Europeiska unionens råd

Bryssel den 16 december 2022
(OR. en)

16124/22

JAI 1695	DROIPEN 165
COSI 328	COPEN 450
ENFOPOL 648	FREMP 275
ENFOCUSTOM 179	JAIEX 106
IXIM 298	CFSP/PESC 1733
CT 227	COPS 616
CRIMORG 184	HYBRID 120
FRONT 464	DISINFO 112
ASIM 108	TELECOM 528
VISA 203	DIGIT 248
CYBER 409	COMPET 1045
DATAPROTECT 369	RECH 665
CATS 74	CULT 133

FÖLJENOT

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	13 december 2022
till:	Thérèse BLANCHET, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	COM(2022) 745 final
Ärende:	MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET om den femte lägesrapporten om genomförandet av EU:s strategi för en säkerhetsunion

För delegationerna bifogas dokument – COM(2022) 745 final.

Bilaga: COM(2022) 745 final

EUROPEISKA
KOMMISSIONEN

Bryssel den 13.12.2022
COM(2022) 745 final

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

om den femte lägesrapporten om genomförandet av EU:s strategi för en säkerhetsunion

1. INLEDNING

I juli 2020 antog kommissionen den övergripande strategin för EU:s säkerhetsunion[1]. Sedan dess har hotmiljön förändrats på mycket betydande sätt. Covid-19-krisen accentuerade vissa sårbarheter, särskilt med tanke på allt större användning av internet. Cyberattackerna har fortsatt att öka i omfattning och övergå i nya former[2]. Effekterna av Rysslands anfallskrig mot Ukraina har påverkat EU:s inre säkerhet, med en ökad risk för människohandel, hot om kemiska och nukleära incidenter och olaglig skjutvapenhandel. Kriget har också resulterat i utländsk informationsmanipulering och inblandning. Det nyligen inträffade sabotaget av Nord Stream-gasledningarna har visat att viktiga sektorer som energi, digital infrastruktur, transport och rymden är beroende av en resilient kritisk infrastruktur. Det har återigen visat att den fysiska och digitala säkerheten är nära sammanflätade med varandra och måste skyddas gemensamt.

Denna lägesrapport om säkerhetsunionen syftar till att ge en halvtidsöversikt över strategins genomförande och belysa vad som har uppnåtts och vad som återstår att göra innan den nuvarande kommissionens mandatperiod löper ut. Sedan juli 2020 har EU gjort stora framsteg mot att slutföra åtgärderna på de centrala områden som omfattas av strategins fyra pelare[3]. Denna rapport visar att de allra flesta åtgärder som anges i strategin har vidtagits[4]. En del arbete återstår dock för att allmänheten ska få full effekt av EU:s strategi för en säkerhetsunion – till exempel antagandet av kvarstående lagstiftningsförslag från Europaparlamentet och rådet och medlemsstaternas genomförande av överenskommen lagstiftning. Säkerhetsunionens mål kan också bäst uppnås genom ett nära samarbete med andra relaterade EU-initiativ inom bl.a. energitrygghet, den europeiska hälsounionen och handlingsplanen för demokratin i Europa. Till kommissionens fortsatta insatser hör bland annat tre förslag som antas tillsammans med denna rapport, nämligen förslagen om olaglig handel med kulturföremål, om de viktiga underrättelser som erhålls i form av förhandsinformation om passagerare[5] och om bekämpning av människohandel[6].

2. SKYDD AV FYSISK OCH DIGITAL INFRASTRUKTUR MOT FYSISKA ATTACKER, CYBERATTACKER OCH HYBRIDATTACKER

Skydd av kritisk infrastruktur i EU mot fysiska och digitala attacker

Redan före den senaste tidens attacker mot kritisk infrastruktur arbetade EU med att bygga upp motståndskraften inom ramen för två sammanlänkade initiativ: det reviderade direktivet[7] om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen **(NIS 2-direktivet)**[8] och ett nytt direktiv om kritiska entiteters motståndskraft **(CER-direktivet)**[9]. Tillsammans bildar

[1] COM(2020) 605 final.
[2] Enisas hotbildsrapport 2022.
[3] 1) En framtidssäkrad säkerhetsmiljö, 2) hantera framväxande hot, 3) skydda EU från terrorism och organiserad brottslighet samt 4) ett starkt säkerhetsekosystem.
[4] I en tabell i bilagan ges en översikt över de lagstiftningsåtgärder och andra åtgärder som vidtagits sedan lanseringen av EU:s strategi för en säkerhetsunion.
[5] En handlingsplan mot olaglig handel med kulturföremål (COM(2022) 800 final och två förslag om översyn av direktivet om förhandsinformation om passagerare (COM(2022) 729 final och COM(2022) 731 final).
[6] Ett förslag till reviderat direktiv om bekämpande av människohandel (COM(2022) 732 final) och den fjärde lägesrapporten om människohandel förväntas bli antagna den 19 december 2022.
[7] Förslag till översyn av direktiv (EU) 2016/1148.
[8] COM(2020) 823 final.
[9] COM(2020) 829 final.

dessa initiativ en ram för hantering av nuvarande och framtida risker online och offline, i form av alltifrån cyberattacker till naturkatastrofer. Medlagstiftarna har enats om dessa direktiv som kommer att träda i kraft under de kommande veckorna. **NIS 2-direktivet** har ett bredare tillämpningsområde och omfattar medelstora och stora entiteter inom en rad nyckelsektorer[10]. Det innebär skärpta säkerhetskrav, bland annat för incidenthantering och krishantering, säkerhet i leveranskedjan, hantering av och information om sårbarheter, cybersäkerhetstester och effektiv användning av kryptering. Direktivet medför också en förenkling av skyldigheten att rapportera incidenter, strängare tillsynsåtgärder och en harmonisering av sanktionssystemen i medlemsstaterna[11]. **CER-direktivet** handlar om kritiska entiteters fysiska motståndskraft mot både risker orsakade av människan och naturliga risker. Direktivet omfattar elva sektorer och är ett viktigt steg för att förbättra förmågan hos kritiska entiteter som tillhandahåller samhällsviktiga tjänster att förebygga, skydda mot, reagera på, stå emot, lindra, absorbera, anpassa sig till och återhämta sig från en incident.

Inom **finanssektorn** har förordningen om digital operativ motståndskraft för finanssektorn (DORA)[12] också antagits som en del av paketet för digitalisering av finanssektorn. När DORA-förordningen väl har genomförts kommer den att stärka den digitala operativa motståndskraften hos entiteter i EU:s finansiella sektor genom att strama upp och uppgradera befintliga regler och vid behov införa nya krav.

För att ytterligare öka skyddet av **kritisk infrastruktur mot storskaliga cyberattacker** håller kommissionen, den höga representanten och samarbetsgruppen för nät- och informationssäkerhet[13] på att utarbeta **riskscenarier** med fokus på cybersäkerhet inom energi-, telekommunikations-, transport- och rymdsektorerna. Arbete pågår också med åtgärder för att förbättra den kollektiva skyddsnivån och cyberresiliensen i rymdsystem och rymdtjänster[14]. Utöver detta kommer det även att göras riktade riskbedömningar av cybersäkerheten i kommunikationsinfrastruktur och kommunikationsnät i EU (inbegripet fast och mobil infrastruktur, satelliter, undervattenskablar och internetdirigering)[15]. Kommissionen har också inlett ett initiativ för att bygga upp scenarier som omfattar **naturkatastrofer kopplade till säkerhetsrelaterade hot**, såsom cyberattacker eller terrorism, för att förbättra förebyggande, beredskap och insatser vid katastrofer.

Sabotaget av Nord Stream-gasledningarna och andra incidenter på senare tid underströk hotet mot **EU:s kritiska infrastruktur** och det brådskande behovet av åtgärder. Ramen för CER-direktivet och NIS 2-direktivet håller därför på att stakas ut för att påskynda åtgärderna för att stärka den kritiska infrastrukturens motståndskraft och förbättra beredskapen och insatserna inom viktiga sektorer. Detta kommer att mynna ut i en **rådsrekommendation**[16] som kommer

[10] Följande sektorer omfattas av NIS 2- och CER-direktiven: energi, transport, bankverksamhet, finansmarknadsinfrastruktur, digital infrastruktur, hälso- och sjukvård, dricksvatten, avloppsvatten, offentlig förvaltning, rymdsektorn och produktion, bearbetning och distribution av livsmedel.

[11] Diskussioner pågår mellan nationella experter i samarbetsgruppen för nät- och informationssäkerhet för att stödja medlemsstaterna i införlivandet och genomförandet av NIS 2-direktivet.

[12] COM(2020) 595 final. En politisk överenskommelse nåddes i maj 2022.

[13] Gruppen består av företrädare för medlemsstaterna, kommissionen och Europeiska unionens cybersäkerhetsbyrå (Enisa) som ska stödja och underlätta strategiskt samarbete mellan medlemsstaterna när det gäller säkerhet i nätverks- och informationssystem.

[14] Rådets slutsatser om utvecklingen av Europeiska unionens arbete på cyberområdet, 23.5.2022.

[15] I linje med den uppmaning om att stärka EU:s cybersäkerhetskapacitet som man enades om under telekommunikationsministrarnas informella möte i Nevers den 9 mars 2022.

[16] Kommissionens förslag COM(2022) 551 final följdes av antagandet av rådets rekommendation den 8 december 2022.

att göra det möjligt att påskynda det faktiska genomförandet av direktiven. Därmed skapas en gemensam inställning till genomförandet av **stresstester** på entiteter som driver kritisk infrastruktur, med utgångspunkt i energisektorn, baserad på överenskomna gemensamma principer. Arbetet med stresstester kommer att inledas omedelbart för att kunna slutföras före utgången av 2023, och följas upp i april 2023. Kommissionen kommer i samarbete med rådet och med stöd och bidrag från berörda unionsbyråer att utarbeta en plan som ska hjälpa till att säkerställa en samordnad hantering på EU-nivå av betydande störningar i kritisk infrastruktur.

Inom **energisektorn** håller kommissionen på att utarbeta en nätföreskrift för cybersäkerhet för gränsöverskridande elflöden[17], inbegripet regler om riskbedömningar, gemensamma minimikrav, planering, övervakning, rapportering och krishantering som kommer att vara helt förenliga med NIS 2-ramen. I en separat åtgärd med anledning av Rysslands aggression mot Ukraina synkroniserades elnäten i Ukraina och Republiken Moldavien med det kontinentala Europas nät i mars 2022, som ett komplement till de riskreducerande åtgärderna, bland annat när det gäller cybersäkerhet.

