Europeiska unionens råd

Bryssel den 18 oktober 2023
(OR. en)

14372/23

JAI 1332	COPEN 363
COSI 179	FREMP 292
ENFOPOL 431	JAIEX 66
ENFOCUSTOM 110	CFSP/PESC 1410
IXIM 194	COPS 489
CT 155	HYBRID 73
CRIMORG 137	DISINFO 85
FRONT 327	TELECOM 306
ASIM 92	DIGIT 223
VISA 208	COMPET 1008
CYBER 247	RECH 456
DATAPROTECT 278	CULT 122
CATS 58	COTER 185
DROIPEN 151	CORDROGUE 94

FÖLJENOT

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	18 oktober 2023
till:	Thérèse BLANCHET, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	COM(2023) 665 final
Ärende:	MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET om den sjätte lägesrapporten om genomförandet av EU:s strategi för en säkerhetsunion

För delegationerna bifogas dokument – COM(2023) 665 final.

Bilaga: COM(2023) 665 final

EUROPEISKA
KOMMISSIONEN

Bryssel den 18.10.2023
COM(2023) 665 final

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

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

I. Inledning

För tre år sedan antog kommissionen strategin för en säkerhetsunion 2020–2025[1], där EU:s viktigaste prioriteringar på säkerhetsområdet fastställs. Sedan dess har vi gjort stora framsteg inom strategins alla fyra pelare – vi har tagit fram banbrytande lagstiftning om allt från skydd av kritiska enheter till förbättrad cyberresiliens. Säkerhetshotbilden i Europa och vårt grannskap utvecklas dock ständigt. Terroristattackerna mot en skola i Frankrike och på Bryssels gator de senaste dagarna är en tydlig påminnelse om hur viktigt det är att fortsätta anpassa och förstärka vår säkerhetsstruktur. Cyberattacker utgör ett allt större hot och situationen blir inte bättre av att illasinnade aktörer tar parti i pågående konflikter. Hybridhot, inklusive desinformation, blir allt vanligare. Europol har identifierat Rysslands anfallskrig mot Ukraina som orsaken till en betydande ökning av cyberattacker mot mål i EU, med omfattande attacker som är politiskt motiverade och samordnade av proryska hackergrupper[2]. Detta har märkts i form av blockerad tillgång till internet och avbrott i viktiga tjänster som energinät[3].

EU:s strategi för en säkerhetsunion utformades för att EU bättre ska kunna stå emot den föränderliga hotbilden. De kriser som orsakats av pandemier och krig har visat hur viktigt det är med det tillvägagångssätt som används i strategin – vår beslutsamhet att sammanföra EU:s säkerhetsekosystem och minska gapet mellan de cyberrelaterade och fysiska dimensionerna av säkerhet, inklusive bekämpning av organiserad brottslighet, terrorism och radikalisering.

Men vi måste vara vaksamma och ständigt undersöka vad som saknas i våra ansträngningar för att hålla våra medborgare säkra. Strategin är inriktad på prioriterade områden där EU kan tillföra mervärde för att hjälpa medlemsstaterna att främja säkerheten för alla som lever i Europa. Sedan strategin antogs har alla fastställda åtgärder vidtagits och nya införlivats för att möta de pågående säkerhetsutmaningarna.

Totalt har kommissionen lagt fram 36 lagstiftningsinitiativ inom ramen för strategin för en säkerhetsunion. För mer än hälften av dessa förslag har interinstitutionella förhandlingar redan avslutats med kraftfull ny lagstiftning, vilket beskrivs i tabellen i bilagan. Flera viktiga initiativ som föreslagits av kommissionen är dock fortfarande föremål för förhandlingar av Europaparlamentet och rådet. Den nuvarande valperioden går mot sitt slut i och med valet till Europaparlamentet i juni 2024, och det krävs ett snabbt arbete för att slutföra dessa utestående ärenden, så att medborgarna kan dra full nytta av säkerhetsunionen. Denna sjätte lägesrapport om säkerhetsunionen är därför inriktad på att beskriva de viktiga lagstiftningsärenden och andra ärenden som kommissionen antagit och för vilka mer måste göras för att de ska kunna slutföras och genomföras effektivt.

För redan överenskommen EU-lagstiftning kommer fördelarna med dessa endast att märkas när de omsätts i praktiken. Arbetet måste koncentreras på medlemsstaternas korrekta och fullständiga införlivande, genomförande och tillämpning. Under 2023 fortsatte kommissionen att se till att EU:s strategi för en säkerhetsunion fungerar genom att använda sina institutionella befogenheter för att inleda överträdelseförfaranden när medlemsstaterna inte hade införlivat EU-lagstiftningen eller hade införlivat den på ett felaktigt sätt.

---

1 COM(2020) 605.

2 Samordnade överbelastningsattacker (DDos): Se Europol Spotlight-rapporten *Cyber-attacks: the apex of crime-as-a-service*, 13.9.2023.

3 Sabotageprogram som raderar data har använts flitigt under konflikten i Ukraina för att förstöra data och system, vilket har påverkat tillgången till internet för tusentals abonnenter i EU och ett stort tyskt energiföretag som förlorade tillgången till fjärrövervakning av över 5 800 vindkraftverk. *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict*, Europaparlamentets studie från september 2023 – PE 702.594.

I rapporten sammanfattas också de fall där medlemsstaternas och/eller EU-byråernas insatser är avgörande för genomförandet. EU:s byråer spelar en avgörande roll för att stödja genomförandet av säkerhetsunionens initiativ, och deras ansvarsområden har utvecklats under de senaste åren. I rapporten beskrivs några av de viktigaste nya uppgifter som de har tilldelats för att ge ökat stöd till medlemsstaterna i genomförandet av viktiga initiativ inom ramen för säkerhetsunionen.

Dessutom understryker den geopolitiska situationen betydelsen av den yttre säkerheten för vår inre säkerhet. En starkare inre EU-ram på säkerhetsområdet är nära förbunden med starkare partnerskap och samarbete med tredjeländer. EU måste fortsätta att aktivt undersöka hur engagemang över hela världen kan bidra till att trygga våra medborgares säkerhet.

II. En framtidssäkrad säkerhetsmiljö

Cybersäkerhet och kritisk infrastrukturs motståndskraft

Inom ramen för säkerhetsunionen har EU åtagit sig att se till att alla europeiska medborgare och företag är väl skyddade, både online och offline, och att främja en öppen, säker och stabil cyberrymd. Cyberincidenternas ökande omfattning, frekvens och konsekvenser utgör ett stort hot mot nätverks- och informationssystemens funktion och mot den inre marknaden. Rysslands anfallskrig mot Ukraina har ytterligare förvärrat detta hot, och de nuvarande geopolitiska spänningarna förvärras av ingripanden från en mängd olika statsanslutna aktörer, kriminella och hacktivister. Sabotaget förra hösten av Nord Stream-gasledningarna har visat att viktiga sektorer som energi, digital infrastruktur, transport och rymden är beroende av en resilient kritisk infrastruktur. Den senaste incidenten med en undervattensgasledning och datakabel i Estland och Finland illustrerar behovet av en hög beredskapsnivå för att hantera denna typ av situationer. Även om orsaken till skadorna fortfarande är oklar och utredningar pågår, har informationsutbytet på olika nivåer mellan medlemsstaterna och kommissionen varit uppmuntrande. Störningarna hade ingen omedelbar effekt på internetuppkopplingen eller på säkerheten i gasförsörjningen på europeisk eller lokal nivå. Detta är ett tecken på de framsteg som gjorts och de förstärkta beredskapsinsatserna under de senaste månaderna.

En tydlig och kraftfull rättslig ram är därför nödvändig för att säkerställa dessa kritiska infrastrukturers skydd och resiliens. I detta sammanhang uppnåddes ett avgörande genombrott genom antagandet av det reviderade direktivet om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen[4] och direktivet om kritiska enheters motståndskraft[5], som båda trädde i kraft den 16 januari 2023. Nu uppmanas medlemsstaterna att införliva dessa grundläggande rättsakter snabbt och fullständigt, senast den 17 oktober 2024, för att inrätta en kraftfull unionsram för att skydda den kritiska infrastrukturen i EU mot fysiska hot och cyberhot.

I juli 2023 fastställde kommissionen i en delegerad förordning väsentliga tjänster inom de elva sektorer som omfattas av direktivet om kritiska enheters motståndskraft[6]. Nästa steg är att

[4] Direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och direktiv (EU) 2018/1972 (NIS 2-direktivet).

[5] Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.

[6] C(2023) 4878.

medlemsstaterna genomför riskbedömningar av dessa tjänster. Efter rådets rekommendation[7] av den 8 december 2022 har arbetet intensifierats med stresstester av kritisk infrastruktur, med början i energisektorn, och med att stärka samarbetet med Nato och viktiga partnerländer. Detta arbete ledde till en rapport från EU:s och Natos arbetsgrupp om motståndskraft hos kritisk infrastruktur i juni 2023, som kartlägger de nuvarande säkerhetsutmaningarna för kritisk infrastruktur inom fyra viktiga sektorer (energi, transport, digital infrastruktur och rymden) och ger rekommendationer för att förbättra motståndskraften. Rekommendationerna, bland annat om ökad samordning, informationsutbyte och övningar, genomförs av EU:s och Natos personal inom ramen för den strukturerade dialogen om resiliens.

