Europeiska unionens råd

Bryssel den 3 april 2025
(OR. en)

7750/25

JAI 415	**COPEN 79**
COSI 55	**FREMP 76**
ENFOPOL 109	**RELEX 413**
CRIMORG 59	**CFSP/PESC 530**
ENFOCUSTOM 53	**PROCIV 32**
IXIM 73	**CIVCOM 85**
CT 42	**COPS 157**
COTER 48	**IPCR 22**
CORDROGUE 43	**HYBRID 29**
CYBER 87	**DISINFO 20**
MIGR 121	**TELECOM 104**
FRONT 80	**DIGIT 58**
ASIM 28	**MI 197**
VISA 51	**COMPET 226**
SCHENGEN 20	**UD 73**
JAIEX 32	**ENV 237**
CATS 13	**TRANS 114**
DATAPROTECT 59	**CULT 27**
DROIPEN 36	**RECH 138**
EU-LISA	***EUDA***
CH	***FRA***
FRONTEX	***NO***
EUAA	***LI***
EUROJUST	***IS***
EPPO	***CEPOL***
EUROPOL	

FÖLJENOT

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	2 april 2025
till:	Thérèse BLANCHET, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	COM(2025) 148 final
Ärende:	MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET, RÅDET, EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN SAMT REGIONKOMMITTÉN om ProtectEU: Europeisk strategi för inre säkerhet

För delegationerna bifogas dokument – COM(2025) 148 final.

Bilaga: COM(2025) 148 final

EUROPEISKA
KOMMISSIONEN

Strasbourg den 1.4.2025
COM(2025) 148 final

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET, RÅDET, EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN SAMT REGIONKOMMITTÉN

om ProtectEU: Europeisk strategi för inre säkerhet

1. ProtectEU: Europeisk strategi för inre säkerhet

Säkerhet är den grundval som alla våra friheter bygger på. Demokrati, rättsstatsprincipen, de grundläggande rättigheterna, EU-medborgarnas välbefinnande, konkurrenskraft och välstånd – de är alla beroende av vår förmåga att tillhandahålla en grundläggande säkerhetsgaranti. I den nya era av säkerhetshot vi nu lever i är EU-medlemsstaternas förmåga att garantera sina medborgare säkerhet mer än någonsin beroende av en **enhetlig, europeisk strategi för att skydda vår inre säkerhet**. I ett skiftande geopolitiskt landskap måste EU fortsätta att leva upp till sitt bestående löfte om fred.

De första stegen mot att bygga upp en europeisk säkerhetsapparat har redan tagits. Under det gångna årtiondet har vi försett unionen med förbättrade kollektiva mekanismer för insatser inom brottsbekämpning och rättsligt samarbete samt gränssäkerhet och mot grov och organiserad brottslighet liksom mot terrorism och våldsbejakande extremism samt för skyddet av EU:s fysiska och digitala kritiska infrastruktur. Det är fortsatt helt avgörande att genomföra tidigare antagen lagstiftning och framtagen politik på ett korrekt sätt.

Karaktären hos dagens hot och den inneboende kopplingen mellan EU:s inre och yttre säkerhet kräver att vi går ännu längre.

Det finns en allvarlig hotbild. Gränserna mellan **hybridhot** och öppen krigföring är inte skarpa. Ryssland har bedrivit en hybridkampanj, både online och offline, mot EU och dess partner för att störa och undergräva sammanhållningen i samhället och de demokratiska processerna samt för att sätta EU:s solidaritet med Ukraina på prov. Fientliga utländska stater och statsunderstödda aktörer försöker infiltrera och störa vår kritiska infrastruktur och våra leveranskedjor, stjäla känsliga uppgifter och positionera sig för att kunna orsaka maximala störningar i framtiden. De använder sig av brott som en tjänst och av kriminella som ombud. Våra leveranskedjors beroende av tredjeländer gör oss dessutom mer sårbara för fientliga staters hybridkampanjer.

Mäktiga **brottsorganisationer** sprider sig i Europa med hjälp av internet, infiltrerar vår ekonomi och påverkar vårt samhälle, vilket framhålls i Europeiska unionens hotbildsbedömning avseende grov och organiserad brottslighet (EU Socta), som nyligen presenterades av Europol[1]. När den organiserade brottsligheten väl har fått fotfäste i ett samhälle eller i en ekonomisk sektor får man kämpa i motvind för att utrota den: en tredjedel av de mest hotfulla kriminella nätverken har varit aktiva i över tio år. Kryptovalutor och parallella finansiella system hjälper dem att tvätta och dölja sin vinning av brott.

Terrorhotnivån i Europa är fortsatt hög. Regionala kriser utanför EU sprider sig och ger terroraktörer med alla olika ideologier förnyad motivation att rekrytera, mobilisera eller bygga upp sin kapacitet. De riktar särskilt sina radikaliserings- och rekryteringsinsatser mot de mest utsatta delarna av våra samhällen, främst vissa unga. De inspirerar till attacker som utförs av ensamagerande och till en kraftig ökning av systemfientlig extremism vars mål är att störa den demokratiska rättsordningen.

De **tekniska framstegen** sker oerhört snabbt och tillhandahåller viktiga verktyg för att förbättra vår säkerhetsapparat. Cyberattacker och utländsk informationsmanipulering blir dock allt vanligare och utnyttjar ny teknik som exempelvis artificiell intelligens. Barn, unga och äldre är särskilt utsatta för risker på nätet, och spridningen av hatpropaganda på nätet hotar yttrandefriheten och den sociala sammanhållningen.

[1] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

Våra liv präglas av en större osäkerhet, och detta blir alltmer kännbart för EU-medborgarna, vars **uppfattning om säkerhet och trygghet i EU** har försämrats till den grad att 64 % av de som tillfrågats om framtiden uttrycker oro över EU:s säkerhet.[2] Företag oroas också i allt högre grad. Felaktig information och desinformation, brottslighet och olaglig verksamhet samt cyberspionage hör alla till de tio största risker som utpekats i 2025 års rapport om globala risker från Världsekonomiskt forum[3].

EU:s medborgare bör **kunna leva utan rädsla**, oavsett om det är på gatan, i hemmet, på offentliga platser, i tunnelbanan eller på internet. I centrum för EU:s säkerhetsarbete ligger skyddet av människor, särskilt de som löper störst risk att utsättas för attacker, vilka tenderar att i oproportionerligt hög grad drabba barn, kvinnor och minoriteter, däribland judar och muslimer. Detta är avgörande för att bygga motståndskraftiga och sammanhållna samhällen.

Kommissionen håller på att ta fram en **europeisk strategi för inre säkerhet** för att bättre kunna motverka hot under de kommande åren. Med hjälp av en kraftfullare rättslig verktygslåda, fördjupat samarbete och ökat informationsutbyte kommer vi att stärka vår motståndskraft och kollektiva förmåga att förutse, förebygga, upptäcka och effektivt svara på säkerhetshot. En enhetlig strategi för inre säkerhet kan hjälpa medlemsstaterna att utnyttja teknikens kraft för att stärka, inte försvaga, säkerheten och samtidigt främja en säker digital miljö för alla. Dessutom utgör den ett stöd i medlemsstaterna gemensamma svar på globala politiska och ekonomiska skiftningar som påverkar unionens inre säkerhet.

Denna strategi vägleds av **tre principer** och sätter respekten för rättsstatsprincipen och de grundläggande rättigheterna i centrum.

För det första fastställs en ambition att förändra säkerhetskulturen. Vi behöver **ett samhälleligt helhetsgrepp** som involverar alla invånare och berörda parter, inbegripet det civila samhället, forskare, den akademiska världen och privata enheter. Åtgärderna inom ramen för strategin bygger därför på en integrerad flerpartsstrategi, där så är möjligt.

För det andra måste **säkerhetsöverväganden integreras i EU:s lagstiftning, politik och program**, däribland EU:s yttre åtgärder. Lagstiftning, politik och program kommer att behöva utarbetas, ses över och genomföras utifrån ett säkerhetsperspektiv, med säkerställande av att det görs nödvändiga säkerhetsöverväganden för att främja en enhetlig och övergripande säkerhetsstrategi.