Inom **transportsektorn** samarbetar kommissionen med medlemsstaterna, Europeiska unionens byrå för luftfartssäkerhet (Easa) och EU:s underrättelse- och lägescentral (EU Intcen) för att regelbundet bedöma hot- och risknivån för EU:s civila luftfart från konfliktområden. EU:s varningssystem för konfliktområden betecknas som bästa praxis på internationell nivå[18]. Åtgärderna omfattar bland annat en nylansering av ett arbetsflöde för riskbedömning av flygfrakt, en första riskbedömning på EU-nivå för att bedöma hot mot passagerarfartyg och en omfattande kartläggning av säkerhetsrisker inom luftfarten för att uppdatera bedömningen av hot mot den civila luftfarten.

Särskild uppmärksamhet ägnas också åt **kritisk sjöfartsinfrastruktur**[19]. Den gemensamma miljön för informationsutbyte för sjöfartsområdet håller för närvarande på att utvecklas och kommer att vara i full drift i slutet av 2023, då sjöövervakningsmyndigheter på frivillig basis kommer att kunna utbyta information med varandra i nära realtid. European Coast Guard Functions Forum har också stärkt sin skyddskapacitet mot cyberattacker.

Flera forskningsprojekt inom **Horisont Europa** syftar också till att göra vår digitala infrastruktur säkrare och bygga upp kapaciteten att förebygga och lindra cyberattacker[20].

Ökad cybersäkerhet i EU

Den 16 december 2020 lade kommissionen och den höga representanten fram **EU:s nya strategi för cybersäkerhet för ett digitalt decennium**[21] för att stärka Europas kollektiva motståndskraft mot cyberhot och säkerställa driftsäkra och tillförlitliga tjänster och digitala verktyg för människor och företag. Strategin har nästan genomförts fullt ut.

---

[17] Detta krävs enligt elförordningen (förordning (EU) 2019/943).

[18] Internationella civila luftfartsorganisationen (dokument 10084, *Risk Assessment Manual for Civil aircraft Operation Over or Near Conflict Zones*, 2018).

[19] Bland annat genom genomförandet av Pescos kapacitetsprojekt och Horisont 2020-projekt.

[20] EU-CIP, för att skapa ett europeiskt kunskapsnav och en politisk provbänk för skydd av kritisk infrastruktur, och Atlantis – den atlantiska testplattformen för robotteknik på sjöfartsområdet med nya ramar för inspektion och underhåll av energiinfrastruktur till havs.

[21] JOIN(2020) 18 final.

Enligt NIS 2-direktivet ska det **europeiska kontaktnätverket för cyberkriser (EU-CyCLONe)**[22] inrättas för att stödja en samordnad hantering av storskaliga cyberincidenter och cyberkriser på operativ nivå. Detta kommer att säkerställa ett regelbundet utbyte av relevant information mellan medlemsstaterna och EU:s institutioner, organ och byråer. Kommissionen håller på att utveckla ett **läges- och analyscentrum för cybersäkerhet** för att öka sin interna kapacitet. Kommissionen samarbetar med medlemsstaterna, bland annat genom att följa upp rekommendationen om en **gemensam cyberenhet**[23] för att säkerställa samordnade EU-insatser vid storskaliga cyberincidenter. Kommissionen och den höga representanten deltar också aktivt i de cyberövningar som anordnats tillsammans med medlemsstaterna under 2022[24].

Nätverk och datasystem kräver ständig övervakning och analys för att upptäcka intrång och avvikelser i realtid. Kommissionen har lagt fram ett förslag om att bygga upp ett nätverk av **säkerhetscentrum** i hela EU för att övervaka kommunikationsnäten och identifiera misstänkta händelser. Genom att utöka befintliga säkerhetscentrum, inrätta nya centrum och koppla samman säkerhetscentrum i flera medlemsstater kommer den kollektiva detektionsförmågan att stärkas. Dessa skulle också kunna bygga på den senaste artificiella intelligensen (AI) och dataanalysen, skydda civila kommunikationsnätverk och påskynda upptäckten av cyberattacker[25].

För att förbättra beredskapen och insatserna vid större cyberincidenter har kommissionen också inrättat ett kortsiktigt program för att genom ytterligare finansiering till Enisa stödja medlemsstaterna med bland annat penetrationstestning av kritiska entiteter för att identifiera sårbarheter. Enisa kan också med stöd av betrodda privata leverantörer av cybersäkerhetstjänster hjälpa medlemsstaterna med incidenthantering efter större incidenter vid kritiska entiteter. Nästa steg blir att se till att medlemsstaterna utnyttjar dessa möjligheter fullt ut.

Både maskinvaru- och programvaruprodukter utsätts i allt högre grad för **cyberattacker**. Cyberattackerna blir allt fler och alltmer sofistikerade, och utnyttjandet av programvarusårbarheter är den viktigaste vektorn. Två tredjedelar av alla incidenter som rapporteras inom ramen för NIS-direktivet handlar om att utnyttja programvarusårbarheter. Konsekvenserna för människor, infrastruktur och företag ökar också[26]. Två tredjedelar av alla incidenter som rapporteras inom ramen för NIS-direktivet handlar om att utnyttja programvarusårbarheter. I september 2022 lade kommissionen fram ett förslag till en **cyberresiliensakt**[27] för att minska sårbarheterna i produkter med digitala element och säkerställa att programfixar och riskreducerande åtgärder snabbt görs tillgängliga.

---

[22] EU-CyCLONe består av företrädare för medlemsstaternas myndigheter för hantering av cyberkriser och kommissionen i fall där en potentiell eller pågående storskalig cyberincident har haft eller väntas få betydande konsekvenser för de tjänster och verksamheter som avses i direktivet.

[23] COM(2021) 4520 final.

[24] Exempel på detta är övningarna Blueprint Operational Level Exercise (Blue OLEx), som organiseras av Litauen och Enisa, och EU Cyber Crisis Linking Exercise on Solidarity (EU CyCLES), som anordnas av det franska ordförandeskapet.

[25] En första fas inleddes med en inbjudan att lämna förslag om kapacitetsuppbyggnad vid säkerhetscentrum och en inbjudan att anmäla intresse för att delta i en gemensam upphandling av verktyg och infrastruktur, tillsammans med Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning, med totalt 110 miljoner euro i EU-finansiering från DIGITAL-programmet, som offentliggjordes i november 2022.

[26] Enisas hotbildsrapport 2022.

[27] COM(2022) 454 final.

Kommissionen föreslår att produkter med digitala element (maskinvara och programvara) endast bör släppas ut på marknaden om de uppfyller vissa väsentliga cybersäkerhetskrav[28]. Tillverkare och utvecklare kommer att behöva säkerställa cybersäkerheten för sina produkter i fem år och vara transparenta gentemot konsumenterna i fråga om cybersäkerhet. Detta kommer att bidra till kraftigt ökad säkerhet i leveranskedjan[29].

Certifiering spelar en avgörande roll för att öka förtroendet och säkerheten för viktiga produkter och tjänster för den digitala världen. Genom cybersäkerhetsakten[30] inrättas ett europeiskt ramverk för cybersäkerhetscertifiering, enligt vilket kommissionen kan uppmana Enisa att utveckla certifieringssystem. Ett europeiskt system för cybersäkerhetscertifiering baserat på gemensamma kriterier har utvecklats och system för molntjänster och 5G-säkerhet håller på att utarbetas.

Kommissionen fortsätter att samarbeta med medlemsstaterna för att säkerställa att **5G-näten** är säkra och motståndskraftiga och för att övervaka genomförandet av EU:s 5G-verktygslåda på nationell nivå och EU-nivå. Även om de allra flesta medlemsstater redan har skärpt eller håller på att skärpa säkerhetskraven för 5G-nät är det nu angeläget att alla medlemsstater slutför genomförandet av åtgärderna i verktygslådan[31]. Till exempel behöver medlemsstaterna införa begränsningar för högriskleverantörer, med tanke på att tidsförlusten kan öka sårbarheten hos näten i unionen och även stärka det fysiska och icke-fysiska skyddet av kritiska och känsliga delar av 5G-nät, bland annat genom strikta åtkomstkontroller.

För att hjälpa EU och medlemsstaterna att ha en proaktiv och strategisk cybersäkerhetspolitik kommer **Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning** att samarbeta med nationella samordningscentrum för att stödja innovation inom cybersäkerhet och utöka den cybersäkerhetstekniska gemenskapens kapacitet[32].

I september 2022 lanserade Enisa formellt en **europeisk ram för cybersäkerhetskompetens** i vilken de nödvändigaste arbetsprofilerna på området identifieras. Ramen bildar en gemensam europeisk grund som ska underlätta erkännandet av färdigheter och utveckla cybersäkerhetsutbildningen. Denna ram kommer att utgöra en byggsten i den **cybersäkerhetsakademi** som föreslås i kommissionens arbetsprogram för 2023. Därmed tas ett helhetsgrepp för att tillgodose det växande behovet av sakkunniga inom cybersäkerhet i Europa.

Med tanke på de känsliga icke-säkerhetsskyddsklassificerade och säkerhetsskyddsklassificerade EU-uppgifter som hanteras av **EU:s institutioner, organ och byråer** är det viktigt att dessa är väl skyddade mot cyberattacker. I mars 2022 lade kommissionen fram ett förslag till förordning om åtgärder för en hög gemensam cybersäkerhetsnivå vid dessa organ[33], där NIS 2-direktivets principer tillämpas på EU:s

---

[28] Samtidigt antog kommissionen i oktober 2021 inom ramen för radioutrustningsdirektivet en delegerad förordning som ålägger tillverkare av trådlösa enheter att förbättra cybersäkerheten, integriteten och skyddet mot bedrägerier.

[29] I linje med rådets slutsatser om säkerheten i IKT-leveranskedjan av den 17 oktober 2022.

[30] Förordning (EU) 2018/881 om att införa av ett EU-omfattande ramverk för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster och IKT-processer.

[31] Medlemsstaterna offentliggjorde tidigare i år, med stöd av kommissionen och Enisa, en rapport om cybersäkerheten i öppna radioaccessnät, som när de är mer välutvecklade kommer att utgöra ett alternativt sätt att utnyttja radioaccessdelen i 5G-nät baserat på öppna gränssnitt.

[32] Europeiska kompetenscentrumets styrelse har inrättats och håller sitt fjärde möte den 20 oktober 2022.