Kommissionen antog också den 6 september 2023 ett förslag[8] till rådets rekommendation om en plan för att förbättra samordningen på EU-nivå vid försök att störa kritisk infrastruktur med betydande gränsöverskridande relevans. Den 4 oktober 2023 anordnades en övning i form av en scenariobaserad diskussion om blåplanen för att testa hur den skulle tillämpas i praktiken och bidra till de pågående förhandlingarna om förslaget i rådet.

Efter uppmaningar från rådet[9] har kommissionen, den höga representanten och samarbetsgruppen för nät- och informationssäkerhet genomfört riskbedömningar och tagit fram riskscenarier ur ett cybersäkerhetsperspektiv. Detta arbete är inledningsvis inriktat på telekommunikations- och elsektorerna. Genom att alla relevanta organ och nätverk, civila och militära, deltar skapas för första gången en heltäckande och inkluderande unionsomfattande bedömning. Det kommer att ytterligare komplettera de samordnade säkerhetsriskbedömningarna av kritiska försörjningskedjor som äger rum inom ramen för NIS 2, och riskbedömningarna och stresstesterna av kritisk infrastruktur inom sektorerna energi, digital infrastruktur, kommunikation, transport och rymd. För samordningens och konsekvensens skull bör dessa aktiviteter bygga på varandra för att bidra till att fastställa en standardmetod, och de bör vara vägledande för utvecklingen av framtida övningar. Dessa åtgärders framgång kommer nu att bero på medlemsstaternas aktiva engagemang.

Ekonomier och samhällen är alltmer beroende av rymdrelaterade tjänster och data, särskilt på säkerhets- och försvarsområdet. Rymden är en alltmer omtvistad strategisk domän och dess betydelse för säkerheten har ökat, särskilt i efterdyningarna av den ryska invasionen av Ukraina. EU:s rymdstrategi för säkerhet och försvar antogs i mars 2023 för att stärka vår strategiska ställning och autonomi i rymden. Som en viktig åtgärd inom ramen för denna strategi kommer kommissionen 2024 att föreslå en EU-rymdlag som reglerar säkerhet, hållbarhet och resiliens/trygghet för rymdverksamhet i EU.

När det gäller den externa dimensionen stöder en säker infrastruktur den globala ekonomins och leveranskedjornas resiliens[10], och därför innehåller EU:s Global Gateway-strategi en stark säkerhetsdimension. Med tanke på sammankopplingen mellan EU:s och partnerländernas infrastruktur är ytterligare internationellt samarbete också avgörande för att stärka den globala cyberresiliensen och stödja en fri, öppen, säker och trygg cyberrymd.

Cyberresiliensakten

[7] Rådets rekommendation av den 8 december 2022 om en unionsomfattande samordnad strategi för att stärka den kritiska infrastrukturens motståndskraft.

[8] COM(2023) 526.

[9] Rådets slutsatser av den 23 maj 2022 om utvecklingen av Europeiska unionens arbete på cyberområdet och uppmaningen från Nevers av den 9 mars 2022 att stärka EU:s cybersäkerhetskapacitet.

[10] JOIN(2021) 30.

Det är av central betydelse för den europeiska cybersäkerheten att se till att konsumenter och företag kan lita på säkra digitala produkter. Kommissionen försökte tillgodose detta behov i förslaget till förordning om cyberresiliens[11], som antogs den 15 september 2022. Cyberresiliensakten skulle införa obligatoriska övergripande cybersäkerhetskrav för produkter med digitala inslag under fem år eller hela deras livscykel (beroende på vad som är kortast). Den skulle skapa förutsättningar för utformning och utveckling av säkra produkter med digitala inslag, genom att se till att hård- och mjukvaruprodukter släpps ut på marknaden med så få sårbarheter som möjligt. Detta skulle vara ett viktigt delmål för att höja Europas cybersäkerhetsstandarder på alla områden och kommer sannolikt att bli en internationell referenspunkt som ger tydliga fördelar för EU:s cybersäkerhetsindustri på globala marknader. Europaparlamentet och rådet antog sina respektive ståndpunkter i juli 2023 och förhandlingarna bör fortskrida snabbt.

Cybersäkerhetscertifiering spelar också en avgörande roll för att öka förtroendet för IKT-produkter och IKT-tjänster, vilket gör det möjligt för konsumenter, företag och myndigheter att göra välgrundade val med en lämplig cybersäkerhetsnivå. Arbetet med cybersäkerhetscertifiering fortskrider med det europeiska systemet för cybersäkerhetscertifiering baserat på gemensamma kriterier, som utvärderas i kommittéförfarandet. EU:s certifieringsordning för molnsäkerhet (EUCS) håller för närvarande på att utarbetas av Europeiska unionens byrå för cybersäkerhet (Enisa) och diskuteras i Europeiska gruppen för cybersäkerhetscertifiering. Det intensiva arbetet med experter från en rad olika sektorer, konsumenter och leverantörer bör leda till en sund rättslig och teknisk strategi som ger de nödvändiga säkerhetsgarantierna i överensstämmelse med unionsrätten, internationella åtaganden och WTO:s skyldigheter. Dessutom förbereder Enisa kandidatsystemet för EU5G och EU:s e-identitetsplånbok. Samordnade insatser från alla medlemsstater är avgörande för att förbättra den övergripande säkerheten för IKT-produkter, IKT-tjänster och IKT-processer.

Förordningar om informationssäkerhet och cybersäkerhet för EU:s institutioner, organ och byråer

De föreslagna förordningarna om cybersäkerhet och informationssäkerhet vid EU:s institutioner, som lades fram tillsammans i mars 2022, har utvecklats i olika takt. En politisk överenskommelse nåddes i juni om cybersäkerhetsförordningen, vilket möjliggjorde en förstärkning av cybersäkerheten inom alla EU:s institutioner, organ och byråer, och återspeglar den vikt EU fäster vid ett snabbt genomförande av detta förslag. I denna situation är det särskilt oroande med de oväntade långsamma framstegen med det samtida förslaget om informationssäkerhet, som är nödvändigt för att färdigställa en robust rättslig ram för EU:s institutioner, organ och byråer. Båda förslagen bör antas före valet till Europaparlamentet för att göra den europeiska administrationen trovärdig och resilient i det nuvarande geopolitiska sammanhanget. En minimiuppsättning regler och standarder för informationssäkerhet för alla EU:s institutioner, organ och byråer skulle skapa säkerhet för alla berörda parter och säkerställa ett konsekvent skydd mot de föränderliga hoten mot deras information, både EU-klassificerad och icke-klassificerad. Sammantaget skulle dessa nya regler ge en stabil grund för ett säkert informationsutbyte mellan EU:s institutioner, organ och byråer och med medlemsstaterna, med standardiserade metoder och åtgärder för att skydda informationsflöden. Som sådana svarar de mot flera uppmaningar från rådet att öka resiliensen hos EU:s institutioner, organ och byråer och att bättre skydda beslutsfattandet i EU mot skadlig inblandning.

Cybersolidaritetsakten

[11] COM(2022) 454.

Den föreslagna cybersolidaritetsakten[12], som antogs av kommissionen den 18 april 2023 och bygger på den befintliga starka strategiska, politiska och rättsliga ramen kommer att ytterligare bidra till att förbättra möjligheterna att upptäcka cyberhot samt stärka resiliensen och beredskapen på alla nivåer i EU:s cybersäkerhetsekosystem. Dessa mål uppfylls genom följande tre huvudsakliga åtgärder:

(1) Inrättande av en ***europeisk cybersköld*** för att bygga upp och förbättra gemensam kapacitet för upptäckt och situationsmedvetenhet. Den skulle bestå av alla nationella säkerhetscentrum och gränsöverskridande säkerhetscentrum.
(2) Skapande av en ***cyberkrismekanism*** för att hjälpa medlemsstaterna att förbereda sig inför, hantera och omedelbart återhämta sig från betydande och storskaliga cybersäkerhetsincidenter. Stöd för incidenthantering skulle omfatta EU:s cybersäkerhetsreserv, som också skulle vara tillgänglig för EU:s institutioner, organ och byråer och tredjeländer som är associerade till programmet för ett digitalt Europa, förutsatt att deras associeringsavtal till programmet föreskriver detta.
(3) Inrättande av en ***europeisk mekanism för granskning av cybersäkerhetsincidenter*** för att granska och analysera specifika betydande eller storskaliga incidenter. Granskningsrapporten efter incidenten skulle samordnas och utarbetas av Enisa.

Diskussioner har inletts i rådet och Europaparlamentet. Det skulle ge ett stort uppsving åt insatserna för att skydda medborgare och företag i hela EU om förhandlingarna slutförs innan Europaparlamentets nuvarande mandat löper ut.