Slutligen kräver ett säkert, tryggt och motståndskraftigt Europa **stora investeringar från EU:s, medlemsstaternas och den privata sektorns sida**. De prioriteringar och åtgärder som anges i denna strategi kräver tillräckliga personalresurser och ekonomiska resurser för att säkerställa att de kan genomföras. Såsom anges i meddelandet om vägen till nästa fleråriga budgetram[4] kommer EU att behöva öka de offentliga anslagen till och främja forskning och investeringar på säkerhetsområdet, vilket kommer att stärka EU:s strategiska oberoende.

Denna strategi kompletterar dels**unionens strategi för krisberedskap**[5], som anger en integrerad ansats för alla slags risker vad gäller konflikter, katastrofer som orsakas av människan, naturkatastrofer och kriser, dels **vitboken om europeisk försvarsberedskap 2030**[6], som stöder utveckling och anskaffning av försvarsresurser i hela EU för att avskräcka utländska fiender. Kommissionen kommer också att föreslå ett **europeiskt demokratiförsvar**

[2] *Flash Eurobarometer FL550: EU Challenges and Priorities*.
[3] https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf, s. 17.
[4] COM(2025) 46 final.
[5] JOIN(2025) 130 final.
[6] JOIN(2025) 120 final.

som ska stärka demokratins motståndskraft i EU. Tillsammans utgör dessa initiativ en vision för ett säkert, tryggt och motståndskraftigt EU.

En ny europeisk styrning av den inre säkerheten

Kommissionen kommer att samarbeta nära med medlemsstaterna och EU:s organ för att uppgradera EU:s strategi för inre säkerhet på både strategisk och operativ nivå.

Detta kommer att ske genom

- **konsekvent identifiering av de potentiella säkerhets- och beredskapskonsekvenserna av nya och reviderade kommissionsinitiativ från början av och under hela förhandlingsprocessen,**
- **regelbundna möten i kommissionens projektgrupp för europeisk inre säkerhet, med stöd av strategiskt sektorsövergripande samarbete inom kommissionen,**
- **presentationer av hotanalyser med anknytning till den inre säkerheten till stöd för säkerhetsakademins arbete,**
- **diskussioner med medlemsstaterna i rådet om de nya hoten mot den inre säkerheten på grundval av hotanalysen och utbyte om centrala politiska prioriteringar,**
- **och regelbunden rapportering till Europaparlamentet och rådet för att spåra och stödja ett systematiskt genomförande av viktiga säkerhetsinitiativ.**

2. Integrerad situationsmedvetenhet och hotanalys

Vi kommer att förse EU med nya sätt att utbyta och kombinera information och tillhandahålla regelbundna analyser av hot mot den inre säkerheten i EU, vilket bidrar till en omfattande bedömning av risker och hot.

Säkerheten börjar med ett **effektivt förutseende**. EU måste förlita sig på omfattande, tillräckligt autonom och aktuell situationsmedvetenhet och hotanalys. Agerbar underrättelseinformation är avgörande för att bedöma och motverka hot och ligger i slutändan till grund för politiska åtgärder och lagstiftningsåtgärder. Medlemsstaterna uppmanas därför att förbättra den ytterligare genom den gemensamma kapaciteten för underrättelseanalys (SIAC), som är den gemensamma kontaktpunkten för medlemsstaternas underrättelseverksamhet[7]. Vi måste utnyttja **underrättelsebaserade analyser** och **hotbildsbedömningar** på EU-nivå på ett mer effektivt och samarbetsinriktat sätt.

Med utgångspunkt i de olika risk- och hotbildsbedömningar som gjorts på EU-nivå och för specifika sektorer[8] kommer kommissionen att utarbeta **regelbundna analyser av hot mot den inre säkerheten i EU** för att kartlägga de viktigaste säkerhetsproblemen, och dessa ska ligga till grund för politiska prioriteringar. Dessa kommer att bidra till att utveckla en flexibel och lyhörd politik för inre säkerhet som effektivt hanterar framväxande hot, bättre skyddar människor och företag mot attacker och möjliggör riktade politiska insatser i rätt tid. Dessa analyser av hot mot den inre säkerheten i EU kommer även att bidra till **EU:s övergripande**

[7] *Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness*, s. 23.

[8] Bland de sektorsvisa hotbildsbedömningar som ska bidra till denna hotanalys ingår Europeiska unionens hotbildsbedömning avseende grov och organiserad brottslighet (EU Socta), rapporten om den rådande situationen och tendenserna inom terrorismen i Europa, EU:s gemensamma cyberbedömningsrapport samt framtida bedömningar av hot, risker och metoder avseende penningtvätt och finansiering av terrorism som ska utföras av kommissionen och Myndigheten för bekämpning av penningtvätt och finansiering av terrorism.

(sektorsövergripande, för alla slags risker) risk- och hotbildsbedömning som utarbetats av kommissionen och den höga representanten, i enlighet med unionens strategi för krisberedskap.

Tillit och säker hantering är avgörande för informationsutbytet, och för detta krävs tillförlitlig och säker infrastruktur. EU:s institutioner, organ och byråer måste säkerställa sin förmåga att använda **säkra kommunikationskanaler** för utbyte av känsliga och säkerhetsskyddsklassificerade uppgifter sinsemellan och med medlemsstaterna. Investeringar i **interoperabla säkra system** och tillförlitlig teknik kommer att stärka EU:s oberoende och förmåga att hantera kriser och säkerställa operativ resiliens. I detta sammanhang uppmanar kommissionen medlagstiftarna att slutföra förhandlingarna om **förslaget till en förordning om informationssäkerhet i unionens institutioner, organ och byråer**, särskilt för att säkerställa en gemensam ram för hantering av känsliga icke-säkerhetsskyddsklassificerade och säkerhetsskyddsklassificerade uppgifter[9].

För att säkerställa sin egen operativa säkerhet och situationsmedvetenhet kommer kommissionen att se över sin ram för styrning av säkerhet för företag och inrätta ett **integrerat säkerhetscentrum (ISOC, Integrated Security Operations Centre)** för att skydda människor, fysiska tillgångar och verksamheten vid alla kommissionens anläggningar. Kommissionen kommer också att öka sin operativa kapacitet och analyskapacitet för att kartlägga och minska hybridhot.

I linje med unionens strategi för krisberedskap kommer beredskaps- och säkerhetsöverväganden att integreras i EU:s lagstiftning, politik och program. När kommissionen utarbetar eller ser över lagstiftning, politik eller program utifrån ett beredskaps- och säkerhetsperspektiv kommer den konsekvent att kartlägga det rekommenderade alternativets potentiella konsekvenser för beredskapen och säkerheten. Detta kommer att stödjas genom regelbunden utbildning för kommissionens beslutsfattare.

För att stödja medlemsstaterna kommer kommissionen att diskutera de nya hoten mot den inre säkerheten och de viktigaste politiska prioriteringarna med rådet och regelbundet uppdatera rådet om genomförandet av strategin. Dessutom kommer kommissionen att hålla Europaparlamentet och berörda parter informerade om och engagerade i alla relevanta åtgärder.

Nyckelåtgärder

Kommissionen kommer att

- **göra och presentera regelbundna analyser av hot mot EU:s inre säkerhet.**

Medlemsstaterna uppmanas att

- **förbättra underrättelseutbytet med SIAC och säkerställa bättre informationsutbyte med EU:s byråer och organ.**

Europaparlamentet och rådet uppmanas att

- **slutföra förhandlingarna om förslaget till en förordning om informationssäkerhet i unionens institutioner, organ och byråer.**

3. Stärka EU:s säkerhetsresurser

Vi kommer att utveckla nya verktyg för brottsbekämpning, till exempel ett moderniserat Europol, och bättre sätt att samordna och säkerställa ett säkert utbyte av uppgifter och laglig tillgång till uppgifter.

[9] COM(2022) 119 final.

För att effektivt motverka framväxande hot måste EU stärka sina säkerhetsresurser och främja innovation. De brottsbekämpande och rättsliga myndigheterna står längst fram i kampen mot hot mot den inre säkerheten, och de behöver de rätta operativa verktygen och resurserna för att kunna agera snabbt och effektivt. Det är viktigt att dessa myndigheter kan kommunicera och samordna sig över gränserna och mellan olika avdelningar för att effektivt kunna förebygga, upptäcka, utreda och lagföra.