[33] COM(2022) 122 final.

institutionella miljö. Det omfattar en ny interinstitutionell cybersäkerhetsstyrelse och ett förstärkt cybersäkerhetscentrum (CERT-EU)[34] för att säkerställa ett lämpligt informationsutbyte och samarbete med medlemsstaternas myndigheter, till exempel genom nätverket av enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter). Samtidigt har kommissionen antagit ett förslag till förordning om informationssäkerhet i unionens institutioner, organ och byråer[35] för att stärka EU:s resiliens mot cyberhot och hybridhot genom att upprätta höga gemensamma informationssäkerhetsstandarder för unionens alla institutioner, organ och byråer. Det är mycket viktigt att rådet påskyndar arbetet med detta förslag, med tanke på medlemsstaternas många uppmaningar till kommissionen om att arbeta med åtgärder för att bättre skydda EU:s beslutsprocess mot skadlig verksamhet av alla slag. CERT-EU och Enisa har också utformat och testat en ny typ av cyberövning som är skräddarsydd för EU:s byråer, i enlighet med Europeiska revisionsrättens rekommendationer.

Exempel på viktiga resultat

Europeiska informationssäkerhetsmånaden: Europeiska informationssäkerhetsmånaden, med bland annat workshoppar, kampanjer i sociala medier och föreläsningar, har utökats från 184 aktiviteter 2014 till 500 aktiviteter i oktober 2022. Dessa hjälper användarna att agera på rätt sätt när de ställs inför ett cybersäkerhetshot på nätet (vilket rapporterades av 73 % av de medlemsstater som deltog i undersökningen 2021).

Databasen för högre cybersäkerhetsutbildning (CyberHEAD): CyberHEAD har varit Enisas mest besökta webbsida under de senaste två åren, med omkring 70 000 besök per år. Den hjälper unga talanger att fatta välgrundade beslut om de olika möjligheter som högre cybersäkerhetsutbildning ger och hjälper universiteten att locka duktiga studenter som är motiverade att upprätthålla cybersäkerheten i Europa.

Åtgärder för att motverka hybridhot, bekämpa utländsk inblandning och stärka EU:s cyberförsvar

EU:s strategiska kompass för säkerhet och försvar innehåller en ambitiös handlingsplan för att öka EU:s förmåga att agera, stärka motståndskraften och investera bättre i EU:s försvarskapacitet.

Medan det främst är medlemsstaternas ansvar att motverka **hybridhot**, kompletterar EU de nationella åtgärderna genom att stödja samordning, förbättra lägesuppfattningen, främja samarbete med likasinnade länder och internationella organisationer och ge möjlighet till gemensamma insatser. Under det senaste årtiondet har mer än 200 åtgärder vidtagits för att öka motståndskraften och motverka hybridhoten på EU-nivå. EU Intcens gemensamma enhet för hybridhot bidrar till EU:s beslutsfattande och är det centrala organ som ska bidra med en övergripande lägesuppfattning och strategisk framsynthet, sammanställa information från alla källor och göra underrättelsebedömningar om hybridhot. Arbetet med att inrätta EU:s snabbinsatsteam för hybridhot, som tillkännagavs i den strategiska kompassen, har inletts för att stödja medlemsstaterna, gemensamma säkerhets- och försvarspolitiska uppdrag och operationer, samt partnerländer, när det gäller att motverka hybridhot genom att med kort varsel utnyttja relevant expertis på nationell nivå och EU-nivå, inbegripet militär expertis vid behov. En EU-verktygslåda för hantering av hybridhot håller på att utarbetas och kommer att

34 CERT-EU har också gjort betydande investeringar i att ytterligare förbättra de befintliga tjänsterna till EU:s institutioner, organ och byråer och i att lägga till nya, för att bättre förebygga, upptäcka och bemöta cyberattacker.

35 COM(2022) 119 final.

utgöra en ram för en samordnad reaktion på hybridkampanjer som påverkar EU och dess medlemsstater och som integrerar den externa och interna dimensionen i ett smidigt flöde och sammanför nationella och EU-omfattande överväganden. Betydande framsteg har också gjorts när det gäller att öka motståndskraften och motverka hybridhot genom att identifiera befintliga utgångsvärden för sektorsspecifik resiliens[36]. Kommissionen har också fortsatt med den analytiska forskningen om uppbyggnad av motståndskraft mot hybridhot[37] och slutfört integreringen av hybridöverväganden i det politiska beslutsfattandet.

Covid-19-pandemin och Rysslands krig mot Ukraina har visat hur manipuleringen av informationsmiljön kan påverka EU och dess partner runt om i världen. I syfte att undergräva förtroendet för EU och den regelbaserade världsordningen är **utländsk informationsmanipulering och inblandning** också en allt viktigare komponent i hybridattacker. Med utgångspunkt i handlingsplanen för demokrati i Europa har kommissionen infört en rad konkreta åtgärder och strukturer för att bekämpa informationsmanipulering och desinformation, bland annat den reviderade uppförandekoden om desinformation, förordningen om digitala tjänster och det förslag om transparens när det gäller politisk reklam som för närvarande är föremål för interinstitutionella förhandlingar. Detta skulle resultera i nya skyldigheter för plattformarna och för första gången en rättsligt bindande tillsynsram. Såsom tillkännagavs i den strategiska kompassen håller Europeiska utrikestjänsten, i nära samarbete med kommissionen och medlemsstaterna, dessutom på att vidareutveckla **EU:s verktygslåda för hantering av utländsk informationsmanipulering och inblandning** för att främja en samordnad respons på utländska aktörers manipulativa beteende[38]. Utrikestjänsten har också fortsatt att stärka samarbetet med internationella partner som G7:s snabbinsatsmekanism och Nato.

Kommissionen fördömer all utländsk inblandning på medlemsstaternas suveräna territorium och är oroad över rapporter om kinesiska polisstationer i EU, vilket, om det stämmer, skulle vara helt oacceptabelt. Även om det är upp till medlemsstaternas myndigheter att utreda dessa anklagelser är kommissionen, med stöd av Europol, redo att underlätta utbytet mellan medlemsstaterna. Kommissionen tog upp frågan vid rådets möte (rättsliga och inrikes frågor) i december 2022.

I november 2022 lade kommissionen och den höga representanten fram en ny EU-politik för **cyberförsvar**[39] med metoder för att öka samarbetet och investeringarna i cyberförsvar för att bättre skydda mot cyberattacker. Målet är att försvara EU:s intressen i cyberrymden genom ökat samarbete mellan EU:s aktörer på cyberförsvarsområdet och genom att utveckla mekanismer för att mobilisera kapacitet på EU-nivå, även inom ramen för GSFP-uppdrag och GSFP-insatser. Detta kommer att främja utvecklingen av en fullskalig cyberförsvarsförmåga och stärka samarbetet mellan EU:s militära och civila cybergemenskaper, förbättra lägesuppfattningen, krissamordningen och krisutbildningen, även med den privata sektorn.

---

[36] SWD(2022) 21 final.

[37] *Hybrid threats: a comprehensive resilience ecosystem*, JRC130097.

[38] Arbetet pågår med den strategiska kompassens uppgifter för att bygga upp ett dataområde för utländsk informationsmanipulering och inblandning och rusta gemensamma säkerhets- och försvarspolitiska uppdrag och operationer med den förmåga och de resurser som behövs för att använda relevanta instrument i verktygslådan. Europeiska utrikestjänsten fortsätter att genom öppna källor ge EU:s medlemsstater en lägesuppfattning via EU:s system för snabbt informationsutbyte, ökar allmänhetens medvetenhet, särskilt genom kampanjen EUvsDisinfo, och har ytterligare fördjupat samarbetet med intressenter som Nato och G7-gruppens snabbinsatsmekanism.

[39] JOIN(2022) 49 final.

Det kommer också att bidra till att minska det strategiska beroendet av kritisk cyberteknik, genom att utveckla en strategisk färdplan för kritisk cybersäkerhet och cyberförsvarsteknik, och stärka den europeiska försvarstekniska och försvarsindustriella basen.

I den strategiska kompassen identifieras **rymden** som ett femte operativt område (vid sidan av land, sjö, luft och cyberrymd) och kommissionen och den höga representanten uppmanas att utarbeta den första rymdstrategin för säkerhet och försvar. I strategin föreslås åtgärder för att förbättra rymdsystemens och rymdtjänsternas gemensamma skyddsnivå och motståndskraft och för att avskräcka från och reagera på alla hot, inbegripet cyberhot, mot känsliga rymdsystem och rymdtjänster i EU.

3 KAMPEN MOT TERRORISM OCH RADIKALISERING

Nästan alla de viktigaste initiativen i EU:s säkerhetsstrategi för att stödja medlemsstaterna i kampen mot terrorism och radikalisering har antagits. Skyddet mot hot på nätet har varit ett särskilt tema. Nästa steg är att se till att dessa initiativ får full effekt.

Kampen mot terrorism

Sedan **EU-agendan för terrorismbekämpning**[40] antogs i december 2020 har den gjort det möjligt för EU att bättre förutse, förebygga, skydda mot och reagera på terroristhot. Särskilda geografiska initiativ har också bidragit till att bemöta den framväxande hotsituationen. Mot bakgrund av utvecklingen i Afghanistan har EU:s samordnare för kampen mot terrorism i samordning med kommissionen, den höga representanten, ordförandeskapet och viktiga EU-organ utarbetat en **handlingsplan för terrorismbekämpning för Afghanistan**[41], som godkändes av medlemsstaterna i oktober 2021. Ett tydligt resultat av denna har varit ett frivilligt förfarande för skärpta säkerhetskontroller av personer som kommer från Afghanistan.

En prioriterad fråga är att ta itu med hotet från **återvändande utländska terroriststridande** i Syrien och Irak. Huvudansvaret ligger hos medlemsstaterna, men samarbetet på EU-nivå hjälper medlemsstaterna att hantera gemensamma utmaningar, som att lagföra dem som har begått terroristbrott, förhindra oupptäckta inresor i Schengenområdet och återanpassa och rehabilitera återvändande utländska terroriststridande. Kommissionen fortsätter att bedriva ett nära samarbete med medlemsstaterna och viktiga partnerländer för att se till att bevis från slagfältet förs in i EU:s databaser och informationssystem. I samförstånd med medlemsstaterna undersöker EU:s samordnare för kampen mot terrorism, i nära samarbete med den höga representanten och kommissionen, nya sätt att förbättra levnadsvillkoren i fängelser och läger i nordöstra Syrien för att bidra till att bekämpa radikalisering.

EU:s lagstiftning om bekämpande av terrorism har uppdaterats. **Direktivet om bekämpande av terrorism**, som antogs 2017, genomförs nu av alla medlemsstater[42] för att kriminalisera handlingar, såsom utbildning och resor för terrorismsyften, samt finansiering av terrorism. Ett felaktigt införlivande av direktivet i ett antal medlemsstater måste fortfarande åtgärdas.

---

[40] COM(2020) 795 final.