EU-akademi för cyberkompetens

Samtidigt som cyberhoten ökar behöver EU snabbt yrkesverksamma med den kompetens och de befogenheter som krävs för att förebygga, upptäcka, avskräcka och försvara EU mot cyberattacker. Dess behov av cybersäkerhetspersonal uppskattas för närvarande till 883 000 yrkesverksamma, medan antalet lediga platser uppgick till mellan 260 000 och 500 000 2022. Alla delar av samhället bör uppmuntras att bidra till att fylla denna lucka, men i synnerhet 2022 utgjorde kvinnor endast 20 % av de utexaminerade inom cybersäkerhet och 19 % av specialisterna på informations- och kommunikationsteknik. Som en del av Europaåret för kompetens 2023 antog kommissionen den 18 april 2023[13] ett initiativ som välkomnades av medlemsstaterna[14] om att inrätta en EU-akademi för cyberkompetens för att överbrygga klyftan mellan cybersäkerhet och talanger. EU-akademin för cyberkompetens skulle sammanföra befintliga initiativ om cyberkompetens och förbättra samordningen. Kommissionen uppmuntrar medlemsstaterna, regionala och lokala myndigheter samt europeiska offentliga organ att anta särskilda strategier eller initiativ för cybersäkerhetskunskaper eller att integrera cybersäkerhetskunskaper i relevanta strategier eller initiativ med ett bredare tillämpningsområde (t.ex. cybersäkerhet, digital kompetens, sysselsättning etc.). Privata intressenters deltagande kommer också att vara avgörande för att minska kompetensklyftan inom cybersäkerhet och den därmed sammanhängande bristen på arbetskraft i Europa.

Drönare

Ett annat ökande hot mot offentliga platser och kritisk infrastruktur är skadlig användning av drönare. Incidenter med drönare har blivit allt vanligare både inom och utanför EU, och

[12] COM(2023) 209.
[13] COM(2023) 207.
[14] Rådets slutsatser av den 22 maj 2023 om EU:s politik för cyberförsvar.

lösningar för att bekämpa drönare är ett viktigt verktyg för bl.a. brottsbekämpande myndigheter samt privata operatörer av kritisk infrastruktur. Samtidigt ger legitim användning av drönare ett viktigt bidrag till den dubbla gröna och digitala omställningen[15]. I enlighet med drönarstrategin 2.0 som antogs i november 2022 antar kommissionen i dag ett meddelande om hur man kan motverka potentiella hot från drönare, som styrks av två handböcker med praktisk vägledning om viktiga tekniska aspekter[16]. Initiativet syftar till att erbjuda en omfattande och harmoniserad politisk ram, med en gemensam förståelse av de regler som finns för att bekämpa eventuella hot från drönare och för att vid behov anpassa sig till den snabba tekniska utvecklingen. Medlemsstaterna och berörda privata aktörer uppmanas att samarbeta nära med kommissionen för att se till att den genomförs fullt ut.

Sjö- och luftfartsskydd

Olaglig verksamhet (piratdåd, väpnade rån till havs, smuggling av migranter och människohandel, vapen- och narkotikahandel samt terrorism) utgör fortfarande utmaningar för sjöfartsskyddet och situationen förvärras av nya hot som hybrid- och cyberattacker. Kommissionen och den höga representanten antog den 10 mars 2023 ett gemensamt meddelande om uppdatering av EU:s strategi för sjöfartsskydd[17], som nu bör genomföras i linje med den uppdaterade handlingsplanen.

På området luftfartsskydd antog kommissionen den 2 februari 2023 ett arbetsdokument *Working towards an enhanced and more resilient aviation security policy*[18], som innehåller ett ambitiöst program för att 1) modernisera regelverket för luftfartsskydd och 2) främja utvecklingen och införandet av mer innovativa lösningar och (3) uppdatera grunden för luftfartsskyddet så att flygplatserna i EU fullt ut kan dra nytta av ny och banbrytande teknik för att hantera de högst prioriterade hoten. Fjorton flaggskeppsåtgärder måste genomföras inom två år.

Kommissionen uppmanar Europaparlamentet och rådet att skyndsamt slutföra förhandlingarna om följande ärenden, under alla omständigheter före utgången av det nuvarande Europaparlamentets valperiod:

- Förslaget till en cyberresiliensakt.
- Förslaget till en cybersolidaritetsakt.
- Den föreslagna förordningen om informationssäkerhet vid EU:s institutioner, organ och byråer.

Kommissionen uppmanar medlemsstaterna att

- fortsätta att prioritera införlivandet av direktivet om kritiska entiteters motståndskraft samt stresstester av kritisk infrastruktur inom energisektorn,
- anta rådets rekommendation om en plan för samordnade insatser vid störningar av kritisk infrastruktur med stor gränsöverskridande betydelse,
- införliva NIS 2-direktivet fullt ut och skyndsamt för att öka cybersäkerheten för väsentliga och viktiga enheter,
- aktivt delta i utförandet av cybersäkerhetsriskbedömningar och bygga upp riskscenarier för kritisk infrastruktur och leveranskedjor,

[15] COM(2022) 652.
[16] COM(2023) 659.
[17] JOIN(2023) 8.
[18] SWD(2023) 37.

- följa upp EU-akademin för cyberkompetens med starkt engagemang på EU-nivå och särskilda nationella strategier eller initiativ för cyberkompetens, där viktiga intressenter, inbegripet regionala och lokala myndigheter, tas med,
- samarbeta med berörda privata aktörer och kommissionen för att säkerställa genomförandet av alla åtgärder som anges i meddelandet om att motverka potentiella hot orsakade av drönare,
- genomföra EU:s handlingsplan för sjöfartsskydd och regelbundet rapportera om resultaten,
- genomföra de 14 flaggskeppsåtgärder som identifierats för att förbättra luftfartsskyddet.

III. Hantera framväxande hot

Nya geopolitiska spänningar har gett tydliga bevis på hur säkerhetsutmaningarna för EU inte bara ökar, utan också blir alltmer instabila och accentueras av många hots hybridkaraktär. Säkerheten måste också anpassas till förändringar i samhället och tekniken. Covid-19-pandemin ökade möjligheterna för cyberbrottslingar och ledde i synnerhet till ett ökat hot från material om sexuella övergrepp mot barn på nätet. Brottslingar och fientliga aktörer är alltid redo att utnyttja den tekniska utvecklingen. Mot bakgrund av sådana ofta komplexa och flerdimensionella hot krävs starka och konsekventa EU-åtgärder.

Förordning om bekämpande av sexuella övergrepp mot barn på nätet

Europols hotbildsbedömning av internetstödd organiserad brottslighet visade att under 2022 hade sexuell exploatering av och sexuella övergrepp mot barn ökat ytterligare i frekvens och allvarlighetsgrad, och förövarna fortsatte att dra nytta av tekniska möjligheter att dölja sina handlingar och identiteter[19]. Det nuvarande systemet som bygger på frivillig upptäckt och rapportering från företag har visat sig vara otillräckligt för att skydda barn. En interimsförordning tillåter frivillig upptäckt och rapportering av företag, förutsatt att detta är lagligt enligt dataskyddsförordningen. Denna förordning upphör att gälla i augusti 2024. I maj 2022 föreslog kommissionen en förordning[20] för att ta itu med missbruk av onlinetjänster för sexuella övergrepp mot barn. I den föreslagna ramen läggs stor vikt vid förebyggande åtgärder. Företagen skulle vara skyldiga att bedöma risken för sexuella övergrepp mot barn via sina system och att vidta förebyggande åtgärder. Som en sista utväg skulle nationella domstolar eller oberoende administrativa myndigheter, endast vid en betydande risk, kunna utfärda riktade spårningsorder till tjänsteleverantörer. Ett nytt oberoende EU-centrum skulle underlätta tjänsteleverantörernas arbete genom att fungera som ett nav för expertis, tillhandahålla tillförlitlig information om identifierat material, ta emot och analysera nätrapporter om sexuella övergrepp mot barn från leverantörer för att identifiera felaktiga rapporter samt ge stöd till offer. Det är viktigt att de nya reglerna antas och genomförs så snart som möjligt för att skydda barn mot ytterligare övergrepp, förhindra att material dyker upp igen på nätet och för att lagföra förövarna. Förhandlingar pågår i rådet och i parlamentet med målet att nå en överenskommelse om ärendet innan parlamentets valperiod löper ut.

[19] Europols hotbildsbedömning av internetstödd organiserad brottslighet (Iocta) 2023.
[20] COM(2022) 209.

Direktiv om bekämpning av våld mot kvinnor och våld i nära relationer

Nätvåld mot kvinnor, även i samband med våld i nära relationer, har vuxit fram som en ny form av våld mot kvinnor som sprids utanför enskilda medlemsstater via internet och it-verktyg. I mars 2022 föreslog kommissionen ett direktiv för att hantera våld mot kvinnor och våld i nära relationer, inklusive särskilda regler om cybervåld och åtgärder för att fylla luckor när det gäller skydd, tillgång till rättslig prövning och förebyggande. Ett tidigt antagande och genomförande skulle ge medlemsstaterna ytterligare verktyg för att bekämpa denna form av brottslighet. Medlagstiftarna inledde interinstitutionella förhandlingar i juli 2023 och siktar på att slutföra förhandlingarna före utgången av Europaparlamentets nuvarande valperiod.

