed bringes i fare af potentielle angreb eller ulykker som følge af kemiske, biologiske, radiologiske eller kemiske agenser i krigszonen. Sårbarheden hos millioner af mennesker, der er flygtet fra krigen, kan hurtigt udnyttes af organiserede kriminelle gennem handel med kvinder og børn, som er særlig udsatte.

I lyset af disse nye og potentielle trusler er EU forblevet resolut og forenet. Mens krigens konsekvenser hidtil hovedsagelig har været begrænset til Ukraines område, har EU øget *årvågenheden og koordineringen*. Desuden har Fællesskabet intensiveret overvågningen af trusselsbilledet og arbejdet på at styrke modstandsdygtigheden for at sikre *beredskabet*.

I Versailleserklæringen af 10.-11. marts 2022[1] understregede de europæiske ledere behovet for at forberede os på, at der hurtigt opstår nye udfordringer, bl.a. ved at "beskytte os selv mod stadig mere udbredt hybrid krigsførelse, styrke vores cyberrobusthed, beskytte vores infrastruktur — navnlig vores kritiske infrastruktur — og bekæmpe desinformation".

Rammerne for sikkerhedsunionen er afgørende for at garantere sikkerheden i hele EU. De fire strategiske prioriteter i strategien for sikkerhedsunionen[2] er fortsat direkte relevante for denne opgave i den nuværende geopolitiske kontekst. Disse prioriteter er i) et fremtidssikret sikkerhedsmiljø, ii) håndtering af foranderlige trusler, iii) beskyttelse af europæerne mod terrorisme og organiseret kriminalitet og iv) et stærkt europæisk sikkerhedsøkosystem. Krigen har understreget behovet for, at EU og dets medlemsstater gør fuld brug af de lovgivningsmæssige og politiske instrumenter, der allerede er til rådighed under strategien for sikkerhedsunionen, og som understøtter koordineret EU-støtte til medlemsstaterne i spørgsmål om alt lige fra organiseret kriminalitet og terrorisme til cybersikkerhed og hybride trusler.

EU-agenturerne på området retlige og indre anliggender har også intensiveret deres indsats som reaktion på krigen i Ukraine og spillet en central rolle med hensyn til at vurdere trusler og støtte operationelle reaktioner[3]. En fortsat styrkelse af Schengenområdets operationelle praksis og forvaltning er en anden vigtig faktor.

Denne fjerde statusrapport om sikkerhedsunionen fokuserer på udviklingen i de seneste måneder siden den russiske angrebskrig mod Ukraine. Den giver et overblik over de foranstaltninger, der er truffet inden for alle områder af sikkerhedsunionen, og tager hensyn til de beredskabsbehov, der opstår på baggrund af potentielle sikkerhedstrusler som følge af krigen i Ukraine. I bilaget anføres en række fremskridt med hensyn til andre sager vedrørende sikkerhedsunionen.

---

1 https://www.consilium.europa.eu/media/54773/20220311-versailles-declaration-en.pdf.
2 COM(2020) 605 final.
3 Joint Statement from EU Justice and Home Affairs Agencies on Ukraine | European Union Agency for Asylum (europa.eu).

II. CYBERSIKKERHED OG KRITISK INFRASTRUKTUR

Siden krigens udbrud har private aktører og kriminelle organisationer offentliggjort, at de udfører cyberaktiviteter til støtte for den ene eller den anden side. Hacktivisme[4] udgør en trussel på grund af risikoen for afsmittende virkninger i EU på kritiske tjenester, risikoen for angreb fra officielle netværk eller andre uforudsete afsmittende virkninger. Krigen er hidtil i vid udstrækning blevet ført med konventionelle midler med kun begrænsede afsmittende virkninger, men der er en reel risiko for eskalering på dette område.

EU har derfor intensiveret sin koordinering og sit beredskab. De trusler, der opstår som følge af krigen, understreger behovet for at opbygge en kultur med udveksling af oplysninger og ekspertise mellem EU og medlemsstaterne og på tværs af cybersikkerhedsfællesskaberne. Dette omfatter opbygning af et integreret situationskendskab, som deles af EU's institutioner, organer og agenturer og medlemsstaterne, navnlig med hensyn til den kritiske infrastruktur, som det indre markeds funktion afhænger af.

Tilskrivelse af cyberangreb mod Ukraine

Cyberangreb på Ukraine selv begyndte før den russiske aggression og i krigens første dage[5]. De havde til formål at kompromittere Ukraines militære personels brugerkonti og forstyrre de væsentlige tjenester, herunder grænsekontrol og telekommunikation.

Den 14. januar 2022 fremsatte den højtstående repræsentant[6] en erklæring på Den Europæiske Unions vegne, hvori den fordømte cyberangrebene på Ukraine og bekræftede EU's utvetydige støtte til Ukraine.

Den 10. maj fordømte Den Europæiske Union og dens medlemsstater sammen med internationale partnere[7] på det kraftigste den ondsindede cyberaktivitet mod Ukraine den 24. februar, som var rettet mod satellitnettet KA-SAT, der ejes af Viasat, og tilskrev Den Russiske Føderation angrebet direkte. Dette cyberangreb havde en betydelig indvirkning og forårsagede vilkårlige kommunikationsafbrydelser og -forstyrrelser hos flere offentlige myndigheder, virksomheder og brugere i Ukraine. Samtidig påvirkede det flere EU-medlemsstater.

Årvågenhed og koordinering

Siden Ruslands angrebskrig mod Ukraine er overvågningen af cybersikkerhedssituationen i medlemsstaterne og EU-institutionerne øget. ENISA, EU's Agentur for Cybersikkerhed, Det Europæiske Center for Bekæmpelse af Cyberkriminalitet under Europol og CERT-EU, IT-

[4] Et nyligt eksempel på hacktivisme er brugen af "protestware" til at sprede malware til russiske IP-adresser gennem en populær open source-pakke, som kan føre til risici i forsyningskæden og tab af tillid til open source-fællesskabet. Kommissionen har gjort det klart, at (selv velmente) cyberangreb på Rusland er ulovlige.

[5] Microsoft Special Report: An overview of Russia's cyberattack activity in Ukraine; The hybrid war in Ukraine — Microsoft On the Issues.

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

[7] Russiske cyberoperationer over for Ukraine: erklæring fra den højtstående repræsentant på Den Europæiske Unions vegne — Consilium (europa.eu).

beredskabsenheden for EU's institutioner, organer og agenturer samt EU's Efterretnings- og Situationscenter (EU INTCEN) har alle bidraget til EU's fælles situationskendskab, bl.a. ved at sørge for regelmæssig overvågning af mistænkelige cyberaktiviteter, herunder inden for specifikke sektorer såsom energi, transport og luftfart. Desuden har de udarbejdet vurderinger, der kan være retningsgivende for forebyggende foranstaltninger.

Der er også foretaget en intensiveret koordinering og udveksling af oplysninger med cybersikkerhedsnetværk såsom Det Europæiske Netværk af Forbindelsesorganisationer for Cyberkriser (CyCLONe), der omfatter nationale cybersikkerhedsagenturer, Kommissionen og ENISA. For at afspejle denne tilgang internt i EU-institutionerne gør en koordineringsmekanisme, Cyber Crisis Task Force, det muligt at udveksle oplysninger mellem alle relevante tjenester, organer og agenturer, herunder ENISA, Europols Europæiske Center for Bekæmpelse af Cyberkriminalitet og CERT EU. Der er behov for en konstant indsats for at sikre kommunikationskanaler mellem det politiske, operationelle og tekniske niveau samt for at styrke samarbejdet med netværket af enheder, der håndterer IT-sikkerhedshændelser (CSIRT).

Desuden har Europol udløst EU's beredskabsprotokol om retshåndhævelse, der gør det muligt at styrke overvågningen af cybertrusler og informationsudvekslingen mellem en bred vifte af interessenter med henblik på at opbygge et omfattende cyberefterretningsbillede.

Medlemsstaterne, EU-Udenrigstjenesten og Kommissionens tjenestegrene udviser også øget årvågenhed med hensyn til kritiske infrastrukturers eksponering for andre fysiske trusler end cybertrusler. Kritisk infrastruktur og enheder, der driver den, kan blive udsat for fysiske risici, såsom sabotage fra statslige eller statsstøttede aktørers side som led i mulige gengældelsesforanstaltninger over for EU.