EU:s byråer och organ för inre säkerhet

EU:s byråer och organ inom rättsliga frågor, inrikes frågor och cybersäkerhet har en nyckelroll i den europeiska säkerhetsordningen – en roll som fortsätter att växa allt eftersom deras ansvarsområden ökar.

I dag, 25 år efter dess inrättande, är **Europol** viktigare än någonsin för EU:s säkerhetsram. Byrån bidrar till komplicerade gränsöverskridande utredningar, underlättar informationsutbyte, utvecklar innovativa verktyg för polisarbete och tillhandahåller avancerad expertis för brottsbekämpning. Flera faktorer hindrar dock Europol från att till fullo utnyttja sin operativa potential när det gäller att underlätta utredningar och stödja den operativa verksamheten för att bekämpa gränsöverskridande brottslighet: det handlar om allt från otillräckliga resurser till det faktum att dess nuvarande mandat inte omfattar nya säkerhetshot såsom sabotage, hybridhot eller informationsmanipulering. Därför kommer kommissionen att föreslå **en ambitiös översyn av Europols mandat** för att omvandla Europol till en verkligt operativ polismyndighet som bättre kan stödja medlemsstaterna. Syftet är att stärka Europols tekniska expertis och kapacitet att stödja nationella brottsbekämpande organ, förbättra samordningen med andra byråer och organ och med medlemsstaterna, stärka de strategiska partnerskapen med partnerländer och den privata sektorn och säkerställa en förstärkt tillsyn över Europol.

Dessutom kommer kommissionen att sträva efter att ytterligare **förbättra effektiviteten vid och komplementariteten mellan EU:s byråer och organ för inre säkerhet och göra samarbetet mellan dem mer friktionsfritt**.

Eurojusts mandat kommer att utvärderas och stärkas för att effektivisera det rättsliga samarbetet och förbättra komplementariteten och samarbetet med Europol. Detta inbegriper att öka Eurojusts effektivitet och dess förmåga att tillhandahålla proaktivt stöd och analyser till medlemsstaternas rättsliga myndigheter. Med tanke på att **Europeiska åklagarmyndigheten (Eppo)** har en unik befogenhet att utreda och lagföra brott som skadar unionens ekonomiska intressen kommer kommissionen dessutom att överväga hur Eppos kapacitet att skydda unionens medel bäst kan förbättras. Detta kommer att inbegripa ett stärkt samarbete mellan Eppo och Europol.

Ett effektivt och säkert informationsutbyte mellan byråerna är avgörande för samarbetet. Europol och Frontex behöver ett snabbt ömsesidigt informationsutbyte, även för operativa ändamål, som en uppföljning av det gemensamma uttalandet från januari 2024[10]. **eu-Lisa** spelar en central roll när det gäller säker lagring och tillgång till uppgifter för bättre samordning och effektivare informationsutbyte mellan byråerna. **Europeiska unionens byrå för grundläggande rättigheter** tillhandahåller expertis om skydd av de grundläggande rättigheterna vid utarbetandet och genomförandet av säkerhetspolitik.

Myndigheten för bekämpning av penningtvätt och finansiering av terrorism (Amla) har getts befogenhet att korsanalysera information, baserat på träff/icke träff, mot information som

[10] https://www.europol.europa.eu/cms/sites/default/files/documents/europol-frontex_joint_statement_signed_31.1.2024.pdf.

gjorts tillgänglig av Europol, Eppo, Eurojust och Europeiska byrån för bedrägeribekämpning för att utföra gemensamma analyser av gränsöverskridande fall.

Enisa spelar en central roll i genomförandet av EU:s lagstiftning om cybersäkerhet. I den kommande **översynen av cybersäkerhetsakten** kommer kommissionen att bedöma dess mandat och föreslå att den moderniseras för att stärka dess europeiska mervärde.

Samarbetet mellan tullmyndigheter och andra brottsbekämpande myndigheter kommer att ökas genom det föreslagna inrättandet av **Europeiska unionens tullbyrå** och **EU:s tulldatacentral** inom ramen för EU:s tullreformpaket. Information från den framtida centralen och relaterade uppgifter från Europol, Eurojust, Eppo, Olaf, Amla och Frontex kommer, inom ramen för deras respektive befogenheter, att förbättra den gemensamma analysen och bidra till mer sammanhängande operativ verksamhet, särskilt vid de yttre gränserna. Kommissionen uppmanar medlagstiftarna att skyndsamt slutföra förhandlingarna om EU:s tullreform och kommer att fortsätta att bistå dem i detta syfte.

Den förbättrade komplementariteten mellan Eppo, Olaf, Europol, Eurojust, Amla och Europeiska unionens föreslagna tullbyrå kommer även att bygga på resultaten av den pågående översynen av **EU:s bedrägeribekämpningsarkitektur**. Den inre säkerheten kan gynnas av denna helhetsstrategi, med fokus på bättre användning av både straffrättsliga och administrativa åtgärder, interoperabilitet mellan it-system och förbättrat samarbete.

Kritisk kommunikation

I dag drivs **system för kritisk kommunikation**[11] i de flesta fall isolerat på nationell nivå. Detta innebär att blåljuspersonal ofta inte kan kommunicera med sina motparter när de korsar gränsen till andra medlemsstater. I vissa medlemsstater finns det också begränsningar i kommunikationen mellan olika typer av blåljuspersonal (t.ex. poliser och ambulanspersonal). Standarderna i de flesta system uppfyller inte dagens krav i fråga om funktionalitet och motståndskraft, vilket avsevärt begränsar blåljuspersonalens svarsförmåga, särskilt över gränserna.

För att stärka EU:s förmåga att reagera på kriser kommer kommissionen att föreslå lagstiftning för att skapa ett **EU-system för kritisk kommunikation** som ska sammanlänka medlemsstaternas nästa generations system för kritisk kommunikation i EU. Målet är att systemet ska bygga på tre strategiska pelare: operativ rörlighet, stark motståndskraft och strategiskt oberoende. Initiativet för EU-systemet för kritisk kommunikation kommer att fastställa harmoniserade krav och bidra till att modernisera medlemsstaternas system för kritisk kommunikation så att de kan fungera friktionsfritt. Det kommer även att utvidga systemets täckning genom det kommande systemet IRIS^{2} [12] med flera omloppsbanor. EU-finansierade projekt kommer att bygga upp den tekniska kapaciteten för systemet, som främst förlitar sig på europeiska teknikleverantörer, för att främja EU:s strategiska oberoende inom denna känsliga sektor.

Laglig tillgång till uppgifter

Brottsbekämpande myndigheter och de rättsliga myndigheterna måste kunna utreda och vidta åtgärder mot brott. I dag lämnar nästan alla former av grov och organiserad brottslighet efter

[11] Det vill säga de nätverk som används av brottsbekämpande myndigheter, gränskontrolltjänstemän, tullmyndigheter, civilskydd, brandmän, räddningspersonal och andra viktiga aktörer inom allmän säkerhet och trygghet.

[12] EU:s infrastruktur för motståndskraft, sammankopplingsmöjligheter och säkerhet via satellit.

sig ett digitalt fotavtryck[13]. Omkring 85 % av brottsutredningarna är nu beroende av de brottsbekämpande myndigheternas förmåga att få tillgång till digital information[14].

Högnivågruppen för tillgång till uppgifter för effektiv brottsbekämpning betonade i sin slutrapport[15] att brottsbekämpningen och rättsväsendet under det senaste årtiondet har tappat mark gentemot kriminella som använder sig av verktyg och produkter som tillhandahålls från andra jurisdiktioner av leverantörer som har infört åtgärder som berövar dem möjligheten att samarbeta när rättsliga begäranden görs i enskilda brottmål. Systematiskt samarbete mellan brottsbekämpande myndigheter och privata parter, däribland tjänsteleverantörer, är därför avgörande i framtida insatser för att störa de mest hotfulla kriminella nätverken och enskilda kriminella i och utanför unionen.

I takt med att digitaliseringen blir allt mer genomgripande, och utgör en ständigt växande källa till nya verktyg för kriminella, är det mycket viktigt med en ram för tillgång till data som tillgodoser behovet av att se till att våra lagar efterlevs och skydda våra värden. Samtidigt är det lika viktigt att säkerställa att digitala system förblir skyddade mot obehörig åtkomst för att upprätthålla cybersäkerheten och avvärja nya säkerhetshot. Sådana ramar för tillgång måste också respektera de grundläggande rättigheterna och bland annat säkerställa att integritet och personuppgifter skyddas på lämpligt sätt.