5G-säkerhet

5G-nätens säkerhet är en viktig prioritering för kommissionen och en viktig del av dess strategi för en säkerhetsunion. 5G-nät är en central infrastruktur som utgör grunden för ett brett spektrum av tjänster som är nödvändiga för att den inre marknaden ska fungera och för viktiga samhälleliga och ekonomiska funktioner. Den 15 juni 2023 offentliggjorde de myndigheter i EU:s medlemsstater som är företrädda i samarbetsgruppen för nät- och informationssäkerhet, med stöd av kommissionen och Enisa, en andra lägesrapport om genomförandet av EU:s verktygslåda för 5G-säkerhet. Enligt rapporten har 24 medlemsstater antagit eller håller på att utarbeta lagstiftningsåtgärder som ger nationella myndigheter befogenhet att göra en bedömning av leverantörer och utfärda restriktioner, och tio medlemsstater har infört sådana restriktioner. Det krävs dock ytterligare åtgärder för att undvika sårbarheter som kan medföra allvarliga negativa effekter på säkerheten för enskilda användare och företag i hela EU och den kritiska infrastrukturen i EU. Alla medlemsstater måste genomföra verktygslådan utan dröjsmål. Samma dag antog kommissionen ett meddelande om medlemsstaternas genomförande av verktygslådan och om kommissionens egen företagskommunikation och EU-finansiering. Detta underströk den starka oron över Huawei och ZTE (leverantörer av kommunikationsutrustning för mobilnät), som utgör en risk mot EU:s säkerhet. I detta sammanhang vidtar kommissionen åtgärder för att undvika att dess företagskommunikation exponeras för mobilnät som använder Huawei och ZTE som leverantörer. Upphandlingar kommer att utesluta nya konnektivitetstjänster som är beroende av utrustning från dessa leverantörer och kommissionen kommer att arbeta med medlemsstaterna och telekomoperatörer för att se till att dessa leverantörer successivt fasas ut från befintliga konnektivitetstjänster på kommissionens webbplatser. Kommissionen undersöker också hur detta beslut ska återspeglas i EU:s relevanta finansieringsprogram och finansieringsinstrument, i full överensstämmelse med unionslagstiftningen.

Tillgång till uppgifter för effektiv brottsbekämpning

I dagens digitala tidsålder har nästan alla brott en digital komponent. Teknik och verktyg används också för brottsliga ändamål, inklusive sådana som är nödvändiga för att garantera vårt samhälles behov av cybersäkerhet, dataskydd och integritet. Detta gör det allt svårare att upprätthålla en effektiv brottsbekämpning i hela EU för att skydda den allmänna säkerheten och förebygga, upptäcka, utreda och lagföra brott; även om betydande ansträngningar har gjorts på unionsnivå och nationell nivå, bland annat genom lagstiftning samt kapacitetsuppbyggnad och innovationsinitiativ, kvarstår rättsliga och tekniska utmaningar. Kommissionen har tillsammans med rådets ordförandeskap inrättat en högnivågrupp om tillgång till uppgifter för effektiv brottsbekämpning för att tillhandahålla en samarbetsplattform för ett brett spektrum av intressenter och experter för att utforska de utmaningar som brottsbekämpande myndigheter står inför (t.ex. kryptering, datalagring, 5G och standardisering). Kommissionen förväntar sig att högnivågruppen formulerar välavvägda, kraftfulla och uppnåeliga rekommendationer senast

i juni 2024, vilket återspeglar komplexiteten i dessa frågor, även ur cybersäkerhets- och dataskyddsperspektiv. Medlemsstaterna och de deltagande experterna uppmanas därför att aktivt engagera sig i denna process och arbeta för effektiva, lagliga och allmänt accepterade lösningar.

Hybridhot

I ett geopolitiskt sammanhang där hybridhot blir alltmer komplexa och sofistikerade gav EU:s strategiska kompass för säkerhet och försvar[21] (*den strategiska kompassen*) en gemensam bedömning av de hot och utmaningar som EU står inför samt en strategisk handlingsplan. Ökningen av skadligt beteende i cyberrymden från stater och icke-statliga aktörer, bland annat i samband med kriget mot Ukraina, har ytterligare understrukit cyberrymden som ett utrikes- och säkerhetspolitiskt område. De potentiella riskerna för illvilliga handlingar och desinformation kräver särskild vaksamhet under valperioder, inklusive inför valet till Europaparlamentet 2024.

Med tanke på de stora riskerna för spridningseffekter har EU fortsatt att utveckla kapacitetsuppbyggande cyberverksamhet och främja partnerskap med tredjeländer, bland annat genom särskilda cyberdialoger, för att aktivt bidra till sin övergripande resiliens. Ett antal verktyg har utvecklats, reviderats och stärkts för att förbättra EU:s förmåga att effektivt hantera hybridhot, vilket beskrivs i den sjunde lägesrapporten om hybridhot som offentliggjordes den 14 september 2023[22]. Exempel på dessa är

- EU-verktygslådan för hantering av hybridhot för att säkerställa en ram för en samordnad och välinformerad reaktion på hybridhot och hybridkampanjer,
- det pågående arbetet med att inrätta EU:s snabbinsatsteam för hybridhot för kortsiktigt skräddarsytt stöd till medlemsstater, partnerländer och uppdrag och insatser inom ramen för den gemensamma säkerhets- och försvarspolitiken (GSFP),
- det reviderade EU-protokollet för att motverka hybridhot (*EU Playbook*)[23], som beskriver EU:s processer och strukturer för att hantera hybridhot och hybridkampanjer,
- de reviderade genomföranderiktlinjerna för ramen för EU:s gemensamma diplomatiska svar på skadlig cyberverksamhet[24] (*verktygslåda för cyberdiplomati*) som möjliggör utveckling av varaktiga, skräddarsydda, konsekventa och samordnade strategier mot ihållande cyberhotande aktörer;
- verktygslådan för hantering av utländsk informationsmanipulering och inblandning för att stärka EU:s befintliga verktyg för att förebygga, avskräcka från och reagera på utländsk informationsmanipulering och inblandning,
- EU:s politik för cyberförsvar[25], för att stärka EU:s cyberförsvarskapacitet, förbättra situationsmedvetenheten och samordna alla tillgängliga försvarsalternativ, i syfte att stärka resiliensen, bemöta cyberattacker och säkerställa solidaritet och ömsesidigt bistånd.

Medlemsstaterna uppmuntras därför att fortsätta och stärka sitt samarbete på detta område genom att säkerställa ett effektivt genomförande av ovannämnda verktygslådor, bland annat genom regelbundna övningar, och genom att nå en överenskommelse om konceptet med snabbinsatsteam för hybridhot, vilket kommer att ge vägledning för ytterligare steg mot att inrätta grupperna.

---

[21] Rådets dokument 7371/22.
[22] SWD(2023) 315.
[23] SWD(2023) 116.
[24] 10289/23, 8.6.2023.
[25] JOIN(2022) 49.

AI i brottsbekämpande sammanhang

Artificiell intelligens (AI) har snabbt blivit ett vanligt inslag i vardagen. Effekterna av användningen av AI på it-brottslighet och it-säkerhet är ännu inte helt kända, men kommer helt klart att innebära nya utmaningar. Även om AI kan ge fördelar när det används på ett säkert och kontrollerat sätt kan det ha en farlig potential i händerna på illvilliga aktörer, bland annat genom att hjälpa brottslingar att dölja sina identiteter vid brott såsom terrorism och sexuella övergrepp mot barn. Det är därför viktigt för myndigheterna att hålla sig uppdaterade om utvecklingen för att förhindra missbruk och reagera på missbruk[26]. Förhandlingarna om den föreslagna rättsakten om artificiell intelligens syftar till att ta itu med dessa frågor och har gått in i ett avgörande skede, där medlagstiftarna nu diskuterar tekniska och politiska frågor som kommer att avgöra interaktionen med denna teknik under de kommande åren. Det kommer att vara viktigt att hitta balanserade lösningar, särskilt när det gäller högrisktillämpningar, inklusive inom brottsbekämpningsområdet.

Kommissionen uppmanar Europaparlamentet och rådet att skyndsamt slutföra de interinstitutionella förhandlingarna, i varje fall före utgången av det nuvarande Europaparlamentets valperiod, om följande ärenden som ännu inte avgjorts:

- Förslag till förordning om bekämpande av sexuella övergrepp mot barn på nätet.
- Förslag till direktiv om bekämpning av våld mot kvinnor och våld i nära relationer.
- Förslag till förordning om harmoniserade regler för artificiell intelligens.

Kommissionen uppmanar medlemsstaterna att

- uppnå ett fullständigt genomförande av EU:s verktygslåda om 5G-säkerhet utan dröjsmål,
- stödja högnivågruppens arbete med tillgång till uppgifter för effektiv brottsbekämpning, i syfte att formulera tydliga, kraftfulla och genomförbara rekommendationer för att på ett proportionellt sätt hantera aktuella och förväntade utmaningar,
- i samarbete med den höga representanten vidta åtgärder för att säkerställa ett effektivt genomförande av EU:s verktygslåda för hantering av hybridhot, den reviderade verktygslådan för cyberdiplomati och verktygslådan för hantering av utländsk informationsmanipulering och inblandning, bland annat genom regelbundna övningar och med beaktande av den globala dynamiken,
- nå en överenskommelse om begreppet snabbinsatsteam för hybridhot.