Beredskab

Beredskab på området for cybersikkerhed og sikring af kritisk infrastruktur er vigtigere end nogensinde i betragtning af Europas øgede eksponering for en ophobning af trusler som følge af krigen. Indsatsen for at øge beredskabet har omfattet en række direkte aktioner, herunder nogle, der allerede var planlagt før Ruslands aggression mod Ukraine. Disse aktioner omfatter øvelser, vejledning, lovgivningsmæssige foranstaltninger, øget modstandsdygtighed i kritiske sektorer og samarbejde med partnere.

Det franske formandskab for Rådet for Den Europæiske Union tilrettelagde i begyndelsen af 2022 sammen med Tjenesten for EU's Optræden Udadtil (EU-Udenrigstjenesten) og Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) en scenariebaseret øvelse kaldet EU CyCLES (Cyber Crisis Linking Exercise on Solidarity) med det formål at øge bevidstheden på politisk plan og styrke samarbejdet mellem det operationelle og politiske niveau i tilfælde af et omfattende cyberangreb.

ENISA og CERT-EU offentliggjorde i februar **retningslinjer** for, hvordan vi kan øge modstandsdygtigheden og beredskabet i EU[8]. I disse retningslinjer tilskyndes alle organisationer i den offentlige og private sektor i EU til at vedtage et minimum af optimale fremgangsmåder inden for cybersikkerhed for at forbedre cybersikkerhedskulturen væsentligt. I marts offentliggjorde CERT-EU en opfølgende teknisk vejledning med støtte fra

[8] Boosting your Organisation's Cyber Resilience — fælles publikation, 14.2.2022.

ENISA[9] og en sikkerhedsvejledning til styrkelse af konfigurationen af såkaldte Signal-apps[10] med en række praktiske anbefalinger til organisationer med henblik på at forbedre deres stilling på cybersikkerhedsområdet.

Lovgivningsmæssige initiativer

Den aktuelle situation understreger, at det haster med at **gennemføre den eksisterende lovgivning** og fremskynde **vedtagelsen af nye initiativer**.

Kommissionen støtter medlemsstaterne i gennemførelsen af **NIS-direktivet**[11], som kræver, at medlemsstaterne er tilstrækkeligt udstyret, f.eks. med en enhed, der håndterer IT-sikkerhedshændelser (CSIRT), og udpeger kompetente myndigheder. Direktivet danner grundlag for et effektivt samarbejde mellem medlemsstaterne. Den politiske enighed, som medlovgiverne er nået frem til om **NIS2-direktivet**[12], er et yderligere gennembrud med hensyn til at skabe en solid EU-ramme for beredskab.

NIS 2 — yderligere styrkelse af beredskabet

- Det nye direktiv om net- og informationssystemer vil afhjælpe manglerne i det tidligere NIS-direktiv, tilpasse det til de nuværende behov og gøre det fremtidssikret. Det fastsætter minimumsregler for en lovgivningsmæssig ramme og fastlægger mekanismer for effektivt samarbejde mellem de relevante myndigheder i hver medlemsstat.
- Det udvider reglernes anvendelsesområde, idet der tilføjes nye sektorer, som er af afgørende betydning for økonomien og samfundet (f.eks. sektorerne for lægemidler, medicinsk udstyr og fødevarefremstilling). Alle mellemstore og store enheder, der opererer inden for sektorerne eller leverer tjenesteydelser, som er genstand for direktivet, vil være omfattet af dets anvendelsesområde. Offentlige forvaltningsenheder i centralregeringer (undtagen retsvæsenet, parlamenter og centralbanker) og på regionalt plan er også omfattet. Desuden kan medlemsstaterne beslutte, at direktivet finder anvendelse på sådanne enheder på lokalt plan.
- NIS2 vil fastlægge grundlaget for foranstaltninger til styring af cybersikkerhedsrisici og formelt oprette Det Europæiske Netværk af Forbindelsesorganisationer for Cyberkriser, EU-CyCLONe, som vil støtte den koordinerede håndtering af omfattende cybersikkerhedshændelser.
- Forslaget indfører også nærmere bestemmelser om proceduren for indberetning af hændelser, indberetningernes indhold og tidsfrister, ligesom det indeholder bestemmelser om retsmidler og sanktioner for at sikre håndhævelse.
- Medlemsstaterne har 21 måneder fra direktivets ikrafttræden til at indarbejde bestemmelserne i deres nationale lovgivning.

Fremskridtene med NIS 2 bør snarest muligt efterfølges af afslutningen af forhandlingerne om det foreslåede **direktiv om kritiske enheders modstandsdygtighed**[13] ("CER-

[9] Security Guidance 2022-01 — Cybersecurity mitigation measures against critical threats.
[10] CERT-EU Security Guidance 22-002 — Hardening Signal.
[11] Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen.
[12] COM(2020) 823.
[13] COM(2020) 829.

direktivet"), som, når det er vedtaget og gennemført, bør øge kritiske enheders modstandsdygtighed over for en række trusler, herunder terrorangreb, insidertrusler og sabotage. Det er også afgørende, at ambitionsniveauet i direktivet om kritiske enheders modstandsdygtighed matcher ambitionsniveauet i Kommissionens forslag, og at der fortsat er overensstemmelse med det politiske kompromis, der blev indgået om NIS2. Tilsammen vil disse foranstaltninger øge modstandsdygtigheden og beredskabet ved at indføre et mere sammenhængende og robust system, bl.a. i kraft af nationale hændelses- og kriseberedskabsplaner. Disse indgik også i Kommissionens henstilling fra sidste år[14] om oprettelse af den **fælles cyberenhed**, som fastsatte, hvordan de forskellige aktører i cybersikkerhedsøkosystemet (diplomatiet, politiet, civilsamfundet og, hvor det er relevant, forsvaret) skal samarbejde på operationelt plan. Det nuværende trusselsbillede understreger værdien af et sådant effektivt samarbejde mellem centrale aktører.

Kommissionen overvåger fortsat gennemførelsen af værktøjskassen til **5G-cybersikkerhed**.[15]. I den forbindelse vedtog NIS-samarbejdsgruppen den 11. maj en rapport om sikkerheden i forbindelse med Open RAN[16]. Den arbejder også fortsat sammen med medlemsstaterne for at gøre det europæiske kompetencecenter for cybersikkerhed fuldt operationelt.

Den 22. marts 2022 foreslog Kommissionen **nye regler for at indføre fælles cybersikkerheds- og informationssikkerhedsforanstaltninger i alle EU's institutioner, organer og agenturer**. Disse regler vil styrke EU-administrationens modstandsdygtighed og evne til at reagere på cybertrusler og -hændelser. Når disse aktiviteter lægges ind i en fælles ramme, vil det interinstitutionelle samarbejde blive styrket, og risikoeksponeringen vil blive minimeret. Den foreslåede forordning om cybersikkerhed for EU's institutioner, organer og agenturer[17] vil styrke CERT-EU's mandat og føre til oprettelsen af et nyt interinstitutionelt cybersikkerhedsråd, styrke cybersikkerhedskapaciteten og stimulere regelmæssige modenhedsvurderinger og bedre cyberhygiejne. Den foreslåede **forordning om informationssikkerhed**[18] vil skabe et minimumssæt af regler og standarder for informationssikkerhed og sikker håndtering og udveksling af oplysninger for alle EU's institutioner, organer og agenturer med henblik på at sikre en bedre og mere konsekvent beskyttelse mod nye trusler mod deres oplysninger. Kommissionen opfordrer Europa-Parlamentet og Rådet til hurtigt at vedtage disse foranstaltninger.

Kommissionen har nu afsluttet sin offentlige høring om foranstaltninger til styrkelse af digitale produkters **cyberrobusthed** og udarbejdet et forslag, der skal offentliggøres i efteråret[19]. Dette vil afhjælpe sårbarhederne i digitale produkter og tilknyttede tjenester, som — selv om de skaber muligheder for EU's økonomier og samfund — også medfører nye udfordringer, da en cybersikkerhedshændelse har lettere ved at påvirke et helt system og dermed forstyrre økonomiske og sociale aktiviteter, jo mere alt er forbundet.

---

[14] Henstilling om oprettelse af en fælles cyberenhed Europas digitale fremtid i støbeskeen (europa.eu).

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

[16] NIS-samarbejdsgruppen, Report on the cybersecurity of Open RAN, 11. maj 2022.

[17] COM(2022) 122.

[18] COM(2022) 119.