Under de senaste åren har EU vidtagit åtgärder både för att bekämpa **brott på internet och för att underlätta tillgången till digitala bevis för alla brott** genom att anta regler för elektroniska bevis som kommer att gälla fullt ut från och med augusti 2026[16]. Dessa kommer att kompletteras med internationella instrument för utbyte av information och bevis. Kommissionen kommer snart att föreslå att den nya **FN-konventionen mot it-brottslighet** undertecknas och ingås.

Som en uppföljning av högnivågruppens rekommendationer[17] kommer kommissionen under första halvåret 2025 att lägga fram en **färdplan med de rättsliga och praktiska åtgärder** som den föreslår **för att säkerställa laglig och ändamålsenlig tillgång till uppgifter**. Vid uppföljningen av denna färdplan kommer kommissionen att prioritera en bedömning av effekterna av **reglerna för lagring av uppgifter** på EU-nivå och av utarbetandet av en **färdplan för krypteringsteknik** för att identifiera och bedöma tekniska lösningar som skulle göra det möjligt för brottsbekämpande myndigheter att få tillgång till krypterade uppgifter på ett lagligt sätt, vilket skulle skydda cybersäkerheten och de grundläggande rättigheterna.

Operativt samarbete

Kommissionen kommer att samarbeta med medlemsstaterna, EU:s byråer och organ och partnerländer för att stärka det operativa samarbetet, vilket är avgörande för en effektivare strategi för att bekämpa gränsöverskridande organiserad brottslighet och terrorism.

Europeiska sektorsövergripande plattformen mot brottshot (Empact), som är EU:s viktigaste ram för gemensamma åtgärder mot grov och organiserad brottslighet, har uppnått betydande operativa resultat. Nästa Empact-cykel 2026–2029 utgör en möjlighet att ytterligare

[13] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.
[14] https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX:52019PC0070.
[15] *Concluding report of the High-Level Group on access to data for effective law enforcement* – 15/11/2024, 4802e306-c364-4154-835b-e986a9a49281_en.
[16] Europaparlamentets och rådets förordning (EU) 2023/1543 av den 12 juli 2023 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden, EUT L 191, 28.7.2023, s. 118.
[17] Rådets slutsatser om tillgång till uppgifter för effektiv brottsbekämpning (12 december 2024) https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/sv/pdf.

stärka denna ram. För att störa de mest hotfulla kriminella nätverken och enskilda kriminella måste unionen effektivisera och inrikta sina insatser på de mest angelägna prioriteringarna, stärka medlemsstaternas åtaganden och säkerställa en effektiv resursanvändning.

I detta syfte kommer kommissionen att samarbeta med rådets ordförandeskap och medlemsstaterna för att **maximera Empacts potential och ta itu med de viktigaste prioriteringarna för nästa Empact-cykel 2026–2029**. På dessa prioriterade områden finns det ett behov av underrättelser om de mest hotfulla kriminella nätverken, gemensamma utredningar och operativa arbetsgrupper samt kraftfulla rättsliga åtgärder, inbegripet en följ pengarna-princip. Unionen måste dessutom ta itu med rekrytering till kriminalitet och kriminell infiltration samt stärka samarbetet mellan och utbildning för olika organ och den internationella brottsbekämpningen.

Kommissionen kommer också att stödja andra former av **gränsöverskridande operativt brottsbekämpande samarbete mellan medlemsstaterna och Schengenassocierade länder**. Schengenområdet, som inte har några kontroller vid de inre gränserna, kräver ett nära samarbete och informationsutbyte mellan medlemsstaternas brottsbekämpande myndigheter för att säkerställa en hög nivå av inre säkerhet. I dag har tjänstemän inom brottsbekämpningen fortfarande svårt att bedriva övervakning eller genomföra akuta insatser över gränserna[18], och för att motverka hybridhot krävs också ett förstärkt gränsöverskridande samarbete. En **högnivågrupp för det framtida operativa brottsbekämpande samarbetet** bör inrättas för att utveckla en gemensam strategisk vision.

Det är också väldigt viktigt med ett effektivt datautbyte mellan brottsbekämpande myndigheter för ett effektivt gränsöverskridande samarbete. När **interoperabilitetsstrukturen** väl har upprättats kommer den att ge brottsbekämpande myndigheter och Europol verklig tillgång till viktig information. Samtidigt bör EU och dess medlemsstater prioritera bilateralt och multilateralt informationsutbyte genom det rättsliga och tekniska genomförandet av **Prüm II-förordningen**[19] i samarbete med eu-LISA och Europol. Detta kommer att möjliggöra ett säkert automatiserat utbyte av fingeravtryck, DNA-profiler, uppgifter ur fordonsregister, ansiktsbilder och uppgifter ur polisregister via EU-routrar. På nationell nivå måste medlemsstaterna genomföra **direktivet om informationsutbyte**[20], som förbättrar kanalerna för informationsutbyte för ett smidigt gränsöverskridande informationsflöde, och se till att kanalerna integreras med system på unionsnivå, såsom Siena[21].

Ett effektivt gränsöverskridande samarbete förutsätter också att man främjar en **gemensam brottsbekämpningskultur i EU**. Gemensamma program för utbildning, kompetenscentrum och rörlighet är avgörande för att uppnå detta mål. Kommissionen kommer att undersöka hur EU bäst kan stödja utbildning för medlemsstaternas myndigheter, med hjälp av **Cepol** i egenskap av Europeiska unionens byrå för utbildning av tjänstemän inom brottsbekämpning.

[18] Enligt kommissionens bedömning av den verkan som medlemsstaterna gett rådets rekommendation (EU) 2022/915 av den 9 juni 2022 om operativt brottsbekämpande samarbete (5909/25).

[19] Europaparlamentets och rådets förordning (EU) 2024/982 av den 13 mars 2024 om automatisk sökning och automatiskt utbyte av uppgifter för polissamarbete och om ändring av rådets beslut 2008/615/RIF och 2008/616/RIF samt Europaparlamentets och rådets förordningar (EU) 2018/1726, (EU) 2019/817 och (EU) 2019/818 (Prüm II-förordningen), EUT L, 2024/982, 5.4.2024.

[20] Europaparlamentets och rådets direktiv (EU) 2023/977 av den 10 maj 2023 om informationsutbyte mellan medlemsstaternas brottsbekämpande myndigheter och om upphävande av rådets rambeslut 2006/960/RIF, EUT L 134, 22.5.2023, s. 1.

[21] Nätapplikation för säkert informationsutbyte.

Förstärkt gränssäkerhet

Förstärkt resiliens och säkerhet vid de yttre gränserna är avgörande för att motverka hybridhot, såsom användning av migration som vapen, förhindra att fientliga aktörer och varor kommer in i EU och effektivt bekämpa gränsöverskridande brottslighet och terrorism. **Schengens informationssystem (SIS) ska förbättras** under 2026 för att göra det möjligt för medlemsstaterna att föra in varningar om tredjelandsmedborgare som är inblandade i terrorism, inbegripet utländska terroristtstridande, och i andra grova brott, på grundval av uppgifter som tredjeländer delar med Europol.

Förbättrad **interoperabilitet** mellan de storskaliga EU-informationssystemen kommer att ge medlemsstaterna viktig information om personer från tredjeländer som passerar eller avser att passera de yttre gränserna, vilket kommer att hjälpa myndigheterna att bedöma på vilka villkor inresa till medlemsstaternas territorium ska tillåtas[22]. Kommissionen kommer att fortsätta sitt nära samarbete med medlemsstaterna och eu-Lisa för ett snabbt genomförande av dessa system, särskilt **in- och utresesystemet, EU-systemet för reseuppgifter och resetillstånd (Etias) och det reviderade informationssystemet för viseringar (VIS)**, så att de fungerar smidigt och ger säkerhetsfördelar.

För att ytterligare stärka gränssäkerheten och EU-samarbetet mot bakgrund av framväxande hot **kommer kommissionen att föreslå en förstärkning av Frontex.** Antalet tjänstemän vid den europeiska gräns- och kustbevakningen bör över tid tredubblas till 30 000. Byrån bör utrustas med avancerad teknik för övervakning och situationsmedvetenhet, inbegripet underrättelser som är relevanta för den europeiska integrerade gränsförvaltningen och tillgång till en tillförlitlig EU-tjänst för jordobservation för statlig gränskontroll som ska sättas in senast 2027. Detta bör ytterligare förbättra förmågan att upptäcka, förebygga och bekämpa gränsöverskridande brottslighet vid de yttre gränserna samt stärka byråns stöd till medlemsstaterna vid genomförandet av återvändanden, särskilt när det gäller tredjelandsmedborgare som utgör en säkerhetsrisk.