[41] Afghanistan: handlingsplan för terrorismbekämpning, den 29 september 2021.

[42] COM(2021) 701 final. Medlemsstaterna var skyldiga att införliva direktivet i nationella bestämmelser senast den 8 september 2018.

Att **beröva terrorister de medel som behövs för att utföra en attack** är avgörande för att bekämpa terrorism. Nästan alla medlemsstater har nu antagit den uppdaterade lagstiftningen om skjutvapen[43] i nationell lagstiftning. Ny lagstiftning för att begränsa tillgången till sprängämnesprekursorer som terrorister skulle kunna använda för att tillverka bomber trädde i kraft i februari 2021. Utifrån den strategi som används för att reglera tillgången till sprängämnesprekursorer kommer kommissionen att undersöka möjligheten begränsa tillgången till vissa farliga kemikalier som skulle kunna användas för att utföra attacker.

Offentliga platser har upprepade gånger varit föremål för terroristattacker. Kommissionen har utfärdat en handbok för att främja inbyggd säkerhet på offentliga platser[44]. Den innehåller detaljerad teknisk vägledning[45], verktyg för sårbarhetsbedömningar av offentliga platser[46] och omfattande stöd till viktiga intressenter[47], samt en rekommendation om frivilliga prestandakrav för röntgenutrustning som används på offentliga platser (utom luftfart)[48]. Under 2022 har Fonden för inre säkerhet också bidragit med 14,5 miljoner euro i stöd till projekt för att förbättra skyddet av offentliga platser, inklusive andaktslokaler. **Drönare** är ett mycket innovativt verktyg som kan användas för legitima men även skadliga ändamål, inbegripet attacker på offentliga platser, individer och kritisk infrastruktur. I november 2022 antog kommissionen en **drönarstrategi 2.0**[49], som under 2023 ska följas av en mer detaljerad EU-strategi för att motverka skadlig användning av drönare.

Bekämpande av radikalisering som leder till våldsbejakande extremism och terrorism på och utanför internet

Att förebygga och bekämpa **radikalisering** är avgörande för en effektiv politik för terrorismbekämpning. Kommissionen stöder medlemsstaterna genom EU:s nätverk för kunskapsspridning om radikalisering (RAN), som består av 6 000 experter som aktivt arbetar med förebyggande insatser. Medlemsstaterna får huvudsakligen stöd för att motverka våldsbejakande extremistiska ideologier och polarisering som leder till radikalisering, förhindra radikalisering på nätet och missbruk av ny teknik, samt för att hantera och förbereda återintegrering av brottslingar som frigetts från fängelset. Kopplingar mellan våldsbejakande extremistgrupper och ideologier och uttryck för hatpropaganda behandlas i EU:s uppförandekod för att motverka olaglig hatpropaganda på nätet[50].

EU arbetar också för att förhindra utländsk påverkan och finansiering till stöd för radikala/extremistiska åsikter i medlemsstaterna. Kommissionen är för sin del vaksam på att förhindra att EU-medel används för att stödja projekt som är oförenliga med europeiska värderingar eller som bedriver olaglig verksamhet. Därför offentliggörs sedan slutet av 2021 projekt som förvaltas av kommissionen så snart bidragsavtalet har undertecknats på en unik plattform kallad finansierings- och anbudsportalen. Det är viktigt att medlemsstaterna använder denna möjlighet att själva granska stödmottagarna och förse kommissionen med all

---

43 COM(2015) 750 final.
44 SWD(2022) 398 final.
45 *Guideline – Building Perimeter Protection*, EUR 30346 EN.
46 http://counterterrorism.jrc.ec.europa.eu.
47 Se särskilt *EU Digital Autumn School*, JRC127168, och *Terrorism and Extremism Database – User Guide*, JRC130461.
48 I denna akt rekommenderas medlemsstaterna att uppfylla EU:s prestandakrav vid upphandling av röntgenutrustning som ska användas för att upptäcka hot på offentliga platser (C(2022) 4179 final).
49 COM(2022) 652 final.
50 https://ec.europa.eu/commission/presscorner/detail/sv/IP_16_1937.

kompletterande information som de har tillgång till. Här vill kommissionen i förslaget till översyn av budgetförordningen bland annat att frågan om en fällande dom för ”uppvigling till hat” läggs till som skäl för uteslutning från EU-finansiering. Kommissionen uppmanar Europaparlamentet och rådet att effektivt ta itu med denna fråga i den slutliga texten. Dessutom vidtar kommissionen interna medvetandehöjande åtgärder och utvecklar interna arbetsmetoder för att säkerställa ökad granskning vid urvalet av projekt.

En annan viktig fråga är att förebygga radikalisering på nätet. **Förordningen om åtgärder mot spridning av terrorisminnehåll online**[51] började tillämpas i juni 2022. Sedan dess kan de nationella behöriga myndigheterna kräva att terrorisminnehåll avlägsnas inom en timme från mottagandet av en officiell avlägsnandeorder. Leverantörer av onlinetjänster som utsätts för terrorisminnehåll måste vidta särskilda åtgärder för att skydda sina plattformar mot missbruk. Detta kompletterar arbetet inom **EU:s internetforum**, som kommissionen lanserat för att tillsammans med medlemsstater, internetföretag och det civila samhället förhindra spridning av våldsbejakande extremistiskt innehåll och terrorisminnehåll online. EU:s internetforum har nyligen stöttat teknikföretag och leverantörer av internetinfrastruktur i deras insatser för att moderera innehåll, bland annat med hjälp av en katalog över terroristdrivna webbplatser och ett årligt uppdaterat kunskapspaket om våldsbejakande högerextrema grupper, symboler och manifest[52]. Sedan 2019 har förebyggandet av sexuella övergrepp mot barn på nätet också tagits upp i detta forum.

Exempel på viktiga resultat

Så ledde samarbetet med Eurojust till en fällande dom mot en utländsk terroriststridande: Huvudföremålet för en terroristrelaterad utredning dömdes 2021 till fyra års fängelse för deltagande i en terroristorganisation, sedan de italienska myndigheterna använt terrorismbekämpningsregistret för att hitta kopplingar mellan misstänkta utländska stridande och andra terroristfall. Eurojust sammanförde de nationella myndigheterna, vilket ledde till verkställighet av europeiska utredningsorder och framställningar om ömsesidig rättslig hjälp.

Europols samordnade insatser mot bombhandböcker på nätet: I ett i en rad regelbundna gemensamma initiativ hittade Europol tillsammans med åtta medlemsstater och Förenade kungariket under en insatsdag i februari 2022 hundratals poster på nätet, bland annat instruktioner om hur man tillverkar bomber med prekursorer och hur man använder dem i samband med terroristattacker. Informationen vidarebefordrades till leverantörerna av onlinetjänster.

4. BEKÄMPANDE AV ORGANISERAD BROTTSLIGHET

Inom den organiserade brottsligheten i Europa är samarbetet mellan brottslingar under ständig förändring. Kriminella nätverk kan vara inblandade i en rad olika brottsliga verksamheter som omfattar såväl narkotikahandel som organiserade egendomsbrott, bedrägerier, smuggling av migranter och människohandel[53]. Cyberbrottslighet och könsrelaterat cybervåld har ökat

[51] Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online, EUT L 172, 17.5.2021, s. 79–109.

[52] Det har även bland annat resulterat i en uppdatering av EU:s krisprotokoll, handböcker med riktlinjer om uppsåtlig användning av gråzonsinnehåll och datorspel som leder till radikalisering, samt en studie om hur algoritmisk förstärkning påverkar användare i riktning mot radikalisering.

[53] Europol, Europeiska unionens hotbildsbedömning avseende grov och organiserad brottslighet: *A Corrupting Influence: the infiltration and undermining of Europe's economy and society by organised crime*, Europeiska unionens publikationsbyrå, Luxemburg 2021.

ytterligare till följd av den ökade användningen av internet och onlinetjänster. Den ökande användningen av krypterade kommunikationskanaler, och behovet av att samtidigt skydda den personliga integriteten och de grundläggande rättigheterna, innebär ytterligare utmaningar för brottsbekämpningen[54]. Samtidigt har störningarna till följd av Rysslands anfallskrig mot Ukraina skapat nya öppningar som snabbt utnyttjas av organiserade kriminella grupper.

I april 2021 antog kommissionen **EU:s strategi för att bekämpa organiserad brottslighet 2021–2025**[55]. Strategin visar vikten av att demontera strukturer för organiserad brottslighet och inrikta sig på de grupper som utgör en större risk för Europas säkerhet och de individer som innehar de högre posterna i kriminella organisationer. Arbetet med att genomföra strategin har nu kommit en bit på väg, och flera nyckelåtgärder har redan antagits eller genomförts. Kommissionen har också gett ekonomiskt stöd till medlemsstaterna för att bekämpa de brottshot som EU står inför[56].

Cyberbrottslighet

Den påskyndade digitaliseringen under covid-19-pandemin bidrog till en ökad spridning av cyberhot, till exempel utpressningsprogram[57]. **Utpressningsprogram** medför betydande cybersäkerhetsrisker för kritisk infrastruktur och allmän säkerhet. Europols it-brottscentrum (EC3) har tillsammans med den gemensamma insatsstyrkan mot it-brottslighet (J-CAT) nyligen utvecklat den internationella modellen för hantering av utpressningsprogram för att operationalisera en övergripande brottsbekämpande insats. EU deltog i det toppmöte som hölls 2022 inom ramen för initiativet för att motverka utpressningsprogram i syfte att stärka det internationella samarbetet om utpressningsprogram. 36 länder och EU enades om att gå vidare med arbetet med den internationella arbetsgruppen för motverkande av utpressningsprogram för att samordna arbetet med resiliens och störningar och att motverka olaglig finansieringsverksamhet[58]. Kommissionen och Europol har gemensamt inrättat en dekrypteringsplattform[59] som snabbare ger kriminaltekniker tillgång till digital bevisning och som hjälper till att komma åt krypterade kriminella kommunikationsnätverk, vilket innebär hårda slag mot den organiserade brottsligheten.

EU bidrog till de framgångsrika förhandlingarna om det andra tilläggsprotokollet till **Budapestkonventionen om it-relaterad brottslighet** i maj 2022. Detta innehåller välbehövliga verktyg för gränsöverskridande samarbete vid utredning och lagföring av it-brottslighet samt detaljerade villkor och garantier om dataskydd. Alla medlemsstater bör snabbt underteckna det andra tilläggsprotokollet och Europaparlamentet uppmanas att ge sitt godkännande för att möjliggöra en snabb ratificering. Kommissionen förhandlar också på EU:s vägnar om en ny FN-konvention om it-relaterad brottslighet.