[19] Retsakten om cyberrobusthed — nye cybersikkerhedsregler for digitale produkter og tilknyttede tjenester (europa.eu).

Den 9. marts 2022 vedtog EU's ministre med ansvar for telekommunikation enstemmigt "Nevers Call to Reinforce the EU's Cybersecurity Capabilities", som omfattede gennemførelse af en ny katastrofeberedskabsfond for cybersikkerhed, der skal oprettes af Kommissionen"[20]. Kommissionen overvejer, hvordan de eksisterende midler bedst kan anvendes til at støtte forebyggende foranstaltninger og indsatsforanstaltninger.

Kritiske sektorer

Sikring af EU's **energiforsyning** er afgørende for borgernes velfærd og for, at vores økonomier kan fungere gnidningsløst, og den nuværende situation har understreget behovet for klare regler om cybersikkerhed i denne sektor. Kommissionen er i færd med at udarbejde netregler om cybersikkerhed for grænseoverskridende elektricitetsstrømme som krævet i elforordningen[21] for at fastsætte regler om risikovurderinger, fælles minimumskrav, planlægning, overvågning, rapportering og krisestyring. Siden Ruslands angrebskrig mod Ukraine er målene for netreglerne om cybersikkerhed blevet endnu mere relevante. Kommissionen har også iværksat et strukturelt samarbejde mellem ENISA, ENTSO-E[22], ENTSOG[23], ENTSO for gas og Energifællesskabet om regelmæssig overvågning af cybersikkerhedssituationen i energisektoren.

EU har arbejdet på at beskytte partnernes sikkerhed uden at skabe nye risici for sig selv. Nødsynkroniseringen af Ukraines og Moldovas elnet med det kontinentaleuropæiske net fandt sted i marts 2022 efter vedtagelsen af risikobegrænsende foranstaltninger, navnlig med hensyn til cybersikkerhed.

Krigen og sanktionerne har også skabt mange udfordringer for EU's **transportsektor**, lige fra sikkerhedsrisici for EU's civile luftfart og lastbilchauffører, der sidder fast i konfliktområder, til ødelæggelse af Ukraines transportinfrastruktur, afbrydelse af forsyningskæder og trusler mod den globale fødevaresikkerhed. Den Europæiske Unions Luftfartssikkerhedsagentur har i tæt samarbejde med Kommissionen og Eurocontrol, Den Europæiske Organisation for Luftfartens Sikkerhed, siden krigens begyndelse rådgivet operatørerne om ikke at operere i Ukraines luftrum og undgå at benytte luftrummet inden for 100 sømil fra grænsen mellem Ukraine og Hviderusland/Rusland.

Kommissionen har også arbejdet på at styrke EU's transportsektors beredskab og modstandsdygtighed. Navnlig trækkes der i en ny beredskabsplan for transport[24], der blev vedtaget den 23. maj, på erfaringerne fra både covid-19-pandemien og Ruslands militære aggression mod Ukraine. I planen foreslås en værktøjskasse med 10 tiltag, der skal vejlede EU og dets medlemsstater i forbindelse med indførelsen af kriseberedskabsforanstaltninger, herunder sikring af et minimum af konnektivitet, opbygning af modstandsdygtighed over for cybertrusler og hybride trusler og styrkelse af samarbejdet med internationale partnere om kriseberedskab og -indsats. Desuden fremhæves betydningen af regelmæssigt at teste

[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] Europa-Parlamentets og Rådets forordning (EU) 2019/943 af 5. juni 2019 om det indre marked for elektricitet, EUT L 158 af 14.6.2019, s. 54. Agenturet for Samarbejde mellem Energireguleringsmyndigheder er i øjeblikket ved at gennemgå et forslag.

[22] Det europæiske net af transmissionssystemoperatører for elektricitet.

[23] Det europæiske net af transmissionssystemoperatører for gas.

[24] COM(2022) 21.

modstandsdygtigheden i forskellige krisescenarier, hvor relevante EU-agenturer eller andre aktører samles, og der bygges videre på eksisterende processer.

I henhold til **EU's ramme for sundhedssikkerhed** skal udveksling af oplysninger baseret på systemet for tidlig varsling og reaktion, herunder støtte til medicinsk evakuering fra Ukraine, beskyttes mod cyberangreb, og derfor styrkes systemets sikkerhed.

Samarbejde med partners

EU arbejder fortsat sammen med sine internationale partnere om at forebygge, modvirke, afskrække fra og reagere på ondsindet adfærd i cyberspace. Ruslands angrebskrig mod Ukraine har gjort samarbejdet på dette område vigtigere end nogensinde før. I den henseende har EU-Udenrigstjenesten arbejdet på at udveksle situationskendskab og koordinere reaktionen på ondsindede cyberaktiviteter rettet mod Ukraine samt på at støtte Ukraine og andre i regionen ved at samarbejde med partnere, herunder USA og NATO, for at sikre komplementaritet og undgå overlapninger.

Det tætte samarbejde med USA er også blevet intensiveret inden for rammerne af EU's og USA's handels- og teknologiråd. Den fælles erklæring[25] efter ministermødet i Paris i maj understregede handels- og teknologirådets centrale betydning for det fornyede transatlantiske partnerskab, som har til formål at koordinere EU's og USA's fælles foranstaltninger over for den russiske aggression mod Ukraine. Begge parter var enige om, at et tæt samarbejde om at fremme forsyningskædernes modstandsdygtighed er vigtigere end nogensinde før. Desuden er der oprettet en særlig taskforce vedrørende offentlig finansiering af sikker og modstandsdygtig digital infrastruktur i tredjelande, som skal bane vejen for fælles offentlig finansiering mellem USA og EU af digitale projekter i tredjelande på grundlag af et sæt fælles overordnede principper.

Det strategiske kompas, der blev vedtaget i marts 2022 (se afsnit VII), vil styrke EU's cyberdiplomatiske værktøjskasse yderligere og udvikle EU's cyberforsvarspolitik med det mål at være bedre forberedt på og kunne reagere på cyberangreb som led i en bredere strategi for at styrke EU's evne til at handle i krisesituationer og forsvare sine interesser.

Støtte til cybersikkerhed til Ukraine og nabolandene

EU støttede allerede Ukraines modstandsdygtighed over for cyberangreb før krigen. Allerede i juni 2021 afholdt EU og Ukraine en første cyberdialog, og EU ydede støtte til cybersikkerhed og en robust digital omstilling via programmet EU4Digital Ukraine til en værdi af 25 mio. EUR. Yderligere 1,5 mio. EUR, der ydes via Twinning-programmet, skal hjælpe med at bringe Ukraines cybersikkerhedsinstitutioner i overensstemmelse med EU's standarder.

Efter krigens udbrud fremmer EU samarbejdet mellem cybereksperter i Unionen og ukrainske cybereksperter, og desuden koordinerer EU leveringen af teknisk bistand, udstyr, software og relevante tjenester for at styrke Ukraines cyberrobusthed og cyberforsvar.

Desuden arbejder EU på at vurdere mulighederne for støtte på mellemlang sigt til Moldova, Georgien og Vestbalkan. En fælles vurderingsmission til Moldova med fokus på cybersikkerhedsbehov, som blev gennemført den 3.-4. marts 2022, har ført til vedtagelsen af en særlig kriseberedskabsforanstaltning for hurtigt at øge cybersikkerheden i landet. EU er

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

ved at forberede lignende hurtige støtteforanstaltninger til et udvalgt antal lande på Vestbalkan, som anses for at være særligt udsatte som følge af deres opbakning til EU's sanktioner. Desuden vurderes det, om der kan ydes yderligere bistand til Moldova gennem den europæiske fredsfacilitet.

III. ORGANISERET KRIMINALITET OG TERRORISME

Ruslands angrebskrig mod Ukraine har tvunget millioner af mennesker til at forlade deres hjem, hvilket har medført en kraftig stigning i bevægelserne på tværs af EU's ydre grænser. Den 18. maj var næsten 6 millioner ankommet til EU fra Ukraine og Moldova, og til dato har 2,8 millioner registreret sig med henblik på midlertidig beskyttelse i EU. EU har forsøgt at sikre den hurtigste og mest fleksible modtagelse af de mennesker, der flygter fra krigen, uden at bringe sikkerheden ved EU's ydre grænser i fare. Desuden har EU truffet hidtil usete foranstaltninger for at tilbyde disse mennesker midlertidig beskyttelse, og Fællesskabet er fast besluttet på at sikre alle nyankomne ligebehandling. Samtidig skal der rettes opmærksomhed med de potentielle risici, der kan opstå, når så mange mennesker er på flugt, og EU er med stærk støtte fra de relevante EU-agenturer hele tiden årvågen over for udviklingen inden for organiseret kriminalitet og terrorisme.