Dokument- och identitetsbedrägerier underlättar smuggling av migranter, människohandel, kriminellas förflyttningar i hemlighet samt olaglig handel med olagliga varor. **Detektorn för multipla identiteter (MID)**[23] kommer att förbättra de nationella myndigheternas förmåga att identifiera personer som använder sig av multipla identiteter och bekämpa identitetsbedrägerier. Kommissionen kommer att undersöka olika sätt att göra rese- och uppehållshandlingar som utfärdas till EU-medborgare och tredjelandsmedborgare säkrare. Dessutom kommer kommissionen att bedöma hur de europeiska digitala identitetsplånböckerna, som ska införas inom ramen för det europeiska ramverket för digital identitet senast i slutet av 2026, kan förbättra säkerheten för resehandlingar och förbättra identitetskontrollen. Detta kommer att komplettera förslagen om digitala resehandlingar och EU:s digitala reseapplikation[24].

Reseinformation är avgörande för att myndigheterna ska kunna identifiera och utreda kriminellas, terroristers och andra säkerhetshots förflyttningar. Det finns en EU-ram för

[22] Framför allt kommer in- och utresesystemet att göra det möjligt för medlemsstaterna att identifiera tredjelandsmedborgare vid Schengenområdets yttre gränser och registrera deras in- och utresor, vilket möjliggör en systematisk identifiering av personer som överskridit den tillåtna vistelsen. Innan en tredjelandsmedborgare anländer till de yttre gränserna kommer EU-systemet för reseuppgifter och resetillstånd (Etias) och informationssystemet för viseringar (VIS) att göra det möjligt för medlemsstaterna att på förhand bedöma om personens vistelse på EU:s territorium skulle utgöra en säkerhetsrisk.

[23] MID är en av de interoperabilitetskomponenter som infördes genom förordning (EU) 2019/818 och förordning (EU) 2019/817.

[24] https://ec.europa.eu/commission/presscorner/detail/sv/ip_24_5047.

information om kommersiella flygresor[25], men behandlingen av uppgifter från andra transportsätt för brottsbekämpande ändamål är fragmenterad. Följaktligen kan kriminella och terrorister utnyttja olika transportsätt för olaglig verksamhet utan att upptäckas. Kommissionen kommer att samarbeta med medlemsstaterna och transportbranschen för att **stärka ramen för reseinformation** genom att undersöka ett unionssystem som ålägger operatörer av privata flygningar att samla in och överföra passageraruppgifter, utvärdera reglerna för behandling av passageraruppgifter och bedöma olika sätt att effektivisera behandlingen av information om resor till sjöss. När det gäller vägtransporter kommer kommissionen att bedöma en utökad användning av system för **automatisk avläsning av registreringsskyltar (ANPR)** och öka möjligheterna till synergier med Schengens informationssystem.

En strategi som styrs av framsyn, innovation och kapacitet

Kommissionen kommer att utveckla **en omfattande framsynsstyrd strategi för inre säkerhet på EU-nivå** som förlitar sig på bästa praxis som kartlagts på nationell nivå. Denna strategi kommer att stödja beslutsfattande och vägleda investeringar i relevant EU-finansierad forskning och innovation på säkerhetsområdet.

Forskning och innovation spelar en avgörande roll inom inre säkerhet genom att skapa lösningar för att motverka framväxande hot, bland annat från missbruk av teknik[26]. EU måste fortsätta att genom EU-finansierad forskning och innovation på säkerhetsområdet[27] investera i utveckling av innovativa verktyg och lösningar för att hantera säkerhetshot samtidigt som man följer EU:s regler och respekterar de grundläggande rättigheterna. Kommissionen bör stödja övergången från forskning till användning för att stödja ett effektivt utnyttjande av denna moderna kapacitet och prioritera **modern teknik** som exempelvis AI. Denna strategi bör inkludera utbildning för att förbättra de brottsbekämpande och rättsliga myndigheternas användning av AI-system och annan teknisk kapacitet. Vidare bör teknikens potential för dubbla användningsområden utnyttjas i båda riktningarna (från civila till försvarsrelaterade och från försvarsrelaterade till civila), där så är relevant[28].

EU:s innovationsknutpunkt för inre säkerhet[29], ett nätverk av innovationslaboratorier som tillhandahåller de senaste innovationsuppdateringarna och effektiva lösningar för att stödja det arbete som utförs av aktörer inom inre säkerhet i EU och medlemsstaterna, kommer att bidra till att integrera forskning i praktik och politik. För att öka Europols effektivitet krävs en förstärkning av Europols verktygsbibliotek som gör det möjligt för Europol att identifiera, utveckla, gemensamt upphandla och tillämpa avancerad teknik operativt. Dessutom kommer kommissionen att inrätta ett **centrum för forskning och innovation på säkerhetsområdet** vid sitt gemensamma forskningscentrum som sammanför forskare för att förkorta cykeln från forskningsresultat till innovation, utveckling och framgångsrikt genomförande, samtidigt som kostnaderna för utveckling, testning och validering minskar.

[25] Ramen för passageraruppgifter (PNR-uppgifter) och förhandsinformation om passagerare (API-uppgifter) upprättades genom direktiv (EU) 2016/681 (”PNR-direktivet”) och förordning (EU) 2025/12 samt förordning (EU) 2025/13 (”API-förordningarna”).

[26] Se rapporten från kommissionens gemensamma forskningscentrum *Emerging risks and opportunities for EU internal security stemming from new technologies* https://publications.jrc.ec.europa.eu/repository/handle/JRC139674.

[27] *Study on strengthening EU-funded security research and innovation – 20 years of EU-Funded Civil Security Research and Innovation* – 2025, https://data.europa.eu/doi/10.2837/0004501.

[28] Enligt Niinistö-rapporten.

[29] EU:s innovationsknutpunkt för inre säkerhet | Europol.

Vårt **europeiska forskningsområde** är till sin natur samarbetsinriktat och är därför genomträngligt för utländsk påverkan och desinformation. Efter antagandet av rådets rekommendation om ökad forskningssäkerhet[30] vidtar kommissionen och medlemsstaterna åtgärder för att ge berörda aktörer nya möjligheter, bland annat genom att inrätta ett expertcentrum för forskningssäkerhet.

Nyckelåtgärder

Kommissionen ska anta

- **ett lagstiftningsförslag om att omvandla Europol till en verkligt operativ brottsbekämpande myndighet under 2026,**
- **ett lagstiftningsförslag om att stärka Eurojust under 2026,**
- **ett lagstiftningsförslag för att stärka Frontex roll och uppgifter under 2026,**
- **ett lagstiftningsförslag om inrättande av ett EU-system för kritisk kommunikation under 2026.**

Kommissionen kommer att

- **presentera en färdplan för hur man ska gå vidare med laglig och ändamålsenlig tillgång till uppgifter för brottsbekämpande myndigheter under 2025,**
- **utarbeta en konsekvensbedömning under 2025 i syfte att uppdatera reglerna om lagring av uppgifter på EU-nivå, beroende på vad som är lämpligt,**
- **presentera en färdplan för krypteringsteknik för att kartlägga och bedöma tekniska lösningar för att ge brottsbekämpande myndigheter laglig tillgång till uppgifter under 2026,**
- **sträva efter att inrätta en högnivågrupp för att stärka det operativa brottsbekämpande samarbetet,**
- **inrätta ett centrum för forskning och innovation på säkerhetsområdet vid sitt gemensamma forskningscentrum under 2026.**

Kommissionen kommer i samarbete med medlemsstaterna och relevanta EU-organ att

- **stärka Empact-arkitekturen,**
- **eftersträva ett snabbt införande av interoperabilitetsstrukturen och genomförandet av Prüm II-förordningen**
- **och stärka ramen för reseinformation.**

Medlemsstaterna uppmanas att

- **införliva och fullt ut genomföra direktivet om informationsutbyte.**

4. Motståndskraft mot hybridhot och andra fientliga handlingar

Vi kommer att bygga upp motståndskraften mot hybridhot genom att förbättra skyddet av kritisk infrastruktur, stärka cybersäkerheten, säkra transportknutpunkter och hamnar och bekämpa hot på nätet.