Enbart under 2021 rapporterades världen över 85 miljoner bilder och filmer som visar **sexuella övergrepp mot barn**, och det finns många fler som inte rapporterats: sexuella övergrepp mot barn är en utbredd företeelse. När barn tillbringar mer tid på nätet blir de mer

---

[54] Europol, Hotbildsbedömning av internetstödd organiserad brottslighet (Iocta), 2021.

[55] COM(2021) 170 final.

[56] I juli 2022 anslog kommissionen genom Fonden för inre säkerhet (ISF) 15,7 miljoner euro till medlemsstaterna för att stödja långsiktiga projekt och verksamheter inom Europeiska sektorsövergripande plattformen mot brottshot (Empact), som arbetar med EU:s tio prioriteringar mot brottslighet som antogs av rådet för 2022–2025.

[57] Hotbildsbedömning av internetstödd organiserad brottslighet (Iocta).

[58] Internationellt initiativ för att motverka utpressningsprogram 2022, Washington DC, den 1 november 2022.

[59] Europols dekrypteringsplattform finns på Gemensamma forskningscentret i Ispra.

mottagliga för gromning, vilket har lett till en ökning av egenproducerat exploativt material. I linje med EU-strategin för en effektivare bekämpning av sexuella övergrepp mot barn som antogs i juli 2020[60] och EU:s övergripande strategi för barnets rättigheter från mars 2021[61] antog kommissionen i maj 2022 ett förslag till förordning om fastställande av regler för att förebygga och bekämpa sexuella övergrepp mot barn på nätet[62], med nya skyldigheter för leverantörer av onlinetjänster. Om förebyggande åtgärder inte räcker för att minska en betydande risk kan tjänsteleverantörer beordras att spåra, rapportera, avlägsna och blockera sexuella övergrepp mot barn på nätet. Genom förslaget inrättas också ett särskilt EU-centrum för att underlätta genomförandet. Den tillfälliga lagstiftning som antogs i augusti 2021 för att göra det möjligt för leverantörer av onlinetjänster att fortsätta att frivilligt spåra och rapportera sexuella övergrepp mot barn på nätet[63] kommer att upphöra att gälla sommaren 2024. Det är därför viktigt att Europaparlamentet och rådet snabbt når en överenskommelse om den föreslagna förordningen. I början av nästa år kommer detta initiativ att kompletteras med ett förslag till uppdatering av direktivet från 2011 om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi[64].

Nätvåld mot kvinnor är en framväxande ny dimension av det **könsrelaterade nätvåldet**. År 2020 uppskattades att varannan ung kvinna upplevt denna form av våld[65]. I förslaget till direktiv om bekämpning av våld mot kvinnor och våld i nära relationer[66], som antogs i mars 2022, föreslog kommissionen riktade regler om könsrelaterat våld mot kvinnor på eller utanför nätet[67].

Organiserad brottslighet

Människohandel är en central del av den organiserade brottslighetens verksamhet i EU[68]. Trots att människohandel redan är en prioritering i EU:s strategi för en säkerhetsunion hittade brottslingarna nya möjligheter att tjäna stora pengar och intensifiera den brottsliga verksamheten under covid-19-pandemin. En snabb samordning på EU-nivå hjälper till att förebygga den ökade risken för människohandel till följd av Rysslands anfallskrig mot Ukraina. EU:s samordnare för kampen mot människohandel har utarbetat en **gemensam plan för kampen mot människohandel**[69] för att sammanföra kommissionens och medlemsstaternas, EU-byråernas och Europeiska utrikestjänstens arbete för att hantera riskerna för människohandel och stödja potentiella offer. Dessa insatser har bidragit till att säkerställa att antalet bekräftade fall av människohandel har förblivit begränsat, även om risken fortfarande är hög.

---

60 COM(2020) 607 final.
61 COM(2021) 142 final.
62 COM(2022) 209 final.
63 COM(2020) 568 final.
64 Direktiv 2011/93/EU av den 13 december 2011 om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi, EUT L 335, 17.12.2011.
65 Europaparlamentets utredningstjänsts (EPRS) studie *Combating gender-based violence: Cyberviolence, European added value assessment*, 2021.
66 COM(2022) 105 final.
67 Förslaget handlar bland annat om att på EU-nivå straffbelägga delning utan samtycke av intimt material, nätstalkning, nättrakasserier och offentlig uppmaning till hat och våld på nätet. Tanken är att komplettera detta med en ny ram för samarbete mellan internetplattformar för att bättre skydda kvinnors säkerhet på nätet.
68 Hotbildsbedömning avseende grov och organiserad brottslighet (Socta), 2021.
69 *An Anti-Trafficking Plan to protect people fleeing the war in Ukraine* (europa.eu).

I april 2021 resulterade EU:s strategi mot människohandel 2021–2025 i en övergripande intern och extern handlingsram[70]. Kommissionen följer upp detta med ett kommande förslag som syftar till att ändra **direktivet mot människohandel**[71] för att komma till rätta med brister i den nuvarande rättsliga ramen och uppdatera den så att den återspeglar onlinedimensionen, och som syftar till att minska efterfrågan. I september 2022 anordnade Empact, med stöd av Europol och Eurojust, och tillsammans med brottsbekämpande myndigheter från 20 länder, en gemensam insatsdag i form av ett första EU-omfattande hackaton mot människohandel, med fokus på kriminella nätverk som använder webbplatser och sociala medieplattformar för att rekrytera offer för sexuellt utnyttjande. Man identifierade 11 misstänkta människohandlare och 45 potentiella offer[72].

Till skillnad från människohandel gör de som betalar smugglare för att irreguljärt resa in i EU detta frivilligt. Smugglarnas verksamhet är dock brottslig, utsätter ofta människors liv för fara och kan medföra ytterligare säkerhetsrisker för EU. Att förebygga och bekämpa **smuggling av migranter** är ett centralt mål i strategin för EU:s säkerhetsunion, EU:s strategi för att bekämpa organiserad brottslighet och den nya migrations- och asylpakten[73]. Det kräver fortlöpande internationellt samarbete och samordning på alla nivåer. Genomförandet av EU:s handlingsplan mot smuggling av migranter 2021–2025[74] går framåt, och operativa partnerskap mot smuggling håller på att utvecklas tillsammans med Marocko, Niger och västra Balkan med stöd av EU:s institutioner, organ och byråer samt EU-finansiering.

Marknaden för **olaglig narkotika**, vars marknadsvärde beräknas uppgå till minst 30 miljarder euro per år, är fortfarande den största kriminella marknaden i EU och är en viktig inkomstkälla för organiserade kriminella grupper samt ett hot mot den sociala stabiliteten och hälsan. Under 2021 resulterade EU:s åtgärder och samarbete i att narkotika till ett värde av 7 miljarder euro togs bort från gatorna[75]. **EU:s agenda och handlingsplan för narkotika 2021–2025**[76] från juli 2020 innehåller konkreta åtgärder för att intensifiera EU:s insatser. Bland annat omvandlades Europeiska centrumet för kontroll av narkotika och narkotikamissbruk till Europeiska unionens narkotikabyrå. Den revidering av byråns mandat som föreslogs i januari 2022[77] skulle stärka dess övervaknings- och hotbedömningskapacitet och dess förmåga att reagera på nya utmaningar. Rådet antog en allmän riktlinje i juni 2022 och arbetet i Europaparlamentet pågår. Kommissionen inledde också ett samarbete i EU:s internetforum för att bekämpa narkotikahandeln på nätet och föreslog en särskild tematisk Schengenutvärdering om smugglingen av kokain till EU:s hamnar. Stödet till centrumet för analys av maritim underrättelseverksamhet beträffande narkotika utökades. EU fortsätter också att föra politiska dialoger om narkotika med tredjeländer, med en andra dialog med Kina i juli 2022 och en ny dialog med Colombia som inleddes i juni 2022.

---

70 COM(2021) 171 final.

71 Den fjärde lägesrapporten om människohandel som ska antas tillsammans med detta förslag innehålleringående information om genomförandet av EU:s strategi 2019–2022 samt viktiga uppgifter och statistik.

72 *20 countries spin a web for human traffickers during a hackathon* | Europol (europa.eu).

73 COM(2020) 609 final.

74 COM(2021) 591 final.

75 Eurojusts årsrapport för 2021.

76 COM(2020) 606 final.

77 COM(2022) 18 final.

Enligt Europol undgår nästan 99 % av vinsterna från brottslig verksamhet **konfiskering** i EU och stannar i händerna på gärningsmännen[78]. De förslag om att stärka EU:s bekämpning av penningtvätt och finansiering av terrorism som kommissionen lade fram i juli 2021 behandlas vidare i rådet[79]. I maj 2022 föreslog kommissionen en skärpning och modernisering av EU:s regler om återvinning och förverkande av tillgångar[80]. Förslaget har diskuterats i rådets arbetsgrupper och framsteg har gjorts på flera områden.

Europeiska åklagarmyndigheten har nu arbetat sitt första hela år med att skydda EU:s ekonomiska intressen. Den mottog 4 006 anmälningar om brott, inledde 929 utredningar och godkände beslut om frysning till ett totalt värde av 259 miljoner euro. Under verksamhetens första sju månader utreddes fall motsvarande 5,4 miljarder euro i potentiella skador för unionens budget[81].

Kommissionen arbetar också med att utarbeta **EU:s verktygslåda mot varumärkesförfalskning**, som tillkännagavs i handlingsplanen för immateriella rättigheter[82] och som betonades i strategin mot organiserad brottslighet.

Korruption skadar inte bara förtroendet mellan staten och medborgarna utan utgör även ett hot mot säkerheten. Det är ett viktigt verktyg för den organiserade brottsligheten och möjliggör en mängd olika typer av brottslig verksamhet. Korruption är ett centralt tema i den årliga rapporten om rättsstatsprincipen[83]. Även om vissa EU-medlemsstater fortfarande är bland de bästa i världen på att bekämpa korruption kvarstår många utmaningar, särskilt när det gäller brottsutredningar, åtal och tillämpningen av påföljder för korruption. Många medlemsstater har vidtagit åtgärder för att stärka ramarna för förebyggande av korruption och integritet, men de resurser som anslås till korruptionsbekämpning är ofta otillräckliga. Kommissionen arbetar med ett antikorruptionspaket för 2023 som kommer att innebära en uppdatering och en uppstramning av lagstiftningen på detta område.