Et stærkt Schengensamarbejde i en tid med tiltagende trusler

Det har aldrig været lige så vigtigt at sørge for et højt sikkerhedsniveau i **Schengenområdet** og i EU som netop nu, hvor vi oplever øgede trusler som følge af krigen lige uden for EU's ydre grænse.

I overensstemmelse med den ambitiøse dagsorden for Schengenområdet, der er fastsat i strategien fra juni 2021, vedtog Kommissionen i maj den første Schengenstatusrapport[26]. Den årlige Schengencyklus omfatter en ny forvaltningsmodel for Schengenområdet med et regelmæssigt sundhedstjek af Schengensituationen. Dette vil bidrage til at sikre hurtig udpegelse af mangler og effektive opfølgningsprocedurer med henblik på at gøre Schengenområdet stærkere og mere modstandsdygtigt.

I denne første rapport anerkendes behovet for at styrke indsatsen for at gennemføre vigtige initiativer på EU-plan, herunder systematisk kontrol ved de ydre grænser af alle rejsende, idet der gøres fuld brug af Frontex' og Europols mandater samt foreslåede og tilgængelige redskaber til grænseoverskridende politisamarbejde.

Navnlig udgør den nye arkitektur for EU's informationssystemer for grænser, migration og sikkerhed og deres interoperabilitet hjørnestenen i bestræbelserne på at forbedre den indre sikkerhed og grænseforvaltningen. Det vil være afgørende at sikre effektiv gennemførelse af alle elementer i interoperabilitetsrammen i overensstemmelse med de aftalte tidsfrister.

Årvågenhed og koordinering

[26] COM(2022) 301.

Et stærkere samarbejde om retshåndhævelse på tværs af medlemsstaterne og med tredjelande er afgørende for at sikre bevidsthed om nye kriminalitets- og terrortrusler og foranstaltninger rettet mod kriminelle netværk og enkeltpersoner, der kan forsøge at drage fordel af krigen mod Ukraine. Medlemsstaterne og de operationelle partnere udveksler aktivt relevante tilgængelige oplysninger og kriminalefterretninger med Europol, som krydstjekker og analyserer oplysningerne og gør dem til anvendelige operationelle efterretningsmeddelelser, såsom meddelelser om tidlig varsling og trusselsvurderinger, som deles med partnere.

Organiseret kriminalitet

Organiserede kriminelle er allerede ved at finde måder at udnytte den nuværende situation på. Indledende efterretningsanalyser har udpeget kriminalitetsmønstre på en række områder, herunder menneskehandel, falske angivelser af importerede og eksporterede varer, onlinesvindel, cyberkriminalitet og ulovlig handel med skydevåben. Der er også dokumentation for, at IT-kriminelle udgiver sig for at være fundraisere for Ukraine for at stjæle penge og kryptovaluta[27]. Desuden kan kriminelle organisationer fra Ukraine forsøge at flytte på grund af den nuværende situation og fortsætte deres aktiviteter i EU.

Kommissionen og det franske formandskab for Rådet har samarbejdet indbyrdes og med EU's RIA-agenturer, navnlig Europol, om at mobilisere den europæiske tværfaglige platform mod kriminalitetstrusler (**EMPACT**) for at vurdere, foregribe, forebygge og imødegå eksisterende eller nye alvorlige trusler i form af bl.a. organiseret kriminalitet. Den 7. april 2022 var Europol vært for et EMPACT-møde, der samlede repræsentanter og eksperter fra EU's medlemsstater og sikkerhedssektor for at fokusere på trusler fra alvorlig og organiseret kriminalitet, der er opstået som følge af krigen i Ukraine. De konkrete skridt, der blev drøftet, handlede bl.a. om indsamling af flere efterretninger, gennemførelse af operationelle nødforanstaltninger og omlægning af eksisterende samt fælles aktionsdage på ad hoc-basis.

CELBET (Ekspertgruppen om toldvæsenet ved den østlige og sydøstlige landgrænse) — et samarbejdsprojekt finansieret af Kommissionen — følger udviklingen ved grænsen som led i dens mission om at yde operationel støtte og vejledning til toldembedsmændene og overvåger toldmyndighedernes beslaglæggelser ved overgangsstederne ved EU's grænse med Ukraine (Polen, Slovakiet, Ungarn og Rumænien).

Kriminelle aktiviteter og terroraktiviteter

Selv om der endnu ikke er opstået nogen umiddelbar terrortrussel i EU i forbindelse med den russiske invasion af Ukraine, er der et klart behov for årvågenhed.

Den øgede risiko for kriminelle aktiviteter og terroraktiviteter understreger betydningen af, at medlemsstaterne gør brug af relevante EU-databaser såsom Schengeninformationssystemet, indlæser oplysninger i disse, når det er nødvendigt, og søger i dem i forbindelse med kontrol af personer, der rejser ind i EU. Dette vil bidrage til at sikre, at personer, der udgør en trussel mod EU's indre sikkerhed, identificeres ved de ydre grænser. Eu-LISA, Den Europæiske Unions Agentur for den Operationelle Forvaltning af Store IT-systemer inden for Området

[27] Googles Threat Analysis Group har observeret et stigende antal trusselsaktører, der bruger krigen i Ukraine som lokkemiddel i phishing- og malware-kampagner. Eksperter hos internetsikkerhedsvirksomheden Cyren rapporterer om en stigning i antallet af kryptosvindelnumre, hvor konflikten udnyttes ved brug af falske websteder til donationer.

med Frihed, Sikkerhed og Retfærdighed, sikrer fortsat, at EU's grænseforvaltningssystemer er fuldt tilgængelige og effektive. I retningslinjer[28] til medlemsstaterne er det blevet præciseret, hvordan der kan foretages en afvejning af behovet for at sikre en gnidningsløs håndtering af ankomster ved de ydre grænser, samtidig med at den nødvendige sikkerhedskontrol foretages.

Beredskab

Ud over retningslinjer og koordinering er EU's beredskab blevet styrket gennem udsendelse af EU-agenturernes personale.

Europol har udsendt operationelle hold til de EU-medlemsstater, der grænser op til Ukraine. Disse hold bestod af gæstemedarbejdere fra Europol fra medlemsstaterne og Europoleksperter i Ungarn, Litauen, Polen, Rumænien og Slovakiet samt Moldova[29]. Gæstemedarbejderne fra Europol hjælper de nationale myndigheder med efterfølgende sikkerhedskontroller ved EU's ydre grænser. Europoleksperterne yder støtte ved at indsamle og vurdere oplysninger med henblik på at opdage terror- og kriminalitetstrusler, støtte efterforskninger og identificere personer, der udgør en risiko ved at forsøge at rejse ind i EU. Disse operationelle hold indsamler oplysninger, der indgår i de trusselsvurderinger af kriminalitetstrusler, som medlemsstaterne har adgang til. Indsamlingen af efterretninger gør det muligt for Europol at foregribe udviklingen og koordinere operationelle aktiviteter med EU-medlemsstaterne for at reagere på aktiviteterne hos kriminelle grupper, der søger at drage fordel af krigen i Ukraine, og for at bygge videre på Europols aktive engagement i Ukraines retshåndhævelsesaktiviteter gennem den ukrainske forbindelsesofficer, der er til stede i Europols hovedkvarter i Nederlandene.

Det **Europæiske Agentur for Grænse- og Kystbevogtning (Frontex)** er også til stede i medlemsstaterne og EU's nabolande for at støtte grænsekontroloperationer, idet der i øjeblikket er indsat mere end 2 100 grænsevagter i hele EU, på Vestbalkan og i Moldova. **Det Europæiske Asylstøttekontor (EUAA)** har indsat næsten 750 medarbejdere i de sydlige EU-medlemsstater og i Litauen for at støtte operationelle aktiviteter, styrke modtagelseskapaciteten og hjælpe med asylprocedurer.