De fientliga handlingar som undergräver EU:s säkerhet har blivit allt vanligare och mer sofistikerade, och fientliga aktörer har ökat sin arsenal avsevärt. Hybridkampanjer som riktas mot EU, dess medlemsstater och partner har intensifierats, med sabotage riktade mot kritisk infrastruktur, mordbränder, cyberattacker, valinblandning, utländsk informationsmanipulering

[30] EUT C/2024/3510, 30.5.2024.

och inblandning, däribland desinformation, samt användning av migration som vapen. På grund av deras politiska och operativa roll, och den typ av information de hanterar, är unionens institutioner, organ och byråer (*unionens enheter*) inte förskonade.

EU måste **stärka sin motståndskraft**, använda de befintliga verktygen effektivt och utveckla nya sätt att bemöta dessa framväxande hot från statliga och icke-statliga aktörer, både nu och i framtiden.

Kritisk infrastruktur

Hot mot **kritisk infrastruktur**, inbegripet hybridhot såsom sabotage och skadlig cyberverksamhet, är ett stort problem, särskilt för den infrastruktur som förbinder medlemsstaterna – vare sig det gäller förbindelseledningar eller gränsöverskridande kommunikationskablar – samt transporter. Sedan Rysslands anfallskrig mot Ukraina inleddes har sabotage mot kritisk infrastruktur ökat, särskilt under 2024, vilket drabbar många medlemsstater. Samarbete mellan brottsbekämpande myndigheter, säkerhetstjänster och cybersäkerhetstjänster, militärt skydd och civilskydd samt privata aktörer är avgörande för att förutse, upptäcka, förebygga och effektivt svara på sådana handlingar.

Det är absolut nödvändigt att minska sårbarheterna och stärka kritiska entiteters motståndskraft för att säkerställa att samhällsviktiga tjänster som är centrala för ekonomin och samhället tillhandahålls utan avbrott. Ett snabbt införlivande och ett korrekt genomförande i alla medlemsstater av **direktivet om kritiska entiteters motståndskraft (CER-direktivet)**[31] och **direktivet om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS 2-direktivet)**[32] är därför avgörande i detta avseende.

För att säkerställa att det görs snabba framsteg kommer kommissionen att hjälpa medlemsstaterna att identifiera kritiska entiteter[33] och utbyta god praxis om nationella strategier och riskbedömningar som avser samhällsviktiga tjänster, i samarbete med **gruppen för kritiska entiteters motståndskraft och samarbetsgruppen för nät- och informationssäkerhet**. Om det skulle uppstå störningar av kritisk infrastruktur med stora gränsöverskridande konsekvenser kommer **EU-planen för kritisk infrastruktur** att samordna insatserna på EU-nivå. Kommissionen uppmanar rådet att snabbt anta **EU:s cyberplan**, som kommer att ytterligare stärka samordningen i samband med krishantering och främja ett närmare samarbete mellan myndigheter kring fysisk och digital resiliens. Efter framgångsrika stresstester inom energisektorn under 2023 kommer kommissionen att främja **frivilliga stresstester** inom andra sektorer som är centrala för den inre säkerheten. Dessutom kommer kommissionen att tillhandahålla en **översikt på unionsnivå över gränsöverskridande och sektorsöverskridande risker** för samhällsviktiga tjänster som underlag för medlemsstaternas riskbedömningar och en omfattande riskbedömning på EU-nivå. Kommissionen kommer, i linje med unionens strategi för krisberedskap, att samarbeta med medlemsstaterna för att identifiera ytterligare sektorer och tjänster som inte omfattas av den nuvarande lagstiftningen, och där åtgärder kan behöva vidtas.

[31] 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.

[32] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

[33] De sektorer som omfattas av direktivet är energi, transport, bankväsende, finansmarknadsinfrastruktur, hälso- och sjukvård, dricksvatten, avloppsvatten, digital infrastruktur, offentlig förvaltning, rymdsektorn samt produktion, bearbetning och distribution av livsmedel.

EU:s och Natos arbetsgrupp för den kritiska infrastrukturens motståndskraft har främjat ett utmärkt samarbete när det gäller utbyte av bästa praxis och ökad motståndskraft inom sektorerna för energi, transport, digital infrastruktur samt rymdsektorn. Detta arbete kommer att fortsätta inom ramen för den **strukturerade dialogen mellan EU och Nato om motståndskraft**. **EU:s verktygslåda för hantering av hybridhot** hjälper i hög grad medlemsstater och partner att förbereda sig för och motverka hybridhot. **Snabbinsatsteam för hybridhot**[34] tillhandahåller skräddarsytt kortsiktigt stöd på begäran till medlemsstater, olika EU-uppdrag och partner. Kommissionen kommer dessutom att gå vidare med EU-samarbetet kring bekämpning av sabotage genom expertverksamhet[35], inbegripet ett **särskilt gemensamt arbetsprogram** där experterna kan effektivisera informationsutbytet och planera motåtgärder.

Incidenter som påverkar **undervattenskablar** i Europa belyser behovet av kraftfullare åtgärder och tydligare svar. Såsom anges i **EU:s handlingsplan för kabelsäkerhet**[36] kommer kommissionen, tillsammans med den höga representanten, att samarbeta med medlemsstater, EU-organ och partner som exempelvis Nato för att förebygga, upptäcka, vidta svarsåtgärder mot och avskräcka från hot mot undervattenskablar. För att ta fram en integrerad situationsbild av hoten kommer kommissionen att samarbeta med medlemsstaterna för att på frivillig basis utveckla och införa en integrerad övervakningsmekanism för undervattenskablar på havsområdesnivå som börjar med ett regionalt nav i Östersjön/Nordeuropa.

Cybersäkerhet

Den ihållande karaktären hos **skadlig cyberverksamhet**, som ofta utgör en del av ett bredare spektrum av flerdimensionella hot och hybridhot, kräver fortsatt uppmärksamhet och fortsatta åtgärder på EU-nivå. De senaste åren har unionen antagit en rad cybersäkerhetslagar som stärker cyberresiliensen hos NIS 2-entiteter inom EU:s kritiska sektorer samt unionens entiteter[37], förbättrar digitala produkters säkerhet (cyberresiliensförordningen) och inrättar en ram för stöd för beredskap och incidenthantering (cybersolidaritetsakten). I januari 2025 antog kommissionen den **europeiska handlingsplanen för cybersäkerhet för sjukhus och vårdgivare**[38] för att förbättra upptäckten av hot, beredskapen och krishanteringen. Det är avgörande att den genomförs fullt ut. För att hantera nya hot och nya skeenden måste vi samtidigt intensifiera våra åtgärder, särskilt när det gäller informationsutbyte, säkerheten i leveranskedjan, utpressningsprogram och cyberattacker samt teknisk suveränitet.

Dessutom kräver genomförandet att den nuvarande kompetensbristen på cybersäkerhetsområdet, som motsvarar 299 000 personer, minskas. Kommissionen kommer att samarbeta med medlemsstaterna inom ramen för kompetensunionen[39] för att utöka arbetsstyrkan inom cybersäkerhet, särskilt genom att använda den nya EU-akademin för cyberkompetens. Den strategiska planen för utbildning inom naturvetenskap, teknik, ingenjörsvetenskap och matematik[40] bidrar till att förbättra talangkedjan och hur EU tillgodoser behoven på arbetsmarknaden inom cybersäkerhet.

---

[34] EU:s strategiska kompass för säkerhet och försvar 2022, s. 22.
[35] EU:s säkerhetsskyddsrådgivare, Europeiska nätverket för ammunitionsröjning (EEODN), Atlasnätverket, EU:s högrisknätverk, den rådgivande gruppen för CBRN-säkerhet, gruppen för kritiska entiteters motståndskraft.
[36] JOIN(2025) 9 final.
[37] Europaparlamentets och rådets förordning (EU, Euratom) 2023/2841 av den 13 december 2023 om åtgärder för en hög gemensam cybersäkerhetsnivå vid unionens institutioner, organ och byråer, EUT L, 2023/2841, 18.12.2023.
[38] https://digital-strategy.ec.europa.eu/sv/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers.
[39] COM(2025) 90 final.
[40] COM(2025) 89 final.