IV. Skydda människor i EU mot terrorism och organiserad brottslighet

Risken för att globala eller lokala händelser utlöser nya utbrott av terrorism är ständigt närvarande. Samtidigt är organiserad brottslighet och narkotikahandel bland de allvarligaste hoten mot EU:s säkerhet. För att intensifiera EU:s gemensamma ansträngningar i kampen mot dessa hot pågår ett gemensamt arbete med att genomföra EU:s strategi för bekämpning av

[26] Se till exempel Europols rapport av den 17 april 2023: *ChatGPT - the impact of Large Language Models on Law Enforcement*.

organiserad brottslighet[27], EU:s strategi mot människohandel[28], EU:s agenda och handlingsplan för narkotika[29] och EU:s agenda för bekämpning av terrorism[30]. För att bemöta den oroväckande försämringen av situationen när det gäller organiserad brottslighet och narkotikahandel krävs det dock att medlemsstaterna och EU intensifierar arbetet ytterligare för att stärka de gemensamma insatserna mot kriminella nätverk och bättre skydda brottsoffer. En EU-färdplan för att bekämpa narkotikahandel och organiserad brottslighet offentliggörs samtidigt med denna rapport[31].

När det gäller terrorismbekämpning stärker EU också sin externa verktygslåda[32] genom att fullt ut utnyttja högnivådialogerna om terrorismbekämpning och nätverket av experter på terrorismbekämpning och säkerhet vid EU-delegationerna samt genom sitt engagemang i multilaterala forum, bland annat som medordförande i det globala forumet för terrorismbekämpning (Global Counter-Terrorism Forum, GCTF).

Narkotikahandel

Med det nya mandatet för EU:s narkotikamyndighet, som ska gälla från och med juli 2024, kommer EU att vara bättre rustat att ta itu med ett komplext säkerhets- och hälsoproblem som påverkar miljontals människor i EU och globalt. Kommissionen håller också på att se över[33] förordningarna om narkotikaprekursorer[34] för att ta itu med de viktigaste utmaningarna i 2020 års utvärdering[35], där man betonade behovet av att ta itu med de utmaningar som designade prekursrer[36] utgör för att minska tillgången till olagliga droger.

Mot bakgrund av en aldrig tidigare skådad ökning av olagliga droger i Europa måste dock kampen mot narkotikahandeln intensifieras i samarbete med internationella partner. Det krävs ytterligare åtgärder från medlemsstaternas och EU:s sida för att avveckla kriminella nätverk och bättre skydda brottsoffer. Kommissionen lägger i dag fram en EU-färdplan för att bekämpa narkotikahandel och organiserad brottslighet. I färdplanen fastställs 17 olika åtgärder på fyra prioriteringsområden: stärka motståndskraften hos logistiska nav med en europeisk hamnallians, upplösa kriminella nätverk, öka de förebyggande insatserna och stärka samarbetet med internationella partner. Dessa åtgärder ska genomföras under 2024 och 2025.

Skjutvapen

Handel med skjutvapen bidrar till organiserad brottslighet inom EU och i grannskapet. Enligt uppskattningar innehas upp till 35 miljoner olagliga skjutvapen av civila i EU, och omkring 630 000 skjutvapen anges som stulna eller försvunna i Schengens informationssystem. I och med utvecklingen av snabba paketleveranser och ny teknik såsom 3D-printing tar sig den olagliga handeln med skjutvapen nya former för att man ska kunna undgå kontroller. Rysslands anfallskrig mot Ukraina har också ökat risken för spridning av skjutvapen. I oktober 2022 antog kommissionen ett förslag om att uppdatera den befintliga lagstiftningen om import, export och

[27] COM(2021)170.
[28] COM(2021) 171.
[29] COM(2020) 606.
[30] COM(2020) 795.
[31] COM(2023) 641.
[32] I enlighet med den strategiska kompassen och rådets slutsatser om hantering av den externa dimensionen av ett ständigt föränderligt hot med koppling till terrorism eller våldsbejakande extremism, som antogs i juni 2022.
[33] Narkotikaprekursorer – reviderade EU-regler (europa.eu).
[34] Förordning (EG) nr 273/2004 om narkotikaprekursorer och rådets förordning (EG) nr 111/2005 om regler för övervakning av handeln med narkotikaprekursorer mellan gemenskapen och tredjeländer.
[35] COM(2020) 768.
[36] Åtgärd 23 i handlingsplanen för narkotika, COM(2020) 606.

transitering av civila skjutvapen, för att täppa till kryphål i de befintliga reglerna som kan öka antalet skjutvapen som smugglas och avleds till EU[37]. På medellång sikt ska de nya reglerna minska risken för kringgående av embargon när det gäller export av skjutvapen för civilt bruk och öka kontrollerna av importen på den typen av skjutvapen från länder utanför EU. Båda medlagstiftarna måste fortfarande anta sina ståndpunkter om detta ärende i syfte att nå en överenskommelse om detta ärende innan parlamentets mandat löper ut.

Människohandel

Människohandel är en särskilt allvarlig form av organiserad brottslighet och en allvarlig kränkning av de grundläggande rättigheterna. Brottsoffer utsätts för människohandel inom EU, främst för sexuell exploatering och arbetskraftsexploatering, men också för påtvingat tiggeri, kriminalitet och andra former. Kommissionen föreslog i december 2022 att direktivet mot människohandel[38] skulle ändras med uppdaterade regler för att åtgärda brister i den nuvarande rättsliga ramen. I synnerhet skulle det reviderade direktivet, när det antagits, lägga till tvångsäktenskap och olaglig adoption till direktivets tillämpningsområde och införa en uttrycklig hänvisning till onlinedimensionen av människohandel. Det skulle också omfatta ett obligatoriskt system med påföljder för förövare och formalisera inrättandet av nationella vidareslussningsmekanismer för att förbättra tidig identifiering och gränsöverskridande vidareslussning för hjälp och stöd till offer. Att medvetet använda tjänster som tillhandahålls av offer för människohandel skulle bli ett brott och årlig insamling av uppgifter om människohandel, som ska offentliggöras av Eurostat, skulle bli obligatorisk. Rådet antog sin allmänna strategi i juni 2023 medan Europaparlamentet fortfarande måste anta sin ståndpunkt. Det kommer att krävas snabba åtgärder för att nå en överenskommelse innan parlamentets mandat löper ut.

Miljöbrott

Miljöbrott har blivit ett globalt hot och ökar uppskattningsvis med mellan 5 och 7 procent varje år. De betydande vinster som kan genereras, kryphålen i lagstiftningen mellan medlemsstaterna och den låga risken för upptäckt lockar till sig organiserad brottslighet. Enligt Europol finns det indikationer på att intäkterna från dessa aktiviteter används för att finansiera terrorism. I december 2021 antog kommissionen ett förslag om att ersätta 2008 års direktiv om skydd för miljön med straffrättsliga bestämmelser. Förslaget är inriktat på att förfina och uppdatera definitionerna av miljöbrottskategorier och att fastställa effektiva, avskräckande och proportionella sanktionstyper och sanktionsnivåer för fysiska och juridiska personer. Nya brott omfattar brott kopplade till olaglig avskogning, överträdelser av EU:s kemikalielagstiftning, olaglig utvinning av ytvatten eller grundvatten och olaglig fartygsåtervinning. Förslaget syftar till att avsevärt stärka brottsbekämpningskedjan och det gränsöverskridande samarbetet mellan medlemsstaternas myndigheter och EU:s byråer och organ. Europaparlamentet och rådet har antagit sina respektive ståndpunkter om förslaget och befinner sig i en förhandlingsprocess som de bör kunna slutföra före årets slut. En reviderad handlingsplan[39] mot olaglig handel med vilda djur och växter kräver genomförande för att ytterligare stärka förebyggandet och efterlevnaden.

Återvinning och förverkande av tillgångar:

[37] COM(2022) 480.
[38] COM(2022) 732.
[39] COM(2022) 581.

Att beröva brottslingar deras olagliga intäkter är avgörande för att störa den organiserade brottsligheten. Utöver förslaget om att ge brottsbekämpande myndigheter tillgång till bankkontoinformation i hela EU[40] (för vilket en politisk överenskommelse nåddes i juni 2023) lade kommissionen därför i maj 2022 fram ett förslag om återvinning och förverkande[41] av tillgångar för att stärka kapaciteten för spårning, identifiering, frysning, förverkande och förvaltning av tillgångar. De viktigaste bestämmelserna i förslaget rör kraven på finansiella utredningar, ytterligare befogenheter och verktyg för kontor för återvinning av tillgångar samt effektivare åtgärder för frysning och förverkande för en bredare uppsättning brott. Ett av de nya brott för vilka dessa åtgärder skulle göras tillämpliga är överträdelse av unionens restriktiva åtgärder. I december 2022 antog kommissionen ett separat förslag om att harmonisera de straffrättsliga definitionerna av och påföljderna för överträdelse av unionens restriktiva åtgärder. Ett effektivt genomförande och verkställande av unionens restriktiva åtgärder är fortfarande en topprioritering för kommissionen och har stärkts av arbetet i arbetsgruppen ”Freeze and Seize”, som kommissionen inrättade som svar på Rysslands anfallskrig mot Ukraina. För båda förslagen har Europaparlamentet och rådet antagit sina ståndpunkter i syfte att nå en överenskommelse före årets slut.