På grundlag af den nuværende **Prümafgørelse**[30], som skaber en ramme for, at medlemsstaterne kan indsætte retshåndhævende personale til fælles operationer såsom fælles patruljer, har Kommissionen og det franske formandskab for Rådet sendt en fælles skrivelse til alle medlemsstater for at få udpeget relevante behov og anmode om indsættelse af politifolk med henblik på at iværksætte fælles patruljer i de medlemsstater i EU's frontlinje, der er mest berørt af massegrænsepassager som følge af krigen. Kommissionen vil finansiere disse indsættelser under Fonden for Intern Sikkerhed/politiet.

Bekæmpelse af menneskehandel

EU har lige fra krigens første dage været opmærksom på risikoen for en bestemt slags kriminelle aktiviteter, hvor der kan drages fordel af de enorme strømme af mennesker, som

[28] Meddelelse fra Kommissionen om fastsættelse af operationelle retningslinjer for forvaltningen af de ydre grænser for at lette grænsepassagen ved grænserne mellem EU og Ukraine, 2022/C 104 I/01.

[29] Pr. 3. maj har agenturet udsendt én Europolmedarbejder og tre gæstemedarbejdere i Slovakiet, én Europolmedarbejder i Polen, én Europolmedarbejder og fire gæstemedarbejdere i Rumænien og to gæstemedarbejdere i Ungarn. Én Europolmedarbejder og to gæstemedarbejdere er udsendt til Moldova.

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

søger sikkerhed i EU. Det har været afgørende at forhindre menneskesmuglere i at gå efter sårbare personer på flugt, som for det meste er **kvinder og børn**, ved f.eks. at give dem falske tilbud om transport eller indkvartering.

I marts udsendte Europol og Eurojust meddelelser om tidlig varsling til de relevante nationale myndigheder om potentiel menneskehandel og udnyttelse af ofre, der ankommer fra Ukraine. Eurojust bidrager til at forbedre udvekslingen af oplysninger og fremskynde det retlige samarbejde, herunder med Ukraine, og efterforskninger af menneskehandel er blevet henvist til agenturet med henblik på koordinering.

EU-koordinatoren for bekæmpelse af menneskehandel har holdt møder med EU-netværket af nationale rapportører eller tilsvarende mekanismer til overvågning af menneskehandel, agenturerne for retlige og indre anliggender og EU's civilsamfundsplatform mod menneskehandel for at udveksle oplysninger om de foranstaltninger, der er nødvendige for at forebygge og bekæmpe misbrug og beskytte ofrene. I flere medlemsstater er der indledt undersøgelser af potentielle sager.

EU har været hurtig og energisk med hensyn til at sikre en koordineret reaktion på denne reelle trussel mod mennesker, der har brug for EU's hjælp. De medlemsstater, der gennemfører direktivet om midlertidig beskyttelse for at støtte de mennesker, der flygter fra krigen i Ukraine, har hurtigt fået tilbudt operationelle retningslinjer[31], bl.a. om den udfordring, der er forbundet med menneskehandel. Som led i 10-punktsplanen for stærkere europæisk koordinering af modtagelsen af mennesker, der flygter fra krigen fra Ukraine[32], som blev forelagt på samlingen i Rådet (retlige og indre anliggender) den 28. marts 2022, har EU-koordinatoren for bekæmpelse af menneskehandel udarbejdet en fælles plan for bekæmpelse af menneskehandel[33] og hjælp til ofrene i samarbejde med EU-agenturerne og medlemsstaterne. Der er særligt fokus på at registrere enheder og enkeltpersoner (herunder frivillige), der har til hensigt at tilbyde indkvartering, transport og andre former for bistand samt foretage baggrundskontrol. Kommissionen har også samarbejdet med Den Europæiske Unions Asylagentur for at støtte opdagelsen af ofre for menneskehandel, når der foretages sundhedsvurderinger i modtagelsescentre. Uledsagede børn eller børn, der er blevet adskilt fra deres familie, er i særlig risiko for misbrug, seksuel udnyttelse eller tvungen kriminalitet. Ovennævnte operationelle retningslinjer omfatter også vejledning, der skal hjælpe medlemsstaterne med at håndtere ankomst, modtagelse og støtte til navnlig børn og uledsagede mindreårige. For at øge bevidstheden blandt dem, der er i fare, har Kommissionen desuden lanceret et særligt websted med et afsnit, hvor der gives praktiske råd om, hvordan menneskehandlere kan undgås.

Selv om der er truffet visse foranstaltninger for at øge beredskabet specifikt som reaktion på de nye forhold, der er opstået som følge af krigen, stammer andre vigtige foranstaltninger fra **lovgivningsinitiativer**, der allerede var under forberedelse før Ruslands angrebskrig mod Ukraine.

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

Kommissionen glæder sig over aftalen fra februar 2022 om det reviderede **Europolmandat**[34], som, når det er gennemført, vil gøre det muligt for Europol at yde bedre støtte til medlemsstaterne i kampen mod organiseret kriminalitet og terrorisme. Agenturet vil derefter have de rette værktøjer og sikkerhedsforanstaltninger til at støtte politistyrkerne i at analysere big data for at efterforske kriminalitet og udvikle banebrydende metoder til bekæmpelse af cyberkriminalitet. Disse ændringer medfører en styrket databeskyttelsesramme samt stærkere parlamentarisk kontrol og ansvarlighed.

Den pakke om **politisamarbejde**, som Kommissionen fremlagde den 8. december 2021[35], og som i øjeblikket er under forhandling, vil styrke samarbejdet mellem det retshåndhævende personale i alle medlemsstaterne ved at gøre det hurtigere, lettere og mere sikkert at udveksle oplysninger og ved at styrke og effektivisere det operationelle politisamarbejde i praksis. Kommissionen opfordrer Europa-Parlamentet og Rådet til hurtigt at vedtage denne pakke.

Når disse lovgivningsforslag er vedtaget og gennemført, vil de støtte retshåndhævelsen i kampen mod grænseoverskridende organiseret kriminalitet. Dette vil være særlig vigtigt i en situation, hvor kriminelle organisationer fra Ukraine kan forsøge at flytte på grund af den nuværende situation og fortsætte deres aktiviteter i EU.

EU's rådgivende mission i Ukraine har støttet reformen af landets retshåndhævende institutioner og retsstatsinstitutioner siden 2014. I marts 2022 blev missionens mandat revideret med henblik på at muliggøre støtte ved grænseovergangsstederne mellem Ukraine og henholdsvis Polen, Rumænien og Slovakiet, hvilket har bidraget til situationskendskab til grænseoverskridende kriminelle aktiviteter, herunder menneskehandel, og strømmen af humanitære forsyninger til Ukraine.

IV. VÅBEN, FARLIGE MATERIALER OG KRITISKE HÆNDELSER

Krigen har i meget høj grad øget mængden af skydevåben og andre våben, der er i omløb i Ukraine, hvilket indebærer nye risici for EU og andre stater, der grænser op til landet.

Årvågenhed og koordinering

I de operationelle retningslinjer, der blev udsendt i marts, får medlemsstaterne rådgivning om, hvordan de kan tackle udfordringen med øget omløb af skydevåben i en tid med massetilstrømning til EU's ydre grænse[36]. I disse retningslinjer understreges det, at forekomsten af skydevåben bør kontrolleres løbende, og at ingen uden tilladelse bør have lov til at rejse ind i EU med et skydevåben. Når Ukraines myndigheder indberetter nogen af disse skydevåben som forsvundne, bør medlemsstaterne indberette dem i Schengeninformationssystemet.

Det er afgørende, at alle forsendelser af skydevåben til Ukraine registreres korrekt med alle relevante oplysninger (herunder type, fremstillingsland og -år, mærke, fabrikat, kaliber og serienummer) for at lette sporbarheden af disse skydevåben, både i Ukraine og i EU.

---

[34] COM(2020) 796 final.

[35] COM/2021/780, COM/2021/782, COM/2021/784.

[36] Meddelelse fra Kommissionen om fastsættelse af operationelle retningslinjer for forvaltningen af de ydre grænser for at lette grænsepassagen ved grænserne mellem EU og Ukraine, 2022/C 104 I/01.

EU har offentligt beklaget Ruslands uforsvarlige militære angreb på og i umiddelbar nærhed af civile nukleare, biologiske og kemiske anlæg i Ukraine og alle andre handlinger, der bringer disse anlægs sikkerhed i fare. Kommissionen overvåger situationen i Ukraine og er særlig opmærksom på den strålingsrisiko, der giver anledning til størst bekymring med hensyn til EU's indre sikkerhed[37]. Kommissionen overvåger også potentielle kemiske trusler og har oprettet en intern koordineringsmekanisme, hvis der er behov for hurtige risikovurderinger.