EU:s handlingsplan mot **olaglig handel med skjutvapen** 2020–2025[84] antogs i juli 2020 tillsammans med strategin för EU:s säkerhetsunion. Den följdes i oktober 2022 upp med ett förslag till översyn av reglerna om import-, export- och transiteringsåtgärder för skjutvapen[85], med ett bredare fokus på digitalisering. På det hela taget bör detta förbättra spårbarheten för civila skjutvapen. Arbete pågår också för att bättre stödja Ukraina och Republiken Moldavien när det gäller **handeldvapen och lätta vapen** i samband med Rysslands aggression mot Ukraina.

---

78 Europol, *Does crime still pay? Criminal Asset Recovery in the EU – Survey of statistical information 2010–2014*, 2016.

79 COM(2021) 421 final, COM(2021) 420 final, COM(2021) 423 final och COM(2021) 422 final. En politisk överenskommelse nåddes i juni 2022 om förordningen om överföring av medel och en partiell allmän riktlinje fastställdes också om förordningen om inrättande av en myndighet för bekämpning av penningtvätt och finansiering av terrorism (utom bestämmelser om resurser och säte) i juni 2022.

80 COM(2022) 245 final.

81 Eppos första årsrapport, 2022.

82 COM(2020) 760 final.

83 Den senaste utgåvan av rapporten antogs den 13 juli 2022 (COM(2022) 500 final).

84 COM(2020) 608 final.

85 COM(2022) 480 final.

Den olagliga handeln med kulturföremål är en lukrativ verksamhet för organiserade kriminella grupper, och i vissa fall även för parter i konflikter och terrorister[86]. Den stimulerar därför den organiserade brottsligheten och har en skadlig inverkan på kulturarvet. Brottslingar kan även missbruka kulturföremål som förvärvats på laglig väg för penningtvätt, kringgående av sanktioner, skatteundandragande eller finansiering av terrorism. För att stärka **kampen mot den olagliga handeln med kulturföremål** antar kommissionen i dag en handlingsplan[87].

Enligt Interpol och FN:s miljöprogram är **miljöbrott** den fjärde största brottsliga verksamheten i världen efter narkotikahandel, människohandel och varumärkesförfalskning. Förhandlingar pågår för närvarande om kommissionens ambitiösa förslag till ett nytt miljöbrottsdirektiv[88], en ny förordning om avfallstransporter[89] och en ny förordning[90] om avskogning. När de väl har antagits kommer de att stärka brottsbekämpningskedjan och leda till hårdare påföljder och ordentliga utredningsverktyg. De kompletteras också av en reviderad handlingsplan mot olaglig handel med vilda djur och växter[91].

Exempel på viktiga resultat

Encrochat: Med stöd av Europol och Eurojust samarbetade rättsliga och brottsbekämpande myndigheter i Belgien, Frankrike och Nederländerna för att blockera storskaliga organiserade kriminella gruppers användning av krypterad kommunikation. Tjänsten hade 60 000 abonnenter när den stängdes – uppskattningsvis 90 % av dem var kriminella.

EU:s rättsliga och polisiära samarbete ledde till upplösandet av en storskalig organiserad kriminell grupp (Pollino-målet): En gemensam utredningsgrupp som inrättades 2016 mellan Italien, Tyskland och Nederländerna anordnade en insatsdag, samordnad av Eurojust och med stöd av Europol, som ledde till att 34 personer dömdes till totalt mer än 400 års fängelse. Senare dömdes ytterligare tolv personer till mer än 173 års fängelse, och förfaranden pågår fortfarande i flera medlemsstater.

4. ÅTGÄRDER FÖR ATT SÄKERSTÄLLA SÄKERHETEN VID VÅRA GRÄNSER OCH STÖDJA BROTTSBEKÄMPNING OCH RÄTTSLIGT SAMARBETE

Vid sidan av de ekonomiska och sociala fördelarna är ett välfungerande **Schengenområde** avgörande för EU:s säkerhet. Detta kräver en effektiv förvaltning av EU:s yttre gränser och ett fördjupat brottsbekämpningssamarbete. I juni 2021 antog kommissionen en strategi för ett fullt fungerande och motståndskraftigt Schengenområde[92]. I den beskrivs hur åtgärder på området säkerhet, polissamarbete och rättsligt samarbete kan säkerställa att EU förblir motståndskraftigt mot säkerhetshot, även utan kontroller vid de inre gränserna. Strategin förs nu vidare genom en årlig Schengencykel – en ny förvaltningsmodell för Schengenområdet. De framsteg som gjorts kartlades i den första rapporten om tillståndet i Schengen, som antogs i maj 2022[93]. Ett viktigt steg är den ändrade kodexen om Schengengränserna[94], som följer av

[86] Se t.ex. FN:s säkerhetsråds resolutioner 2199 (2015), 2253 (2015), 2322 (2016), 2347 (2017), 2462 (2019) och 2617 (2021), samt G20-ländernas kulturministrars Romförklaring av den 30 juli 2021.
[87] COM(2022) 800 final.
[88] COM(2021) 851 final.
[89] COM(2021) 709 final.
[90] COM(2021) 706 final.
[91] COM(2022) 581 final.
[92] COM(2021) 277 final.
[93] COM(2022) 301 final.
[94] COM(2021) 891 final.

kommissionens förslag från december 2021. Det innehåller nya bestämmelser till stöd för ett effektivt säkerhetssamarbete och åtgärder för en effektivare förvaltning av de yttre gränserna i krissituationer. I och med rådets allmänna riktlinje från juni 2022 är det viktigt att Europaparlamentet och rådet snabbt slutför förhandlingarna. Kommissionen underströk också fördelarna med att inkludera Bulgarien, Rumänien och Kroatien i alla aspekter av Schengen, vilket stärker säkerheten och det ömsesidiga förtroendet för Schengenområdet[95]. I december 2022 antog rådet ett beslut om att tillämpa Schengenregelverket fullt ut i Kroatien[96].

I ett område utan inre gränskontroller bör poliser ha tillgång till samma information som kollegorna i övriga medlemsstater. Normen måste vara ett fullständigt och effektivt samarbete. Därför är det viktigt att förbättra de verktyg som brottsbekämpande och rättsliga myndigheter i hela EU har tillgång till för **informationsutbyte och gränsöverskridande samarbete**. Det paket om polissamarbete som antogs i december 2021[97] innebar en betydande förbättring av de tillgängliga verktygen. Europaparlamentet och rådet har nu nått en politisk överenskommelse om **direktivet om informationsutbyte**, och i juni 2022 antog rådet en rekommendation om att stärka det operativa gränsöverskridande polissamarbetet. Förhandlingarna fortsätter om en förordning om översyn av Prümramen[98] i syfte att underlätta för brottsbekämpande myndigheter att automatiskt utbyta uppgifter på vissa områden, såsom DNA, fingeravtrycksuppgifter och uppgifter ur fordonsregister, och att lägga till ytterligare kategorier, såsom uppgifter ur polisregister och ansiktsbilder. En snabb överenskommelse om **Prüm II-förordningen** skulle ge brottsbekämpande myndigheter i medlemsstaterna möjlighet att använda alla de nya verktygen för informationsutbyte på fältet.

För att mer effektivt bekämpa den gränsöverskridande brottsligheten måste medlemsstaternas brottsbekämpande myndigheter och rättsväsende arbeta hand i hand med stöd från EU-byråer som Europol och Eurojust. **Europols** nya mandat trädde i kraft i juni 2022, vilket gav Europol möjlighet att öka expertisen och den operativa kapaciteten för att bättre stödja medlemsstaterna i kampen mot grov och organiserad brottslighet och terrorism. Mandatet stärker också Europols dataskyddsram och Europeiska datatillsynsmannens tillsyn. Utredande myndigheter och domstolar i olika medlemsstater måste samarbeta och stödja varandra vid utredning och lagföring av brott och utbyta information och bevis på ett säkert och snabbt sätt. **Paketet för digital rättvisa**[99], som antogs i december 2021, bestod av praktiska åtgärder för att förbättra det digitala informationsutbytet om gränsöverskridande terrorismfall, inrätta en samarbetsplattform för att stödja de gemensamma utredningsgruppernas funktion och förbättra digitaliseringen av det gränsöverskridande rättsliga samarbetet och tillgången till rättslig prövning i civilrättsliga, handelsrättsliga och straffrättsliga frågor. Europaparlamentets och rådets snabba antagande av detta paket skulle avsevärt underlätta informationsutbytet mellan rättsliga myndigheter.

Elektroniska bevis används i nästan alla utredningar. Den preliminära politiska överenskommelse om **e-bevisning**[100] som nåddes i november 2022 kommer att möjliggöra ett

[95] COM(2022) 636 final.

[96] Från och med den 1 januari 2023 kommer personkontrollerna vid de inre land- och sjögränserna mellan Kroatien och övriga länder i Schengenområdet att upphöra. Kontrollerna vid de inre luftgränserna kommer att upphöra från och med den 26 mars 2023.

[97] COM(2021) 782 final och COM(2021) 780 final.

[98] COM (2021) 784 final.

[99] COM(2021) 756 final, COM(2021) 757 final och COM(2021) 759 final.

[100] COM(2018) 225 final och COM(2018) 226 final.

säkert utbyte av bevis, vilket är värdefullt för de nationella rättsliga myndigheternas möjligheter att bedriva en effektivare brottsbekämpning.

EU har ett gemensamt ansvar för att **säkra EU:s yttre gränser**. De första enheterna i den europeiska gräns- och kustbevakningens stående styrka är utplacerade sedan januari 2021 och den stående styrkan uppgår nu till omkring 4 800 Frontex-tjänstemän och nationella tjänstemän.

Det ökade antalet irreguljära inresor som i år har noterats på de flesta migrationsrutter har visat hur viktigt det är med systematiska identitets- och säkerhetskontroller av alla migranter som anländer till EU:s yttre gränser samt hälsokontroller som uppfyller gemensamma normer. Säkerheten är ett viktigt tema i den nya migrations- och asylpakten. Möjligheten att snabbt kunna slussa migranter till lämpliga förfaranden enligt **förslaget om screening av tredjelandsmedborgare** skulle bidra till att säkerställa att säkerhetskontroller genomförs, med full respekt för alla skyldigheter i fråga om grundläggande rättigheter. Europaparlamentet har fortfarande inte avgett sin ståndpunkt i fråga om detta förslag.

Den belarusiska regimens **utnyttjande av migranter** för politiska ändamål under andra halvåret 2021 gav upphov till exempellösa rättsliga, operativa och mänskliga utmaningar, bland annat när det gäller säkerheten. Förslaget till kodex om Schengengränserna tar också upp frågan om tredjeländers utnyttjande av migranter för politiska ändamål. De medlemsstater som ställs inför denna situation skulle till exempel kunna begränsa antalet gränsövergångsställen och intensifiera gränsövervakningen.