Paketet för bekämpning av penningtvätt

Penningtvätt är kopplat till praktiskt taget all brottslig verksamhet som genererar vinning av brott i EU[42] och är därför en viktig hävstång för att bekämpa brottsligheten i EU. I juli 2021 lade kommissionen fram ambitiösa förslag för att stärka EU:s åtgärder för att förebygga penningtvätt och finansiering av terrorism[43], med fyra lagstiftningsförslag för att stärka förebyggande och upptäckt av kriminellas försök att tvätta olaglig vinning eller finansiera terroristverksamhet genom det finansiella systemet. Ett av paketets fyra initiativ för att säkerställa spårbarhet för överföringar av kryptotillgångar antogs av medlagstiftarna i maj 2023[44]. Denna förordning kommer att börja tillämpas den 30 december 2024, då alla leverantörer av kryptotillgångstjänster måste samla in och lagra information om upphovspersonen till och mottagaren av överföringar av kryptotillgångar. De återstående tre förslagen syftar till att i) inrätta en ny EU-myndighet för bekämpning av penningtvätt för att säkerställa en konsekvent tillsyn av hög kvalitet på hela den inre marknaden, inbegripet av de mest riskfyllda gränsöverskridande enheterna samt stödja och samordna finansunderrättelseenheternas arbete, ii) fastställa harmoniserade regler för den privata sektorn, inbegripet införandet av en EU-gräns på 10 000 euro för stora kontantbetalningar i utbyte mot tjänster och varor, och iii) stärka de behöriga myndigheternas befogenheter och samarbetsverktyg. Paketet förväntas avsevärt förbättra EU:s förmåga att bekämpa penningtvätt och skydda EU-medborgare mot terrorism och organiserad brottslighet. De tre återstående förslagen håller för närvarande på att förhandlas fram av medlagstiftarna i syfte att nå en överenskommelse om detta ärende innan parlamentets mandat löper ut.

Kommissionen uppmanar Europaparlamentet och rådet att skyndsamt slutföra de interinstitutionella förhandlingarna, i varje fall före utgången av det nuvarande Europaparlamentets valperiod, om följande ärenden som ännu inte avgjorts:

- Förslag till direktiv om återvinning och förverkande av tillgångar.

[40] COM(2021) 429.
[41] COM(2022) 245.
[42] Europol, *Enterprising criminals – Europe's fight against the global networks of financial and economic crime*, 2020.
[43] COM(2021) 420.
[44] Förordning (EU) 2023/1113 av den 31 maj 2023 om uppgifter som ska åtfölja överföringar av medel och vissa kryptotillgångar och ändring av direktiv (EU) 2015/849.

- Förslag till direktiv om harmonisering av de straffrättsliga definitionerna av och påföljderna för överträdelser av unionens restriktiva åtgärder.
- Förslag till direktiv mot människohandel.
- Förslag till direktiv om förbättring av miljöskyddet genom straffrättsliga bestämmelser.
- Förslag till ett paket för bekämpning av penningtvätt.
- Förslag om uppdatering av befintlig lagstiftning om import, export och transitering av civila skjutvapen.

Kommissionen uppmanar medlemsstaterna samt EU:s byråer och organ att
- samarbeta för att genomföra de 17 åtgärderna i EU:s färdplan för att bekämpa narkotikahandel och organiserad brottslighet 2023 och 2024.

V. Ett starkt europeiskt säkerhetsekosystem

Under de senaste åren har säkerhetshot blivit alltmer gränsöverskridande till sin karaktär och krävt ytterligare synergieffekter och närmare samarbete på alla nivåer. Sedan strategin för säkerhetsunionen antogs har viktiga initiativ tagits för att maximera det gränsöverskridande samarbetet, rationalisera och uppgradera de tillgängliga instrumenten och förfarandena både vid de yttre gränserna och inom Schengenområdet, samt förbättra informationsutbytet mellan brottsbekämpande och rättsliga myndigheter för att bättre bekämpa den organiserade brottsligheten. Mot denna bakgrund är ett effektivt genomförande av interoperabilitetsramen för utbyte av uppgifter en viktig pelare för att öka säkerheten och ett effektivt europeiskt svar på gränsöverskridande hot, samtidigt som den fria rörligheten inom EU garanteras.

Ökat informationsutbyte inom Schengenområdet: Förhandsinformation om passagerare (API-uppgifter), passageraruppgifter (PNR-uppgifter) och Prüm II

De två förslag om API-uppgifter som antogs av kommissionen i december 2022[45] skulle stärka EU:s inre säkerhet genom att ge medlemsstaternas brottsbekämpande myndigheter ytterligare verktyg för att bekämpa grov brottslighet och terrorism. Framför allt skulle förhandsinformation om passagerare på flygningar inom EU, som används tillsammans med PNR-uppgifter om flygresenärer, göra det möjligt för medlemsstaternas brottsbekämpande myndigheter att avsevärt öka effektiviteten i sina utredningar genom mer målinriktade insatser. Det är viktigt att de föreslagna reglerna antas så snart som möjligt: Detta skulle inte bara stödja kampen mot organiserad brottslighet och terrorism utan också avsevärt minska behovet av systematiska kontroller av alla resenärer i händelse av ett tillfälligt återinförande av kontroller vid de inre gränserna och underlätta flygresor och fri rörlighet. Den 6 september 2023 rekommenderade kommissionen att rådet skulle godkänna förhandlingar med Schweiz, Island och Norge om avtal om överföring av PNR-uppgifter. Antagandet av dessa tre rekommendationer skulle bidra till en konsekvent och effektiv extern PNR-politik för EU.

Prümutbyten används dagligen av polisen för att bekämpa organiserad brottslighet, narkotika, terrorism, sexuellt utnyttjande och människohandel. Förslaget till förordning om automatiskt

[45] COM(2022) 729, COM(2022) 73.

utbyte av uppgifter för polissamarbete (”Prüm II”)[46] innebär en översyn av den befintliga Prümramen i syfte att täppa till informationsluckor och främja förebyggande, upptäckt och utredning av brott i EU. De reviderade reglerna om automatiskt utbyte av uppgifter för polissamarbete kompletterar förslagen om polissamarbete i detta mandat, tillsammans med den redan antagna rådsrekommendationen om förstärkning av det operativa gränsöverskridande samarbetet och direktivet om informationsutbyte mellan brottsbekämpande myndigheter. Ett snabbt antagande och genomförande av dessa relaterade instrument skulle förbättra, underlätta och påskynda utbytet av uppgifter mellan brottsbekämpande myndigheter och bidra till att identifiera brottslingar.

Fullt interoperabelt gränsförvaltningssystem för ett säkert, starkt, digitalt och enat Schengenområde

Ett välfungerande Schengenområde utan inre gränser bygger på ömsesidigt förtroende mellan medlemsstaterna. Detta bygger i sin tur på effektiva kontroller, antingen vid EU:s yttre gränser eller som alternativa åtgärder på medlemsstaternas territorium. I kommissionens ändringsförslag till kodexen om Schengengränserna[47] anges hur medlemsstaterna bättre kan utnyttja alternativ till inre gränskontroller, som kan erbjuda en hög säkerhetsnivå. Det är viktigt att ändringen av kodexen om Schengengränserna antas och genomförs fullt ut för att garantera en hög och proportionell säkerhetsnivå inom Schengenområdet. Den nya strukturen för EU:s informationssystem fortsätter också att utvecklas för att bättre stödja de nationella myndigheternas arbete för att säkerställa säkerhet och gränsförvaltning. Det omfattar Schengens förnyade informationssystem, EU-systemet för reseuppgifter och resetillstånd, in- och utresesystemet, uppdateringen av informationssystemet för viseringar och interoperabilitetsramen för att koppla samman systemen på ett helt säkert sätt. När den nya strukturen är färdig skulle den ge de nationella myndigheterna mer omfattande och tillförlitlig säkerhetsinformation. Alla komponenter i interoperabilitetsramen är väsentliga, vilket innebär att en försening i en aspekt eller i en medlemsstat leder till en försenad lansering för alla. Förseningar i den tekniska utvecklingen av in- och utresesystemet bör minimeras, så att in- och utresesystemet kan tas i drift så snart som möjligt och alla viktiga delar av ramen för driftskompatibilitet kan inrättas.

Förslaget om screening[48] skulle öka säkerheten inom Schengenområdet genom att skapa enhetliga regler för identifiering av tredjelandsmedborgare som inte uppfyller inresevillkoren enligt kodexen om Schengengränserna, och för att låta dem genomgå hälso- och säkerhetskontroller vid de yttre gränserna. Det föreslagna Eurodac-systemet skulle stödja dessa mål genom att ange när det efter screening visar sig att en person kan utgöra ett hot mot den inre säkerheten. Detta skulle i sin tur underlätta genomförandet av den föreslagna förordningen om asyl- och migrationshantering. Kommissionen uppmanar medlagstiftarna att snabbt slutföra förhandlingarna om dessa ärenden före utgången av den innevarande valperioden.