Beredskab

Ukraine er allerede et af de lande, der er udpeget som centrale for specifikke foranstaltninger udadtil i EU's handlingsplan for 2020-2025 om ulovlig handel med skydevåben. Der gennemføres desuden en specifik operationel indsats i regionen, som omfatter Ukraine, inden for rammerne af EMPACT på området skydevåben. I betragtning af risikoen for, at skydevåben omledes til det ulovlige marked, vil der imidlertid være behov for specifikke EU-finansierede projekter samt operationelt samarbejde med Europol, Frontex og EMPACT på området skydevåben. Kommissionen vil snart fremsætte et forslag til revision af forordningen om udførsel, indførsel og transit i forbindelse med civile skydevåben[38] som led i den overordnede retlige og operationelle ramme for forebyggelse, afsløring, efterforskning og retsforfølgning af ulovlig handel med skydevåben.

For at forbedre EU's beredskab og indsats over for folkesundhedsmæssige risici såsom CBRN-trusler er Kommissionen i færd med at opbygge strategiske beredskabskapacitetsreserver gennem EU's civilbeskyttelsesmekanisme (UCPM), der finansieres af Myndigheden for Kriseberedskab og -indsats på Sundhedsområdet (HERA)[39]. Kommissionens tjenestegrene samarbejder om at opbygge et strategisk beredskabslager til en værdi af 540,5 mio. EUR under rescEU-ordningen. Dette lager vil omfatte udstyr og lægemidler, vacciner og andre behandlinger til patienter, der har været udsat for CBRN-agenser, samt omfatte en rescEU-dekontamineringsreserve med henblik på at stille dekontamineringsudstyr og eksperthold til rådighed. Som et umiddelbart første skridt har EU mobiliseret sin medicinske reserve under rescEU-ordningen til indkøb af kaliumiodidtabletter, der kan anvendes til at beskytte mennesker mod de skadelige virkninger af stråling, samt andre genstande, der er akut behov for i Ukraine. Der er allerede blevet leveret næsten 3 mio. iodidtabletter til Ukraine via EU's civilbeskyttelsesmekanisme med hjælp fra Frankrig og Spanien.

V. KOORDINERET INDSATS FOR AT STILLE RUSLAND TIL REGNSKAB FOR SIN AGGRESSION

EU spiller en afgørende rolle i det internationale samfunds bestræbelser på at lægge pres på Rusland for at sætte en stopper for dets aggression mod den ukrainske stat og de civile, der er

---

[37] Kommissionen vil — i samarbejde med sine partnere i USA — afholde en workshop med fokus på risiciene i forbindelse med radiologiske materialer på hospitaler, der ikke længere er underlagt myndighedskontrol.

[38] Europa-Parlamentets og Rådets forordning (EU) nr. 258/2012 af 14. marts 2012 om gennemførelse af artikel 10 i De Forenede Nationers protokol om bekæmpelse af ulovlig fremstilling af og handel med skydevåben og dele, komponenter samt ammunition hertil, der supplerer De Forenede Nationers konvention om bekæmpelse af grænseoverskridende organiseret kriminalitet ("FN's våbenprotokol"), og om fastsættelse af udførselstilladelse og indførsels- og transitforanstaltninger for skydevåben og dele, komponenter samt ammunition hertil.

[39] HERA's arbejdsprogram for 2022 (europa.eu).

fanget i konflikten, da denne aggression er uacceptabel og i strid med folkeretten. Dette pres omfatter foranstaltninger, der skal understrege konsekvenserne for gerningsmændene, herunder strenge sanktioner, og foranstaltninger, som skal blotlægge krigsforbrydelser og lette retsforfølgelsen af disse.

Restriktive foranstaltninger og konfiskation

Siden Ruslands anerkendelse af de ikkeregeringskontrollerede områder Donetsk og Luhansk i Ukraine den 21. februar 2022 og invasionen af Ukraine den 24. februar 2022 har EU indført den største række restriktive foranstaltninger over for Rusland nogensinde. Indtil videre er der vedtaget fem sanktionspakker. Disse foranstaltninger fokuserer på nøglesektorer, herunder finans, handel, transport, forsvar og medier, og er rettet mod den politiske og militære elite samt fremtrædende russiske og belarussiske oligarker. Listerne omfatter allerede mere end 1 000 personer og 80 enheder. En sjette sanktionspakke drøftes i øjeblikket i Rådet.

Disse og tidligere restriktive foranstaltningers virkninger over for russiske og belarussiske enkeltpersoner og virksomheder vil afhænge af, hvor effektivt de håndhæves. EU-koordinering kan yde et væsentligt bidrag til at lukke potentielle smuthuller, og Kommissionen har ydet omfattende støtte til interessenter gennem skriftlig vejledning, møder med interessenter og en særlig ekspertgruppe samt i kraft af en række ressourcer, der skal lette overholdelsen.

Desuden har Kommissionen oprettet en "Freeze and Seize"-taskforce, der samler Kommissionens tjenestegrene, medlemsstaterne, Eurojust og Europol. Indtil videre har medlemsstaterne rapporteret, at de har indefrosset aktiver til en værdi af 9,89 mia. EUR[40]. Den 11. april iværksatte Europol sammen med medlemsstaterne, Eurojust og Frontex Operation Oscar for at støtte finansiel og strafferetlig efterforskning rettet mod kriminelle aktiver, der ejes af enkeltpersoner og juridiske enheder, som er omfattet af EU's sanktioner i forbindelse med Ruslands krig mod Ukraine. EU's "Freeze and Seize"-taskforce arbejder tæt sammen med taskforcen "Russian Elites, Proxies and Oligarchs (REPO)", der er oprettet af G7-landene (Canada, Frankrig, Tyskland, Italien, Japan, Det Forenede Kongerige og USA) og ligesindede partnere såsom Australien samt USA's KleptoCapture Task Force og den ukrainske taskforce.

"Freeze and Seize"-taskforcen fungerer som en platform, der anvendes til at koordinere og lette udvekslingen af oplysninger og erfaringer på tværs af medlemsstaterne og vejlede om gennemførelsen af sanktioner. Den skal desuden lette udvekslingen af bedste praksis vedrørende strafferetlig efterforskning og konfiskation. Det er navnlig vigtigt, at de retshåndhævende myndigheder er opmærksomme på og proaktive i forbindelse med potentielle forbrydelser begået af personer og enheder, der er blevet pålagt sanktioner. Taskforcen har også til formål at fremme drøftelser om eventuel brug af konfiskerede midler, f.eks. for at bidrage til genopbygningen af Ukraine.

Kommissionen vedtager i dag en pakke om **inddrivelse og konfiskation af aktiver**[41], hvori erfaringerne fra gennemførelsen af Unionens restriktive foranstaltninger over for russiske og belarusisske personer og enheder tages i betragtning. Det vil lette en effektiv gennemførelse

[40] Derudover findes der blokerede aktiver til en værdi af ca. 23 mia. EUR i den russiske centralbank.
[41] COM(2022) 245.

af EU's restriktive foranstaltninger i hele Unionen ved at muliggøre hurtig opsporing og udpegelse af ejendom, der ejes eller kontrolleres af personer eller enheder, som er omfattet af disse foranstaltninger. De forbedrede rammer for inddrivelse og konfiskation af aktiver vil også finde anvendelse på overtrædelse af restriktive foranstaltninger, og de vil således sikre effektiv opsporing, indefrysning, forvaltning og konfiskation af udbytte fra overtrædelse af restriktive foranstaltninger. For at sikre, at aktiver tilhørende personer og enheder, der overtræder de restriktive foranstaltninger, rent faktisk kan konfiskeres, vedtager Kommissionen i dag også forslag til Rådets afgørelse om at tilføje overtrædelser af sanktioner til listen over strafbare handlinger i EU i artikel 83, stk. 1, i TEUF[42], ledsaget af en meddelelse[43], med henblik på at foreslå et direktiv om indbyrdes tilnærmelse af definitionen af strafbare handlinger og straffene for overtrædelse af restriktive foranstaltninger.