Parallellt med att stärka sin resiliens kommer EU att fortsätta att fullt ut utnyttja **verktygslådan för cyberdiplomati** för att förebygga, avskräcka från och hantera cyberhot som härrör från statliga och icke-statliga aktörer.

Säkerhet i IKT-leveranskedjorna

Verktygslådan för 5G-cybersäkerhet utgör den relevanta ramen för att skydda 5G-näten, men genomförs för närvarande inte i tillräcklig utsträckning av medlemsstaterna. Oacceptabla säkerhetsrisker kvarstår, särskilt när det gäller att byta ut högriskleverantörer. En harmoniserad strategi för säkerheten i IKT-leveranskedjan kan ta itu med den nuvarande fragmenteringen av den inre marknaden på grund av olika strategier på nationell nivå, undvika kritiska beroendeförhållanden och minska de risker för våra IKT-leveranskedjor som högriskleverantörer medför och på detta sätt säkra vår kritiska infrastruktur.

I linje med denna strategi kommer kommissionen i den kommande **översynen av cybersäkerhetsakten** att titta mer allmänt på säkerheten och resiliensen hos IKT-leveranskedjor och IKT-infrastruktur. Dessutom kommer kommissionen att föreslå en förbättring av det **europeiska ramverket för cybersäkerhetscertifiering** så att framtida certifieringssystem kan antas i tid och tillgodose politiska behov.

Med utgångspunkt i befintliga eller pågående sektorsbedömningar[41] kommer kommissionen tillsammans med medlemsstaterna att utarbeta en **strategisk planering för samordnade bedömningar av cybersäkerhetsrisker**.

Molntjänster och telekommunikationstjänster har blivit en hörnsten i leveranskedjorna för kritisk infrastruktur, företag och offentliga myndigheter. Kommissionen kommer att vidta åtgärder för att uppmuntra kritiska entiteter att välja **moln- och telekommunikationstjänster med en lämplig cybersäkerhetsnivå**, med beaktande av inte bara tekniska risker utan även strategiska risker och beroendeförhållanden.

Utpressningsprogram och cyberattacker

Utpressningsprogram är fortfarande ett stort och ihållande problem i EU och globalt. I en rapport uppskattas den globala årliga kostnaden uppgå till över 250 miljarder euro fram till 2031[42]. Både **NIS 2-direktivet** och **cyberresiliensförordningen** kommer att avsevärt förbättra entiteternas säkerhet, vilket gör det dyrare för utpressningsnätverk att utföra sina attacker. Dessutom kommer kommissionen att ha ett nära samarbete med medlemsstaterna för att se till att fler attacker med utpressningsprogram, särskilt avancerade ständiga hot, och betalning av lösensummor rapporteras till brottsbekämpande myndigheter, vilket underlättar utredningar.

För att förebygga och stoppa cyberattacker måste EU stärka informationsutbytet mellan brottsbekämpande myndigheter, cybersäkerhetsmyndigheter och cybersäkerhetsentiteter samt privata parter, under ledning av Europol och Europeiska unionens cybersäkerhetsbyrå (Enisa).

Europol och Eurojust bör fortsätta att bygga vidare på de framsteg de har gjort när det gäller att sätta stopp för utpressningsattacker och stödja samarbetet mellan brottsbekämpande myndigheter. I detta syfte bör brottsbekämpande myndigheter maximera användningen av samarbetsmekanismer, inbegripet **Europols internationella modell för hantering av utpressningsprogram** och det **internationella initiativet för att motverka**

[41] Exempelvis vad gäller 5G-nät, telekommunikation, el, förnybar energi och uppkopplade fordon.

[42] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

utpressningsprogram[43], och Enisa och Europol bör samarbeta för att utöka antalet dekrypteringsverktyg för olika typer av utpressningsprogram[44].

Teknisk suveränitet

Cybersäkerhet och teknisk suveränitet är nära sammankopplade, och tekniska beroenden måste hanteras som en prioriterad fråga. Unionen måste **styra utvecklingen och spridningen av ny teknik**, och kommissionen måste sträva efter att **förbättra kapaciteten inom strategisk teknik** såsom AI, kvantteknik, avancerad konnektivitet, molnteknik, kantdatorteknik och sakernas internet[45], genom kommande initiativ såsom handlingsplanen för en AI-kontinent, kvantstrategin med flera[46]. Kommissionen kommer att fortsätta att stödja ett snabbt införande av de senast tillgängliga internationellt överenskomna **internetprotokoll** som är nödvändiga för att upprätthålla ett skalbart och effektivt internet med en högre cybersäkerhetsnivå. Det krävs även ytterligare åtgärder för att ta itu med **radiospektrumproblem**, t.ex. när det gäller GNSS-spoofing, störning, risker och beroenden i leveranskedjan, såsom användning av kvantdetektionsteknik och undersökning av utveckling av kapaciteten för radiofrekvensövervakning.

Lösningar för **postkvantkryptografi** kommer att vara avgörande för att skydda känslig kommunikation, data i vila och digitala identiteter i den nya kvanteran. På grundval av 2024 års rekommendation om en samordnad färdplan för genomförandet av övergången till postkvantkryptografi[47] strävar kommissionen och medlemsstaterna efter att främja denna övergång. I detta avseende bör medlemsstaterna kartlägga högriskfall i kritiska entiteter och säkerställa kvantsäker kryptering för dessa högriskfall så snart som möjligt och senast i slutet av 2030. Kommissionen samarbetar också med medlemsstaterna och Europeiska rymdorganisationen (ESA) för att utveckla och bygga ut den **europeiska kvantkommunikationsinfrastrukturen (EuroQCI)**[48] som bygger på kvantnyckeldistribution, som en del av **IRIS²**, unionens program för säker konnektivitet. Båda initiativen kommer i slutändan att göra det möjligt för entiteter att överföra uppgifter och lagra information på ett säkert sätt.

Kvantteknik kommer också att spela en nyckelroll i säkerhetstillämpningar: en **färdplan för kvantdetektion i säkerhetstillämpningar** kommer att utvecklas som en del av **kvantstrategin**. I samma anda strävar kommissionen efter att kvantsäkra sina system som är kritiska för företags säkerhet, däribland säkerhetsskyddsklassificerade it-system.

En företagsvänlig cybersäkerhetsram

Den kommande översynen av cybersäkerhetsakten utgör ett tillfälle att **förenkla EU:s cybersäkerhetslagstiftning**, i linje med konkurrenskraftskompassen. Kommissionen kommer att samarbeta nära med medlemsstaterna för att säkerställa ett snabbt, enhetligt och företagsvänligt genomförande av den övergripande cybersäkerhetsram som fastställs i NIS 2-direktivet, cyberresiliensförordningen och cybersolidaritetsakten, främja enkelhet och samstämmighet och undvika fragmentering eller dubblering av cybersäkerhetsregler i EU-lagstiftningen och nationell lagstiftning.

[43] https://counter-ransomware.org/.
[44] Tillgängliga via projektet No More Ransom, https://www.nomoreransom.org/sv/index.html.
[45] https://strategic-technologies.europa.eu/about_en#step-scope.
[46] T.ex. det gemensamma företaget EuropHPC https://eurohpc-ju.europa.eu/index_en, kvantflaggskeppet (Quantum Flagship) – Hemsida för Quantum Flagship | Kvantflaggskeppet, 3C-näten (COM(2024) 81 final) och EU:s handlingsplan för kabelsäkerhet (JOIN(2025) 9 final).
[47] Rekommendation om en samordnad färdplan för genomförandet av övergången till postkvantkryptografi | Shaping Europe's digital future.
[48] https://digital-strategy.ec.europa.eu/sv/policies/european-quantum-communication-infrastructure-euroqci.

För att möjliggöra säker tillgång till onlinetjänster och stärka den digitala säkerheten i hela EU kommer det **europeiska ramverket för digital identitet** att erbjuda alla medborgare och invånare i EU tillförlitliga digitala identitetsplånböcker före utgången av 2026. Den kommande **europeiska företagsplånboken** kommer att underlätta säker gränsöverskridande samverkan mellan företag och offentliga förvaltningar. Båda är förutsättningar för en säker och mer effektivt fungerande datadriven inre marknad med verktyg som den gemensamma digitala ingången, e-fakturering, e-upphandling och det digitala produktpasset.