Korruptionsbekämpning

Korruption är mycket skadligt för demokratin, för ekonomin och för vår säkerhet, eftersom korruption fungerar som en grogrund för organiserad brottslighet och underlättar fientlig utländsk inblandning. Det är viktigt att framgångsrikt förebygga och bekämpa korruption både för att värna om EU:s värderingar och EU-politikens ändamålsenlighet och för att upprätthålla

[46] COM(2021) 784.
[47] COM(2021) 891.
[48] COM(2020) 612.

rättsstatsprincipen och förtroendet för de styrande och de offentliga institutionerna. Som ordförande Ursula von der Leyen meddelade i sitt tal om tillståndet i unionen 2022 antog kommissionen den 3 maj 2023 ett paket med korruptionsbekämpande åtgärder[49]. Kommissionens förslag till direktiv om bekämpande av korruption omfattar skärpta regler som kriminaliserar korruptionsbrott och harmoniserar påföljder i hela EU. Det möjliggör också effektiva utredningar och åtal och lägger stor vikt vid förebyggande åtgärder och att skapa en integritetskultur där korruption inte tolereras. Diskussioner om detta förslag har inletts i Europaparlamentet och rådet. Dessutom uppmanas medlemsstaterna att genomföra rekommendationerna från pelaren för korruptionsbekämpning i 2023 års rapport om rättsstatsprincipen som antogs den 5 juli 2023. Ett förslag, som lagts fram av den höga representanten och som stöds av kommissionen, föreslår också inrättandet av ett särskilt sanktionssystem inom ramen för den gemensamma utrikes- och säkerhetspolitiken (Gusp) för att bekämpa allvarliga korruptionshandlingar i hela världen.

Förstärkning av brottsoffers rättigheter

Den 12 juli 2023 föreslog kommissionen ändringar av direktivet om brottsoffers rättigheter för att stärka brottsoffers tillgång till information, stöd och skydd, deltagande i straffrättsliga förfaranden och tillgång till ersättning. Ett av de övergripande målen med översynen är att bidra till en hög säkerhetsnivå genom att skapa en säkrare miljö för brottsoffer för att uppmuntra rapportering av brott och minska rädslan för repressalier.

Kommissionen uppmanar Europaparlamentet och rådet att skyndsamt slutföra de interinstitutionella förhandlingarna, i varje fall före utgången av det nuvarande Europaparlamentets valperiod, om följande ärenden som ännu inte avgjorts:

- Förslag till Prüm II-förordning.
- Förslag om förhandsinformation om passagerare (API-uppgifter).
- Förslag om korruptionsbekämpning, särskilt för att inrätta ett särskilt sanktionssystem för den gemensamma utrikes- och säkerhetspolitiken (Gusp).
- Förslag till ändring av förordningen om kodexen om Schengengränserna.
- Förslag till direktiv om brottsoffers rättigheter.
- Förslag om screening.

Kommissionen uppmanar medlemsstaterna att

- säkerställa att in- och utresesystemet träder i kraft så snart som möjligt för att slutföra genomförandet av EU:s arkitektur för informationsutbyte.

VI. Genomförande

Att garantera säkerheten i hela Europa är ett gemensamt ansvar, där varje aktör måste spela sin roll, från att kommissionen och medlagstiftarna antar nya starka, omfattande och praktiska regler, till att medlemsstaterna genomför sådana regler i rätt tid, samt det operativa arbete som utförs på plats av olika myndigheter, organisationer och intressenter. EU:s byråer på områdena rättsliga frågor, inrikes frågor och cybersäkerhet spelar också en nyckelroll, som har ökat genom den senaste tidens utvidgning av deras ansvarsområden.

Förbättrad granskning av mottagare av EU-finansiering

[49] COM(2023) 234.

När kommissionen genomför EU:s budget har den ett ansvar för att se till att mottagarna av EU-finansiering respekterar EU:s värden. De mekanismer och kontrollsystem som avgör vem som kan dra nytta av EU-finansiering är redan kraftfulla, och den pågående omarbetningen av budgetförordningen syftar också till att ge kommissionen starkare rättsliga medel att agera om det behövs. Dessutom arbetar kommissionen för närvarande med att ytterligare förbättra kontrollen av nuvarande och potentiella framtida mottagare av EU-finansiering, genom att förbättra vägledningen om skyldigheter när det gäller respekt för EU:s värden och de konsekvenser som bör följa på en överträdelse av EU:s värden. Detta kommer att klargöra ansvaret både för stödmottagarna och för dem som utför kontroller på EU-nivå och kan fungera som en inspirationskälla för den nationella nivån. Om finansieringsvillkoren inte uppfylls tvekar kommissionen inte att avbryta samarbetet med stödmottagarna i det berörda projektet och att återkräva medel om så krävs. Det är viktigt att medlemsstaterna proaktivt delar med sig av information till kommissionen när de är medvetna om eventuella risker när det gäller organisationer som ansöker om EU-finansiering.

Överträdelser

På säkerhetsområdet har kommissionen genomfört många överträdelseförfaranden. Under 2023 inleddes till exempel ett stort antal överträdelseärenden på grund av underlåtenhet att fullgöra skyldigheter enligt 2021 års förordning om spridning av terrorisminnehåll online (16 medlemsstater)[50], och under åren 2022 och 2023 mottog 20 medlemsstater ytterligare formella underrättelser på grund av felaktigt genomförande av 2011 års direktiv om bekämpande av sexuella övergrepp mot barn[51]. Ett betydande antal överträdelseärenden är fortfarande öppna för bristande överensstämmelse mellan nationell lagstiftning och 2017 års direktiv om bekämpande av terrorism[52] och för underlåtenhet att införliva regler som underlättar användningen av finansiell och annan information för att förebygga, upptäcka, utreda eller lagföra vissa brott[53]. Andra områden där överträdelseförfaranden pågår är skjutvapenlagstiftning, regler om psykoaktiva ämnen som används i narkotika, bekämpning av bedrägeri och förfalskning av andra betalningsmedel än kontanter, bekämpning av penningtvätt, utbyte av kriminalregister mellan EU:s medlemsstater och brottsofferdirektivet. Medlemsstaterna har fått stöd (tekniskt och ekonomiskt) för att genomföra överenskomna initiativ och åtgärder, och kommissionen står till förfogande för att arbeta tillsammans med medlemsstaterna för att optimera genomförandet.

Övervakning genom Schengenutvärderingar och det nya systemet för förvaltning av Schengensamarbetet

Schengenregelverkets utvärderings- och övervakningsmekanism har fortsatt att bidra till ett effektivt genomförande av Schengenreglerna i syfte att öka säkerheten inom området utan interna kontroller. Under 2023 genomfördes de första utvärderingarna inom ramen för Schengenregelverkets förstärkta utvärderings- och övervakningsmekanism, vilket gjorde det möjligt att i tid identifiera och åtgärda strategiska sårbarheter som har en gränsöverskridande inverkan på säkerheten och tryggheten inom EU. Under 2023 inledde kommissionen dessutom en tematisk Schengenutvärdering för att bedöma praxis i medlemsstater som står inför liknande utmaningar i kampen mot narkotikahandeln i EU, med särskilt fokus på stora volymer. Genom

[50] Förordning om åtgärder mot spridning av terrorisminnehåll online.

[51] Direktiv (EU) 2011/93 om bekämpande av sexuella övergrepp mot barn.

[52] Europaparlamentets och rådets direktiv (EU) 2017/541 av den 15 mars 2017 om bekämpande av terrorism, om ersättande av rådets rambeslut 2002/475/RIF och om ändring av rådets beslut 2005/671/RIF.

[53] Europaparlamentets och rådets direktiv (EU) 2019/1153 av den 20 juni 2019 om fastställande av bestämmelser för att underlätta användning av finansiell information och andra uppgifter för att förebygga, upptäcka, utreda eller lagföra vissa brott och om upphävande av rådets beslut 2000/642/RIF.

dessa utvärderingar infördes en förstärkt och mer övergripande inriktning på säkerhetsaspekterna av Schengen. På grundval av resultaten av de regelbundna, tematiska och oanmälda Schengenutvärderingarna fastställde rådet i juni 2023 prioriteringarna för Schengencykeln 2023–2024. I den fastställs fokusområden som kräver ytterligare stimulans för ett säkrare och starkare Schengenområde. Ett effektivt och snabbt genomförande av dessa prioriteringar tillsammans med en ökad politisk samordning inom Schengenrådet kommer att ytterligare stärka kampen mot organiserad brottslighet och maximera det gränsöverskridande operativa samarbetet.

EU-byråernas och EU-organens roll

Partnerskap är avgörande för genomförandet av säkerhetsunionens initiativ, eftersom det krävs arbete av olika nationella och europeiska myndigheter och organ för att uppnå konkreta resultat. Exempelvis möjliggör Europeiska sektorsövergripande plattformen mot brottshot (Empact) ett strukturerat sektorsövergripande samarbete mellan medlemsstaterna, med stöd av alla EU:s institutioner, organ och byråer (bl.a. Europol, Frontex, Eurojust, Cepol, Olaf och eu-Lisa). De insatser som genomförs av Empact, bland annat genom särskilda operativa insatsstyrkor, samordnar medlemsstaternas och operativa partners insatser för att bekämpa kriminella nätverk och grov brottslighet. Bara under 2022 ledde Empact till totalt 9 922 gripanden, över 180 miljoner euro i beslagtagna tillgångar, 9 263 inledda utredningar, 4 019 identifierade offer, över 62 ton beslagtagna droger, 51 identifierade ledande kriminella och tolv gripna samt insatser i samband med anfallskriget mot Ukraina, särskilt för att bekämpa människohandel och skjutvapenrelaterade hot54.