Mere generelt markerer denne pakke et afgørende skridt i kampen mod organiseret kriminalitet. Den følger Kommissionens tilsagn i strategien for sikkerhedsunionen og strategien for bekæmpelse af organiseret kriminalitet 2020-2025[44]. Pakken reviderer konfiskationsdirektivet fra 2014, Rådets afgørelse fra 2007 om kontorer for inddrivelse af aktiver (ARO) og rammeafgørelsen fra 2005 om konfiskation af udbytte, redskaber og formuegoder fra strafbart forhold. Målet er at styrke kapaciteten til at opspore, identificere og i sidste ende konfiskere ulovlige gevinster og dermed hæve de meget lave konfiskationsprocenter i EU[45]. Pakken udvider anvendelsesområdet til flere strafbare handlinger og udvider reglerne om konfiskation i tilfælde, hvor en straffedom for en bestemt forbrydelse ikke er mulig, men hvor aktiverne klart stammer fra kriminelle aktiviteter. Revisionen styrker også en effektiv forvaltning af indefrosne og konfiskerede aktiver, ligesom den styrker ARO'ernes kapacitet til at opspore og identificere ulovlige aktiver. EU's nye ramme for inddrivelse af aktiver er udformet med henblik på at håndtere de komplekse modus operandi blandt kriminelle organisationer, som ofte opererer på tværs af grænserne og anvender forskellige metoder til at skjule deres aktiver, herunder ved hjælp af kryptoaktiver.

Koordineret retlig reaktion

På EU-plan er der også blevet arbejdet for at sikre en koordineret retlig reaktion på **internationale forbrydelser**, der angiveligt er begået i Ukraine, således at gerningsmændene kan drages til ansvar.

To medlemsstater og Ukraine har oprettet et fælles efterforskningshold for at efterforske krigsforbrydelser, forbrydelser mod menneskeheden og andre internationale forbrydelser, der angiveligt er begået på ukrainsk område. Eurojust yder juridisk, analytisk, finansiel og logistisk støtte til dette fælles efterforskningshold. Den 25. april 2022 sluttede anklagemyndigheden ved Den Internationale Straffedomstol (OTP-ICC) sig til det fælles efterforskningshold som deltager[46], og flere deltagere forventes snart at komme med ombord.

---

42 COM(2022) 247.
43 COM(2022) 249.
44 COM(2021) 170.
45 Europol anslår, at kun 2 % af de kriminelle aktiver er indefrosset (2,4 mia. EUR) og 1 % konfiskeret (1,2 mia. EUR), mens de kriminelle indtægter på de vigtigste kriminelle markeder i EU beløb sig til 139 mia. EUR i 2019 (1 % af EU's BNP).
46 https://www.eurojust.europa.eu/eurojust-and-the-war-in-ukraine.

Den 25. april 2022 fremlagde Kommissionen et forslag om ændring af Eurojustforordningen[47], så Eurojust kan sikre, analysere og opbevare bevismateriale vedrørende folkeretlige kerneforbrydelser. Eurojust og Europol vil fortsat arbejde tæt sammen under hele denne proces. Netværket vedrørende folkedrab, hvis sekretariat har til huse hos Eurojust, spiller også en afgørende rolle i koordineringen af den retlige reaktion. Dette sekretariat har udarbejdet et atlas over NGO'er, der i øjeblikket er aktive i Ukraine, og støtter nationale fagfolk fra medlemsstaterne og Ukraine, som behandler aktive sager med relation til krigen.

I april 2022 reviderede Rådet mandatet for **EU's rådgivende mission i Ukraine** yderligere. Herved banede det vejen for missionens støtte til de ukrainske myndigheder i forbindelse med efterforskning og retsforfølgning af internationale forbrydelser begået i forbindelse med Ruslands militære aggression. Missionen vil give de ukrainske myndigheder strategisk rådgivning om efterforskning og retsforfølgning af internationale forbrydelser, nødvendige ændringer af Ukraines lovgivning og kommunikationsstrategi samt uddannelse i relaterede spørgsmål. Missionen indgår i en række koordineringsinitiativer i denne forbindelse og er sammen med EU-delegationen en del af USA's og EU's rådgivende gruppe vedrørende efterforskning og retsforfølgning af forbrydelser og grusomheder til støtte for Ukraine.

VI. UDENLANDSK MANIPULATION AF OPLYSNINGER OG INDBLANDING

Den aktuelle geopolitiske udvikling har understreget risikoen for udenlandsk indblanding. Ruslands militære aggression mod Ukraine er blevet ledsaget af **manipulation af oplysninger og indblanding**. Der er blevet fremsat grundløse påstande om "nazisme" og "folkedrab" mod den ukrainske regering, "false flag"-operationer og grundløse beskyldninger mod NATO og Vesten for at retfærdiggøre brutale angreb på Ukraine, samtidig med at ytringsfriheden og den uafhængige rapportering i Rusland er blevet afskaffet. Der er en fortsat risiko for manipuleret audiovisuelt materiale og desinformation, som Rusland kan forsøge at bruge som påskud for yderligere militære angreb for at svække den ukrainske modstand, splitte det internationale samfund i dets modstand mod krigen eller så tvivl om Ruslands krænkelser af folkeretten. I det strategiske kompas har EU forpligtet sig til at reagere beslutsomt på udenlandsk manipulation af oplysninger og indblanding og til at øge sin modstandsdygtighed og evne til at imødegå sådanne trusler.[48] Manipulation af den demokratiske debat i EU er emnet for den europæiske handlingsplan for demokrati og Kommissionens koordinerede plan for bekæmpelse af desinformation og styrkelse af den demokratiske modstandsdygtighed[49].

Årvågenhed og koordinering

Den Europæiske Union reagerede med en beslutsom og koordineret indsats over for Ruslands desinformationskampagne i forbindelse med den militære aggression mod Ukraine. EU har arbejdet tæt sammen med sine medlemsstater via det hurtige varslingssystem og med internationale partnere såsom NATO, USA, Canada og G7's mekanisme for hurtig reaktion for at udveksle viden om de manipulationstendenser og -taktikker, der anvendes af Kreml. Arbejdet med at dekonstruere Kremls manipulationer er blevet intensiveret, navnlig via webstedet EUvsDisinfo, som sender på engelsk, russisk, ukrainsk og andre sprog, for at

[47] COM(2022) 187 final.
[48] https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/da/pdf.
[49] COM(2020) 790.

levere faktuelle oplysninger inden for EU, i Ukraine og i regionen samt i Rusland. Siden den 2. marts har de russiske statslige medier RT's og Sputniks transmission og udsendelser i EU eller rettet mod EU været suspenderet som følge af restriktive foranstaltninger, som EU har vedtaget. Onlineplatforme, førende sociale netværk, annoncører og reklamevirksomheder, der har underskrevet adfærdskodeksen om desinformation[50], træffer omgående foranstaltninger for at begrænse desinformation i forbindelse med Ruslands aggression mod Ukraine. Kommissionen og EU-Udenrigstjenesten overvåger disse bestræbelser. De fremlagte oplysninger viser, at platformene har styrket deres overvågnings- og interventionsværktøjer med relation til krigen.

Desuden iværksættes der hurtigt foranstaltninger for at støtte lande i Centralasien og Vestbalkan med henblik på at styrke modstandsdygtigheden over for falsk og vildledende information og bekæmpe udenlandsk manipulation af oplysninger og desinformation.

Beredskab

Den åbenlyse brug af udenlandsk informationsmanipulation og indblanding, herunder desinformation som et af værktøjerne bag hybride trusler, har understreget, hvor vigtigt det er at følge op på den europæiske handlingsplan for demokrati. I de seneste måneder har EU-institutionerne støttet medlemsstaterne i bekæmpelsen af udenlandsk informationsmanipulation og indblanding, navnlig inden for rammerne af det hurtige varslingssystem, ved at udveksle viden om de taktikker, som aktørerne bag denne manipulation og indblanding anvender, og om bekæmpelsesstrategier. Der føres drøftelser om en yderligere styrkelse af EU's overordnede reaktion på udenlandsk informationsmanipulation og indblanding på grundlag af en konceptnote fra EU-Udenrigstjenesten om udvikling af en særlig **værktøjskasse** til håndtering af denne trussel. Dette initiativ samler eksisterende interne foranstaltninger og nye EU-værktøjer under den fælles udenrigs- og sikkerhedspolitik. Det vil også nyde godt af den intensiverede indsats fra Stratcom under EU-Udenrigstjenesten[51] og fra Kommissionen.

Det europæiske observatorium for digitale medier ("EDMO") har efter krigens udbrud i Ukraine oprettet en taskforce om desinformation og koordinerer faktatjekkeres og forskeres tiltag i sit netværk. Det har analyseret, hvordan covid-19-konspirationsteoretikere hurtigt har bevæget sig i retning af at udbrede falske prorussiske budskaber, og dette skift er observeret i flere medlemsstater[52].