En ny struktur för EU:s **informationssystem** håller på att utvecklas för att bättre stödja de nationella myndigheternas arbete med att säkerställa säkerheten samt gränsförvaltningen och migrationshanteringen. En central del i detta är Schengens förnyade informationssystem, som bör kunna tas i drift i mars 2023. Andra viktiga verktyg är in- och utresesystemet (planerad drift från och med maj 2023), EU-systemet för reseuppgifter och resetillstånd (Etias) (planerad drift före utgången av 2023) och uppdateringen av informationssystemet för viseringar (VIS). Detta kommer att möjliggöra fler kontroller och täppa till luckor i säkerhetsinformationen genom bättre informationsutbyte mellan medlemsstaterna. Avgörande för detta arbete är systemens interoperabilitet. Det är viktigt att eu-LISA och medlemsstaterna utan dröjsmål vidtar de åtgärder som krävs för att detta ambitiösa projekt ska kunna genomföras fullt ut före utgången av 2024.

Det krävs effektiva **kontroller av inkommande varor** för att minska riskerna för EU och invånarna, samtidigt som legitima EU-företags konkurrenskraft säkerställs. Säkerhetskontrollerna av dessa varor har skärpts genom EU:s uppgraderade importkontrollsystem[101] i syfte att stödja effektiva riskbaserade tullkontroller och åtgärder för att skydda flygfrakten mot terroristhot. Inom programmet för instrumentet för ekonomiskt stöd för tullkontrollutrustning[102] finansieras också öppenhet vid inköp, underhåll och uppgradering av relevant och tillförlitlig tullkontrollutrustning som är anpassad till den senaste tekniska utvecklingen.

[101] Importkontrollsystemet 2 (ICS2) kommer att tas i drift i tre versioner (mars 2021, mars 2022 och mars 2023). Varje version påverkar olika ekonomiska aktörer och transportmodeller.

[102] Förordning (EU) 2021/1077 av den 24 juni 2021 om inrättande, som en del av Fonden för integrerad gränsförvaltning, av instrumentet för ekonomiskt stöd för tullkontrollutrustning.

Möjligheten att med **förhandsinformation om passagerare (API)** bidra till säkerheten hindras av föråldrade och ojämnt tillämpade regler. Kommissionens nya förslag skulle upphäva det nuvarande API-direktivet för att förtydliga och förbättra användningen av API för både gränsförvaltning och brottsbekämpning[103]. Det skulle medföra en utökad användning av API vid utvalda flygningar inom EU och ge medlemsstaternas brottsbekämpande myndigheter inom Schengenområdet en större verktygslåda att arbeta med. Diskussioner pågår om den externa dimensionen av EU:s politik för **passageraruppgifter** (PNR-uppgifter), eftersom allt fler tredjeländer håller på att utveckla förmågan att behandla sådana uppgifter inom brottsbekämpning och gränssäkerhet. Kommissionen håller också på att utarbeta ett lagstiftningsförslag om en ram för ömsesidigt tillträde till säkerhetsrelaterad information för tjänstemän i frontlinjen i EU och partnerländer utanför EU för att effektivt upptäcka brottslingar och terrorister.

Bedrägerier med resehandlingar underlättar för brottslingar och terrorister att förflytta sig i hemlighet, och spelar en viktig roll i människohandeln och i narkotikahandeln. Detta måste hanteras parallellt med behovet av att underlätta för lagliga resenärer. Sedan augusti 2021 utfärdar medlemsstaterna därför identitetskort med harmoniserade säkerhetsstandarder, bland annat ett chip med biometriska kännetecken som kan kontrolleras av alla EU:s gränsmyndigheter[104]. Kommissionen håller på att utarbeta ytterligare ett initiativ om digitalisering av resehandlingar och underlättande av resor[105] som kommer att öka säkerheten och påskynda rese- och gränsförfaranden genom papperslös avancerad kommunikation av rese- och personuppgifter och biometriska kontroller vid gränserna.

Brottsbekämpning och ny teknik

Teknik som **artificiell intelligens** eller kryptering kan tillföra ett mervärde för brottsbekämpande och rättsliga myndigheter, men kan också hämma deras arbete. I meddelandet om artificiell intelligens (AI) och i rättsakten om artificiell intelligens[106] underströk kommissionen att AI i hög grad kan bidra till målen i strategin för EU:s säkerhetsunion, motverka aktuella hot och föregripa framtida risker och möjligheter[107]. Inom ramen för Horisont Europa kan inom EU:s forsknings- och innovationsprogram för perioden 2021–2027 finansiering sökas för **forskning** och innovation på området **civil säkerhet**, bland annat om AI eller biometri. Bara för 2021 och 2022 har 413,8 miljoner euro redan avsatts[108].

Exempel på viktiga resultat

Användning av Schengens informationssystem (SIS): Under 2021 gjorde medlemsstaterna nästan 7 miljarder sökningar i SIS. Medlemsstaternas myndigheter gjorde i genomsnitt nästan 20 miljoner sökningar i systemet per dag. Detta ledde i genomsnitt till 600 träffar på utländska registreringar per dag, vilket bidrog till att lösa lika många ärenden. Efter ett brutalt dubbelmord i Rumänien 2021

[103] COM(2022) 729 final och COM(2022) 731 final.

[104] Baserat på Europaparlamentets och rådets förordning (EU) 2019/1157 av den 20 juni 2019 om säkrare identitetskort för unionsmedborgare och uppehållshandlingar som utfärdas till unionsmedborgare och deras familjemedlemmar när de utövar rätten till fri rörlighet (EUT L 188, 12.7.2019, s. 67).

[105] EUR-lex 52022PC0658.

[106] COM(2021) 206 final.

[107] COM(2021) 205 final.

[108] Horisont Europa investerar också betydande medel i innovativ teknik som brottsbekämpande myndigheter kan använda i kampen mot radikalisering samt i projekt för att upptäcka narkotika och sprängämnen, handel med kulturföremål, smuggling av migranter, säkerhet på offentliga platser och identitetsstöld.

kunde till exempel gärningsmannen spåras till Italien bara några dagar senare. Tack vare en SIS-registrering om gripande kunde italienska utredare gripa mannen i Rom.

5. KOPPLINGEN MELLAN INRE OCH YTTRE SÄKERHET: SÄKERHET I EU:S GRANNSKAP OCH PARTNERLÄNDER

Det finns ett nära samband mellan det som händer utanför EU:s gränser och säkerheten inom Europa. Att stödja och hjälpa våra grannar och partner att förbättra sin inre säkerhet och att samarbeta med våra allierade och med internationella organisationer som Nato eller FN är absolut nödvändigt för att stärka EU:s inre säkerhet.

Europeiska utrikestjänsten och kommissionens avdelningar bedriver ett nära samarbete med viktiga partnerländer och internationella organisationer genom regelbundna dialoger om **terrorismbekämpning**. För närvarande förs mer än 30 dialoger om terrorismbekämpning med tredjeländer och internationella organisationer[109]. Samtidigt har nätverket av experter på terrorismbekämpning och säkerhet vid EU:s delegationer i viktiga tredjeländer förstärkts.

För att bättre motverka hot mot den inre säkerheten till följd av Rysslands anfallskrig mot Ukraina kom kommissionens avdelningar och utrikestjänsten tillsammans med EU:s samordnare för kampen mot terrorism överens med **Ukraina** om att inrätta ett fortlöpande strukturerat säkerhetssamarbete. Syftet med detta samarbete är att fördjupa det operativa samarbetet, bland annat med Europol och Frontex, och att stärka informationsutbytet om hot mot den inre säkerheten. EU:s byråer gav omedelbart stöd för att hantera utmaningarna efter invasionen. Frontex har för närvarande 277 anställda utstationerade i regionen, Europol 15 och Europeiska unionens asylbyrå 60.

Medlemsstaternas brottsbekämpande myndigheter och deras partner samarbetar inom ramen för **Europeiska sektorsövergripande plattformen mot brottshot (Empact)** för att organisera operativa insatser och gemensamma insatsdagar mot nya eller framväxande brottshot i samband med Rysslands aggression mot Ukraina.

Dialogen om cybersäkerhet mellan EU och Ukraina har intensifierats med samordnat politiskt, ekonomiskt och materiellt stöd från EU för att hjälpa Ukraina att stärka sin cyberresiliens. Det totala stödet på 29 miljoner euro för att öka Ukrainas cyberresiliens och digitala resiliens har använts till it-säkerhetsutrustning, programvara och resilient digitalisering.

På grund av landets geografiska läge spelar **Moldavien** en viktig roll när det gäller att hantera de straffrättsliga och säkerhetsmässiga konsekvenserna av Rysslands invasion av Ukraina. I juli 2022 lanserade kommissionen, i samarbete med utrikestjänsten, ett EU-stödcentrum för inre säkerhet och gränsförvaltning tillsammans med Moldavien. Dess huvuduppgift är att underlätta samarbete och operativa åtgärder för att hantera gemensamma säkerhetshot inom sex prioriterade områden som EU och Moldavien gemensamt har fastställt: olaglig handel med skjutvapen, smuggling av migranter, människohandel, förebyggande och bekämpande av terrorism och våldsbejakande extremism, cyberbrottslighet och narkotikahandel. I mars 2022 undertecknade Moldavien ett statusavtal med Frontex på grundval av dess förstärkta mandat.

[109] Under 2022 hölls dialoger om terrorismbekämpning med FN, Israel och Indien. Dialoger med Turkiet, Qatar och Förenade Arabemiraten är på gång. Under 2023 förväntas viktiga dialoger hållas med Marocko, Tunisien, Egypten, Kenya, Förenta staterna och Saudiarabien, eventuellt även med Algeriet.

Det brottsbekämpande samarbetet mellan EU och **länderna på västra Balkan** – även med hjälp av EU-byråer – har gradvis fördjupats under de senaste tre åren. I enlighet med rådets slutsatser från mars 2021 integrerades brottsbekämpningssamarbetet med tredjeländer i alla operativa handlingsplaner inom ramen för Europeiska sektorsövergripande plattformen mot brottshot (Empact), vilket också ökade västra Balkans deltagande i Empacts verksamhet. EU fortsätter att inom ramen för instrumentet för stöd inför anslutningen tillhandahålla betydande finansiering för reformer och resultat på brottsbekämpningsområdet, där EU:s byråer också ger säkerhetsaktörer stöd till kapacitetsuppbyggnad. Goda framsteg har gjorts i arbetet med den gemensamma handlingsplanen för terrorismbekämpning som undertecknades 2018. När det gäller Nordmakedonien och Albanien undertecknades i december 2022, med tanke på att de flesta av åtgärderna slutförts, en reviderad och uppdaterad version av respektive bilaterala avtal för att ytterligare uppgradera vårt samarbete när det gäller att bekämpa terrorism och förebygga och motverka våldsbejakande extremism.