Frontex, Europeiska sjösäkerhetsbyrån (Emsa) och Europeiska fiskerikontrollbyrån (EFCA) fortsätter att stärka sitt samarbete om kustbevakningsfunktioner för att hjälpa nationella myndigheter att öka säkerheten och tryggheten till sjöss. Dessa byråer kommer att bidra stort till genomförandet av EU:s strategi för sjöfartsskydd.

Flera av säkerhetsunionens initiativ har medfört nya ansvarsområden och uppgifter för berörda organ, ibland med personalkrav.

Europeiska unionens cybersäkerhetsbyrå (Enisa)

När det gäller beredskap och incidenthantering för att förbättra cybersäkerheten har kommissionen inrättat en kortsiktig åtgärd för att stödja medlemsstaterna genom att överföra medel från programmet för ett digitalt Europa till **Europeiska unionens cybersäkerhetsbyrå (Enisa)** för att stärka beredskapen och kapaciteten att hantera större cyberincidenter. Förslaget till cybersolidaritetsakt, som antogs i april 2023, bygger på denna åtgärd och kan, när det antagits av medlagstiftarna, ge Enisa ytterligare uppgifter, såsom drift och förvaltning av EU:s framtida cybersäkerhetsreserv eller utarbetande av en incidentgranskningsrapport efter storskaliga cybersäkerhetsincidenter. Den föreslagna cyberresiliensakten skulle ge Enisa i uppdrag att ta emot anmälningar från tillverkare om sårbarheter i produkter med digitala element och incidenter som påverkar säkerheten för dessa produkter, vilka Enisa förväntas vidarebefordra till de relevanta CSIRT-enheterna eller till de relevanta enheterna för hantering av it-säkerhetsincidenter. Enisa förväntas också vartannat år utarbeta en teknisk rapport om

[54] Empacts faktablad med resultat 2022: https://www.consilium.europa.eu/media/65450/2023_225_empact-factsheets-2022_web-final.pdf

framväxande trender när det gäller cybersäkerhetsrisker i produkter med digitala inslag och överlämna den till samarbetsgruppen för nät- och informationssäkerhet.

Europeiska kompetenscentrumet för cybersäkerhet

Europeiska kompetenscentrumet för cybersäkerhet arbetar tillsammans med nätverket av nationella samordningscentrum som EU:s nya organ för att stödja innovation och industripolitik inom cybersäkerhet. Detta ekosystem kommer att stärka kapaciteten hos cybersäkerhetstekniksamhället, upprätthålla spetskompetens inom forskningen och stärka unionsindustrins konkurrenskraft på detta område. Europeiska kompetenscentrumet för cybersäkerhet och de nationella samordningscentrumen kommer att fatta strategiska investeringsbeslut och samla resurser från EU, medlemsstaterna och indirekt från industrin för att förbättra och stärka den tekniska och industriella cybersäkerhetskapaciteten. Europeiska kompetenscentrumet för cybersäkerhet har därför en viktig roll att spela när det gäller att uppnå de ambitiösa cybersäkerhetsmålen i programmet för ett digitalt Europa och programmet Horisont Europa.

Europeiska kompetenscentrumet för cybersäkerhet har rekryterat mer än hälften av sin personal och kommer snart att rekrytera sin verkställande direktör. Redan pågående arbete omfattar cybersäkerhetsdelen av programmet DIGITAL och en ny strategisk agenda[55] för teknikutveckling och spridning som fastställer prioriterade åtgärder för att stödja små och medelstora företag i utvecklingen och användningen av strategiska tekniker, tjänster och processer för cybersäkerhet, för att stödja och öka den yrkesverksamma arbetskraften, och för att stärka forsknings-, utvecklings- och innovationsexpertisen i det bredare europeiska cybersäkerhetsekosystemet.

Europol

Med ett helt nytt mandat kommer **Europol** att vara bättre rustat att stödja medlemsstaterna i kampen mot organiserad brottslighet. Kampen mot narkotikahandeln är en viktig prioritering med tanke på dess växande betydelse och ökande negativa inverkan på EU-medborgarnas säkerhet. Efter godkännande från Europeiska unionens råd den 15 maj 2023 har kommissionen aktivt arbetat för att ingå internationella avtal med Bolivia, Brasilien, Ecuador, Mexiko och Peru om utbyte av personuppgifter med Europol i syfte att förebygga och bekämpa grov brottslighet och terrorism.

Eurojust

Med över 20 års erfarenhet av att ge rättsligt stöd till nationella myndigheter för att bekämpa en lång rad allvarliga och komplexa gränsöverskridande brott har **Eurojust** befäst sin ställning inom EU:s område med frihet, säkerhet och rättvisa. För att stärka det övergripande samarbetet förhandlar kommissionen om internationella avtal för att underlätta samarbetet mellan Eurojust och 13 tredjeländer när det gäller utbyte av personuppgifter för att bekämpa organiserad brottslighet och terrorism[56]. Förhandlingarna har redan slutförts med Armenien och Libanon, pågår med Algeriet och Colombia och har inletts med Bosnien och Hercegovina. Kommissionen uppmanar Europaparlamentet och rådet att ingå avtal med dessa länder före slutet av parlamentets valperiod, för att stärka det gränsöverskridande rättsliga samarbetet och bredda kampen mot gränsöverskridande brottslighet.

Eppo

[55] https://cybersecurity-centre.europa.eu/strategic-agenda_en.

[56] Algeriet, Argentina, Armenien, Bosnien och Hercegovina, Brasilien, Colombia, Egypten, Israel, Jordanien, Libanon, Marocko, Tunisien och Turkiet.

Sedan **Europeiska åklagarmyndigheten (Eppo)** inledde sin operativa verksamhet i juni 2021 har den visat sig vara ett kraftfullt verktyg i EU:s verktygslåda för att utreda och lagföra brott som påverkar EU-budgeten, inbegripet brott som rör deltagande i en kriminell organisation. Kommissionen uppmanar de medlemsstater som ännu inte deltar i Eppos fördjupade samarbete att göra det så snart som möjligt, så att Eppos fulla potential att skydda skattebetalarnas pengar kan utnyttjas.

EUDA

Med ett nytt mandat som antogs av medlagstiftarna i juni 2023 kommer det befintliga Europeiska centrumet för kontroll av narkotika och narkotikamissbruk (EMCDDA) att omvandlas till ett fullvärdigt organ – **Europeiska unionens narkotikamyndighet (EUDA)** – med en stärkt roll. Byrån kommer att kunna bedöma nya hälso- och säkerhetsutmaningar som olaglig narkotika utgör på ett mer omfattande sätt och bidra mer effektivt till arbetet i medlemsstaterna och på internationell nivå. Insamling, analys och spridning av uppgifter kommer även fortsättningsvis att vara byråns huvuduppgift, men det utökade mandatet kommer också att göra det möjligt för byrån att utveckla en allmän kapacitet för bedömning av hot mot hälsa och säkerhet för att identifiera nya hot, inklusive användning av flera substanser, stärka sitt samarbete genom nationella kontaktpunkter och inrätta ett nätverk av laboratorier som förser byrån med rättsmedicinsk och toxikologisk information. Detta kommer att hjälpa byrån att utfärda varningar när särskilt farliga ämnen förekommer på marknaden och öka medvetenheten.

Kommissionen uppmanar Europaparlamentet och rådet att skyndsamt slutföra de interinstitutionella förhandlingarna, i varje fall före utgången av det nuvarande Europaparlamentets valperiod, om följande ärenden som ännu inte avgjorts:

- Förslag till omarbetning av budgetförordningen.

Kommissionen uppmanar medlemsstaterna att

- proaktivt dela med sig av information till kommissionen när de är medvetna om eventuella risker när det gäller organisationer som ansöker om EU-finansiering,
- snabbt genomföra prioriteringarna för Schengencykeln 2023–2024 för ett säkrare och starkare Schengenområde,
- ta itu med de överträdelseförfaranden som har inletts mot dem för att säkerställa ett korrekt införlivande av den berörda lagstiftningen.

VII. Slutsats

De senaste tre åren har präglats av en ständig och beslutsam strävan att ge liv åt ambitionen att skapa en säkerhetsunion för EU. Stora framsteg har gjorts inom hela det säkerhetspolitiska området. Nu kräver verkligheten med ständigt nya hot kontinuerliga ansträngningar med förnyad motivation. Arbetet med den rättsliga ramen måste slutföras i god tid före slutet av parlamentets /valperiod våren 2024. Medlemsstaterna har ett ständigt ansvar för att införliva, genomföra och tillämpa nya lagar. Genomförandet kräver samordnade insatser, även med stöd av EU:s byråer – och mycket ofta ett allt starkare samarbete med våra internationella partner.

Det är bara med gemensamma och beslutsamma ansträngningar från alla berörda som vi kan uppnå de nivåer av trygghet och säkerhet i EU som medborgarna förväntar sig – och under dagens omständigheter bör det vara en prioritet för alla aktörer att bidra till att stärka EU:s säkerhet.