Forslaget til retsakten om digitale tjenester har til formål at sikre tilpasning til digitale teknologier i hastig udvikling og de deraf følgende teknologiske og demokratiske udfordringer med hensyn til bl.a. hadefuld tale, desinformation på internettet og destabiliseringsstrategier. Betydelige fremskridt i forhandlingerne i Europa-Parlamentet og Rådet bør muliggøre en hurtig vedtagelse af pakken.

---

[50] https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

[51] Afdelingen for strategisk kommunikation, taskforcer og informationsanalyse under EU-Udenrigstjenesten yder strategisk kommunikationsstøtte i forbindelse med gennemførelsen af EU's udenrigs- og sikkerhedspolitik i relaterede prioriterede regioner (de sydlige og østlige nabolande, Vestbalkan) ved at udvikle og gennemføre specifikke strategiske kommunikationstiltag med fokus på at fremme EU's politikker, værdier, mål og interesser.

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

VII. BREDERE BEREDSKAB

På et tidspunkt, hvor der igen er krig i Europa, og der sker store geopolitiske forandringer, er koordinationen af sikkerhedsforanstaltningerne i EU blevet intensiveret, idet der trækkes på initiativer, som allerede var under forberedelse før Ruslands angrebskrig mod Ukraine. Initiativer, der primært fokuserer på EU's eksterne sikkerhed, har store konsekvenser for sikkerhedsunionens interne dagsorden.

Den 15. februar 2022 fremlagde Kommissionen **forsvarspakken**[53] med en række initiativer på områder af afgørende betydning for forsvar og sikkerhed i EU. Dette bidrag fra Kommissionen til europæisk forsvar og sikkerhed dækker hele spektret af udfordringer. I pakken foreslås konkrete skridt hen imod et mere integreret og konkurrencedygtigt europæisk forsvarsmarked, navnlig ved at styrke samarbejdet inden for EU og skabe stordriftsfordele. Den omfatter også en køreplan for teknologier af afgørende betydning for sikkerhed og forsvar, som skal fremme forskning, teknologisk udvikling og innovation i disse sektorer og mindske afhængigheden af kritiske teknologier og værdikæder. Pakken har endvidere til formål at styrke forsvarsdimensionen i rummet på EU-plan. Desuden ses der på, hvordan Kommissionen kan intensivere sine tiltag mod hybride trusler, herunder på cyberområdet, øge den militære mobilitet i og uden for Europa og i højere grad tackle udfordringerne i forbindelse med klimaændringer med relation til forsvar. Som supplement til dette arbejde tages der i den fælles meddelelse om **analyse af investeringsunderskud på forsvarsområdet og vejen frem**[54] af 18. maj hånd om de kapacitetsmæssige og industrielle mangler, der skal afhjælpes med henblik på at støtte de mest udsatte EU-medlemsstater og udpege foranstaltninger til afhjælpning af de konstaterede mangler.

Sikring af EU's modstandsdygtighed over for disse trusler indebærer også kapacitetsdrevne tilgange på tværs af sikkerhedssektorer som anbefalet i Kommissionens handlingsplan om synergier mellem civil-, forsvars- og rumindustrien[55]. Der arbejdes på at fremme kapacitetsdrevne tilgange på området for intern sikkerhed og retshåndhævelse.

21. marts 2022 vedtog Rådet **det strategiske kompas for sikkerhed og forsvar**[56], som Det Europæiske Råd godkendte kort tid efter. I kompasset skitseres en ambitiøs handlingsplan for styrkelse af EU's sikkerheds- og forsvarspolitik senest i 2030. Målet er at gøre EU til en stærkere og mere kompetent sikkerhedsgarant, der beskytter sine borgere og bidrager til international fred og sikkerhed. Kompasset indeholder konkrete forslag med en meget præcis tidsplan for gennemførelsen med henblik på at forbedre EU's evne til at handle beslutsomt i krisesituationer.

Et af formålene med det strategiske kompas er at udvikle en **EU-hybridværktøjskasse**, der bør udgøre rammerne for en koordineret reaktion på hybride kampagner, der berører EU og dets medlemsstater, herunder interne og eksterne foranstaltninger. Efter kortlægningen af de sektorspecifikke referencescenarier for modstandsdygtighed, der blev foretaget i begyndelsen

---

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

[54] JOIN(2022) 24.

[55] COM(2021) 70.

[56] Et strategisk kompas for sikkerhed og forsvar — For en Europæisk Union, der beskytter sine borgere, værdier og interesser og bidrager til international fred og sikkerhed: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/da/pdf.

af 2022[57], vil der blive foretaget en analyse af mangler og behov. Det er inden for denne ramme, at EU vil fortsætte med at opbygge beredskab, modstandsdygtighed og reaktioner på trusler som følge af Ruslands aggression og ethvert andet forsøg på at destabilisere demokratier og den regelbaserede multilaterale orden.

VIII. FREMTIDSUDSIGTER

Fremover vil EU fortsat skulle være yderst opmærksom på nye trusler og opbygge **beredskab og modstandsdygtighed over for alle eventualiteter**. Følgerne af krigen kan antage forskellige former, som ikke alle kan vurderes endnu.

Det omfang, hvori ukrainske kriminelle netværk fordrives, kendes endnu ikke. Eurojusts hidtidige sagsarbejde viser en tendens til ulovlig handel med heroin fra Afghanistan til EU via Ukraine, hvilket bekræftes af Det Europæiske Overvågningscenter for Narkotika og Narkotikamisbrug (EONN)[58]. Ustabilitet kan gøre det vanskeligere at gribe ind over for heroinhandelen via denne rute og dermed øge risikoen for en mulig stigning i strømmen af narkotika til EU.

Nogle risici for EU er mere tilbøjelige til at øges i slutningen af eller under potentielle pauser i kampene. Der vil blive rettet særlig opmærksomhed mod skydevåben i omløb, og risikoen vil stige, når kampene i Ukraine stilner af. Tidligere erfaringer peger også på risikoen for, at udenlandske krigere, der har opnået kamperfaring, og som kan have været i kontakt med ekstremistiske grupper, vender tilbage og udfører terrorhandlinger i EU på et senere tidspunkt. Dette potentielle fænomen bør overvåges nøje, og Kommissionen er allerede i færd med at fremme drøftelser blandt medlemsstaterne om de udfordringer, der opstår som følge af, at udenlandske frivillige med voldelig ekstremistisk baggrund vender tilbage.

I lyset af disse mulige trusler er det vigtigt, at gennemførelsen af strategien for sikkerhedsunionen fortsætter, bl.a. med gennemførelsen af centrale strategier såsom EU's strategi for cybersikkerhed, strategien for bekæmpelse af organiseret kriminalitet (2020-2025), dagsordenen for bekæmpelse af terrorisme i EU (2020-2025), EU's handlingsplan om ulovlig handel med skydevåben (2020-2025), EU-strategien for bekæmpelse af menneskehandel (2021-2025) og EU's narkotikastrategi (2021-2025).

Bestræbelserne på at give EU de nødvendige lovgivningsmæssige rammer vil fortsætte. Kommissionen er f.eks. i færd med at udarbejde konsekvensanalysen til et forslag om regulering af markedsføringen og anvendelsen af kemikalier i højrisikogruppen.

IX. KONKLUSION

Sikkerhedsunionen spiller fortsat sin rolle med hensyn til at forberede EU og dets medlemsstater på at tackle eksisterende og potentielle trusler. Ruslands angrebskrig mod Ukraine har vist, hvor hurtigt teoretiske trusler kan blive reelle, og understreger betydningen af årvågenhed, koordinering og beredskab.

---

[57] SWD(2022) 21 final.

[58] Rapport om narkotika- og alkoholsituationen i Ukraine for 2020 (ifølge data fra 2019), OEDT, Stopping the trafficking of a heroin substitute in France, Poland and Ukraine, including the planning and execution of a controlled delivery, 2021/00446, Eurojust, maj 2020.

Denne fjerde statusrapport om gennemførelsen af strategien for EU's sikkerhedsunion viser, at EU er i stand til at tilpasse sig, selv i lyset af ekstraordinære og uventede trusler fra f.eks. Ruslands angrebskrig mod Ukraine. En beslutsom gennemførelse af strategien for sikkerhedsunionen er vigtigere end nogensinde.