Den 18 november 2022 godkände rådet att förhandlingar skulle inledas om **Frontex statusavtal** mellan EU och Albanien, Serbien, Montenegro och Bosnien och Hercegovina[110]. Dessa avtal skulle göra det möjligt för Frontex att placera ut gränsförvaltningsenheter för att utföra gränskontrolluppgifter under de berörda nationella myndigheternas ledning. Detta kommer att vara särskilt värdefullt när det gäller att bekämpa smuggling av migranter. Nordmakedonien undertecknade ett statusavtal med Frontex i oktober 2022, på grundval av dess förstärkta mandat.

EU och Förenta staterna har också en lång historia av partnerskap och samarbete i säkerhetsfrågor, som syftar till ett mer systematiskt och snabbt informationsutbyte i frågor som terrorism, radikalisering och organiserad brottslighet. EU och Förenta staterna håller regelbundna gemensamma möten om rättsliga och inrikes frågor för att fördjupa samarbetet i frågor av gemensamt intresse, främja global säkerhet och uppdatera varandra om hur lagstiftningsarbetet fortskrider i rättsliga och inrikes frågor. Europeiska rättsliga och brottsbekämpande organ har ett nära samarbete med de amerikanska kollegorna i operativa och rättsliga frågor. Amerikanska brottsbekämpande myndigheter deltar aktivt i flera av Empacts åtgärder och nätverk inom ramen för ett operativt samarbetsavtal mellan Förenta staterna och Europol. Ett tydligt exempel på det effektiva samarbetet är den operativa insatsstyrkan Greenlight/Trojan Shield, som är en av de största och mest sofistikerade brottsbekämpande insatserna hittills i kampen mot krypterad brottslig verksamhet. Programmet för att spåra finansiering av terrorism mellan EU och Förenta staterna bidrar med många konkreta ledtrådar till terroristutredningar[111]. Samarbetet bygger också på en tydlig övervakning av skyddsåtgärder och kontroller.

Regelbundna dialoger mellan EU och USA om cybersäkerhet stärker samarbetet och samordningen när det gäller både cyberdiplomati och cyberresiliens, inbegripet cybersäkerhetsstandardisering. Handels- och teknikrådet mellan EU och USA har också möjliggjort ett fördjupat samarbete, bland annat i form av ett gemensamt uttalande om cybersäkerhet och åtgärder för potentiellt samarbete när det gäller forskning och utveckling bortom 5G och 6G, exportkontroller och granskning av investeringar samt sanktioner mot Ryssland och Belarus. Handels- och teknikrådet kommer också att ytterligare främja det transatlantiska samarbetet om utländsk informationsmanipulering och inblandning.

[110] Rådets beslut (EU) 2022/2271 – Albanien, Rådets beslut (EU) 2022/2272 – Bosnien och Hercegovina, Rådets beslut (EU) 2022/2273 – Montenegro, Rådets beslut (EU) 2022/2274 – Serbien.

[111] Se den sjätte gemensamma översynen av genomförandet av TFTP-avtalet, COM(2022) 585 final.

Viktiga säkerhetsutmaningar i Afrika har en direkt påverkan på afrikanerna själva och på EU:s säkerhet. Många projekt genomförs för att hjälpa partnerländerna att bygga upp kapacitet för att hantera dessa utmaningar, till exempel genom finansiering av den internationella terrorismbekämpningsakademin (AILCT) i västra Afrika eller genom det regionala initiativet för att öka kapaciteten att bekämpa penningtvätt och motverka finansiering av terrorism i regionen kring Afrikas horn.

Länderna i **Latinamerika och Karibien** är viktiga partner för EU, och ett nytt regionalt Team Europe-initiativ för säkerhet och rättvisa lanserades i maj 2022 för att inrätta ett partnerskap mellan EU och Latinamerika/Karibien för att stärka rättsstatsprincipen och kampen mot organiserad brottslighet.

EU:s förordning om **granskning av utländska direktinvesteringar** trädde i kraft i oktober 2020[112] och utgör en ram för att förbättra skyddet mot utländska direktinvesteringar som utgör en risk för säkerheten eller den allmänna ordningen i mer än en medlemsstat. Under det första hela verksamhetsåret anmäldes över 400 ärenden till kommissionen. Genom förordningen om produkter med dubbla användningsområden[113], som antogs i september 2021, uppgraderades och stärktes EU:s ordning för **kontroll av export av produkter med dubbla användningsområden**. Därmed infördes även nya bestämmelser som innebär att EU – i samordning med medlemsstaterna – kan anta autonoma kontroller av export av produkter och teknik som inte tas upp i förteckningen.

I vår globaliserade värld har grov brottslighet och terrorism blivit alltmer gränsöverskridande. Brottsbekämpande och rättsliga myndigheter bör ges fullständiga möjligheter att samarbeta med externa partner för att garantera allmänhetens säkerhet. Detta kräver att rättsliga myndigheter i tredjeländer öppnar dörren för samarbete och informationsutbyte med **Europol och Eurojust**. Ett avtal som undertecknades i juni 2022 mellan Europol och Nya Zeeland om utbyte av personuppgifter för att bekämpa grov brottslighet och terrorism[114] följs upp av förhandlingar med ett antal andra länder, men i de flesta fall går framstegen fortfarande långsamt. Eurojust har kommit långt i förhandlingarna med Armenien, där en överenskommelse om texten har nåtts, och har inlett förhandlingar med Colombia, Algeriet och Libanon.

I april 2022 vidtog **EU och FN** konkreta åtgärder för att stärka det befintliga partnerskapet för att bekämpa ihållande men föränderliga hot mot internationell fred och säkerhet under den fjärde högnivådialogen om terrorismbekämpning. Det strategiska partnerskapet stärktes ytterligare genom lanseringen av EU:s och FN:s nya facilitet för globala terroristhot – ett EU-finansierat initiativ för att stödja stater som drabbas av terrorism och våldsbejakande extremism, bland annat genom bistånd, utbildning och mentorskap. Andra frågor av gemensamt intresse är framväxande hot med anknytning till ny teknik, bland annat hur de påverkar ungdomar som är en särskild målgrupp för radikalisering till våld, och terrorism som bygger på främlingsfientlighet, rasism och andra former av intolerans, eller i religionens eller trosuppfattningens namn.

[112] Förordning (EU) 2019/452.
[113] Förordning (EU) 2021/821 (omarbetning).
[114] Avtalet beskrevs i positiva ordalag av Europeiska datatillsynsmannen som en förebild för framtida avtal om utbyte av personuppgifter för brottsbekämpande ändamål.

Samarbetet mellan **EU och Nato** har också intensifierats, vilket har gett konkreta resultat på alla samarbetsområden[115]. EU och Nato har intensifierat arbetet och samarbetet efter Rysslands anfallskrig, i form av en enad politisk hållning och samordning för att hjälpa Ukraina att försvara sig och skydda befolkningen. Det strategiska partnerskapet mellan EU och Nato är mer kraftfullt och relevant än någonsin i detta avgörande ögonblick för den euroatlantiska säkerheten. När det gäller resiliens inleddes i januari 2022 en särskild strukturerad dialog, som nu håller på att fördjupas för att underlätta skyddet av kritisk infrastruktur, och EU och Nato kommer att bilda en arbetsgrupp på området. När det gäller militär rörlighet har ytterligare förbättringar gjorts av aspekter som rör transport och tillsyn, bland annat transport av farligt gods. Motverkandet av hybridhot förblir också ett centralt område för samarbetet med Nato. Utbyten sker inom terrorismbekämpning, strategisk kommunikation, utländsk informationsmanipulering och inblandning samt cyberfrågor. En av övningarna var EU Integrated Resolve i november 2022 inom ramen för konceptet parallell och samordnad övning (PACE). Övningen genomfördes tillsammans med Nato-personal i syfte att förbättra samverkan mellan respektive krishanteringsmekanismer.

Sedan september 2022 har EU varit medordförande för det **globala forumet för terrorismbekämpning**. Bland prioriteringarna ingår att ta itu med terroristhotet i Afrika och att integrera jämställdhet och utbildning i politiken för terrorismbekämpning.

Förhandlingar pågår om ett samarbetsavtal mellan unionen och **Interpol** i syfte att nå ett avtal på teknisk nivå under första halvåret 2023. Huvudsyftet är att ytterligare stärka informationsutbytet mellan Interpol och EU:s byråer och organ, att bättre stödja medlemsstaterna och att öka säkerheten för människor inte bara i EU utan i hela världen.

Exempel på viktiga resultat

Operation Desert Light: Europeisk narkotikakartell utslagen i sex länder: I november 2022 genomfördes samordnade razzior i hela Europa och Förenade Arabemiraten, inriktade på både ledningscentralen och logistikinfrastrukturen för narkotikahandeln i Europa. Ledande kriminella hade bildat en ”superkartell” som kontrollerade omkring en tredjedel av kokainhandeln i Europa. Totalt 49 misstänkta har gripits efter utredningar i Spanien, Frankrike, Belgien, Nederländerna och Förenade Arabemiraten med stöd av Europol. Under utredningarna beslagtog brottsbekämpande myndigheter 30 ton narkotika.

6. SLUTSATS

Under de senaste två och ett halvt åren har kommissionen i nära samarbete med Europeiska utrikestjänsten framgångsrikt genomfört nästan alla de åtgärder som anges i strategin för EU:s säkerhetsunion. De många olika förslagen måste antas och framför allt genomföras. Europaparlamentets, rådets och de enskilda medlemsstaternas beslut och åtgärder kommer att vara avgörande för att säkerställa att EU skapar ett robust säkerhetsekosystem för invånarna.

Samtidigt kommer den säkerhetsmiljö som vi befinner oss i att fortsätta att förändras. Sedan strategin för EU:s säkerhetsunion antogs har EU behövt hantera både covid-19-pandemin och effekterna av Rysslands aggression mot Ukraina. Spridningen av hot på nätet har ökat lavinartat liksom behovet av snabb anpassning och framsynthet. EU måste fortsätta att rusta sig för att hantera alla former av framväxande hot som äventyrar allmänhetens säkerhet.

[115] Se sjunde lägesrapporten om genomförandet av den gemensamma uppsättning förslag som godkändes av EU:s och Natos råd den 6 december 2016 och den 5 december 2017, av den 20 juni 2022.

Ständig vaksamhet, beslutsam handling och gemensamma insatser kommer att vara avgörande för EU:s gemensamma framgång framöver.