Säkerhet på nätet

Några av de allvarligaste hybridhoten, som äventyrar människors skydd och säkerhet i Europa och riktar sig mot EU:s demokratiska sfär, äger rum online. Dessa hot omfattar olaglig verksamhet och olagligt innehåll online, informationsmanipulering som inbegriper förstärkning på konstgjord väg, vilseledande information och utländsk informationsmanipulering och inblandning.

En strikt tillämpning av **förordningen om digitala tjänster** är av största vikt för att säkerställa en säker och tillgänglig onlinemiljö med ansvarsskyldiga aktörer som också är motståndskraftiga mot hybridhot. Enligt förordningen om digitala tjänster är leverantörer av mycket stora onlineplattformar och av mycket stora onlinesökmotorer skyldiga att genomföra riskbedömningar och vidta riskreducerande åtgärder för systemrisker som härrör från deras tjänsters utformning, funktion eller användning. Sådana risker kan omfatta negativa effekter på det offentliga samtalet och på valprocesser samt på den allmänna säkerheten, exempelvis långtgående inblandning av illasinnade utländska statliga aktörer, till exempel i valprocesser. Det är viktigt att utbilda medlemsstaternas behöriga myndigheter i användningen av rättsliga verktyg för att snabbt avlägsna olagligt innehåll online, särskilt när det gäller könsrelaterat nätvåld. I förordningen om digitala tjänster föreskrivs en krishanteringsmekanism som kan aktiveras om extraordinära omständigheter leder till ett allvarligt hot mot den allmänna säkerheten eller folkhälsan i unionen eller i betydande delar av den. För att komplettera denna mekanism har kommissionen och de nationella behöriga myndigheter som utsetts till samordnare för digitala tjänster också utvecklat en frivillig **ram för incidenthantering enligt förordningen om digitala tjänster**. Samordnarna för digitala tjänster har också vidtagit åtgärder för att bidra till att skydda integriteten i samband med val, till exempel genom att anordna rundabordssamtal om val samt stresstester[49]. Tillsammans med förordningen om politisk reklam[50] tillhandahåller förordningen om digitala tjänster en av flera delar som är kopplade till skyddet av demokratin och integriteten hos den demokratiska processen, som är sårbara för attacker av fientliga aktörer, bland annat med hjälp av digitala verktyg och på sociala medier.

Genomförandet av verktygslådan för hantering av **utländsk informationsmanipulering och inblandning** är en annan viktig komponent som erbjuder betydande stöd på EU-nivå. Stöd till digital kompetens och mediekunnighet och kritiskt tänkande är också centralt för dessa insatser[51].

Motverkande av att migration används som vapen

Ryssland har, med hjälp och beslutsamt stöd av Belarus, avsiktligt använt migration som vapen och olagligen främjat migrationsströmmar till EU:s yttre gränser i syfte att destabilisera våra samhällen och undergräva Europeiska unionens enighet. Detta äventyrar inte bara

[49] *DSA Elections Toolkit for Digital Services Coordinators 2025* https://digital-strategy.ec.europa.eu/sv/library/dsa-elections-toolkit-digital-services-coordinators.

[50] Europaparlamentets och rådets förordning (EU) 2024/900 av den 13 mars 2024 om transparens och inriktning när det gäller politisk reklam, EUT L, 2024/900, 20.3.2024.

[51] Handlingsplanen för digital utbildning (2021–2027) – Det europeiska utbildningsområdet.

medlemsstaternas nationella säkerhet och suveränitet utan även Schengenområdets säkerhet och integritet och säkerheten i unionen som helhet. I sina slutsatser från oktober 2024 betonade Europeiska rådet att varken Ryssland och Belarus eller något annat land får tillåtas att missbruka våra värden, inklusive asylrätten, eller att undergräva vår demokrati.

Såsom anges i kommissionens meddelande från 2024 om användning av migration som vapen har unionen, utöver att tillhandahålla starkt politiskt stöd, vidtagit finansiella, operativa och diplomatiska åtgärder, inbegripet samarbete med ursprungs- och transitländerna, för att effektivt hantera dessa hot[52]. Dessa svarsåtgärder inbegriper att använda den nya ram som inrättats av rådet för att bestraffa personer och organisationer som deltar i handlingar eller politik såsom Rysslands användning av migration som vapen genom att frysa tillgångar och införa reseförbud[53]. EU kommer att fortsätta att använda denna ram vid behov och stödja medlemsstaterna i arbetet med att motverka detta hot.

Transportsäkerhet

Kusthamnar, flygplatser och landinfrastruktur är viktiga införsel- och utförselställen. De spelar en mycket viktig roll för EU:s ekonomi och samhälle och är avgörande för den militära rörligheten. Dessa transportnav och transportmedel är dock också de främsta målen för externa hot och brottslig verksamhet. Den senaste tidens incidenter, bland annat brott mot fraktsäkerheten inom luftfarten och attacker mot järnvägsinfrastruktur, belyser de allvarliga riskerna. **Transportföretag** kan vara både måltavlor och instrument för fientliga aktörer. EU:s befintliga rättsliga instrument har förbättrat luftfartsskyddet[54], men den höga hotnivån mot den civila luftfarten kräver ett sätt att förutse incidenter och snabbt samråda med berörda medlemsstater. Kommissionen kommer att samarbeta med medlemsstaterna för att ändra befintlig genomförandelagstiftning på luftfartsskyddsområdet för utbyte av säkerhetsskyddsklassificerade uppgifter om **incidenter som rör luftfartsskydd**. Dessutom kommer kommissionen att överväga **lagstiftningsåtgärder** för att hantera nya hot som exempelvis **flygfraktsincidenter** och för att stärka standarderna för luftfartsskydd. Detta kommer också att innebära en förstärkning av **lagstiftningen om luftfartsskydd** för att möjliggöra omedelbara svarsåtgärder samtidigt som området med en enda säkerhetskontroll på EU:s flygplatser bibehålls.

Vid utarbetandet av den kommande **europeiska hamnstrategin**, som bygger på den **europeiska hamnalliansen**, kommer kommissionen att undersöka olika sätt att ytterligare stärka lagstiftningen om sjöfartsskydd för att effektivt hantera framväxande hot, säkra hamnar och förbättra säkerheten i EU:s leveranskedjor. I detta syfte kommer kommissionen att se till att den genomförs på ett kraftfullt sätt och sträva efter att harmonisera nationell praxis och stärka säkerhetskontrollerna i hamnar. Utöver säkerhetsprotokollen för flygfrakt kommer kommissionen att samarbeta med medlemsstaterna och den privata sektorn för att utvidga dessa protokoll för att säkra sjötransportkedjorna.

EU:s föreslagna tullbyrå kommer att analysera och bedöma risker på grundval av **tullinformation** om varor som förs in i och ut ur samt transiteras genom EU för att hjälpa medlemsstaterna att förhindra att illvilliga aktörer utnyttjar internationella leveranskedjor. I linje med EU:s strategi för sjöfartsskydd[55] kommer den förestående **europeiska världshavspakten** att spela en nyckelroll för att stärka sjöfartsskyddet i havsområden runt om

[52] COM(2024) 570 final.
[53] Rådets förordning (EU) 2024/2642 av den 8 oktober 2024 om restriktiva åtgärder med anledning av Rysslands destabiliserande verksamhet, ST/8744/2024/INIT, EUT L, 2024/2642, 9.10.2024.
[54] Europaparlamentets och rådets förordning (EG) nr 300/2008 av den 11 mars 2008 om gemensamma skyddsregler för den civila luftfarten, EUT L 97, 9.4.2008, s. 72.
[55] JOIN(2023) 8 final.

i och utanför EU, bland annat genom att uppmuntra till ökade multifunktionella maritima insatser och övningar.

Resiliens i leveranskedjorna

Europa måste minska sitt beroende av teknik från tredjeländer, som kan leda till beroende- och säkerhetsrisker. Kommissionen strävar efter att minska beroendet av enskilda utländska leverantörer, minska de risker för våra leveranskedjor som högriskleverantörer medför och säkra kritisk infrastruktur och den industriella kapaciteten på EU:s territorium i enlighet med **konkurrenskraftskompassen**[56] och **given för en ren industri**[57]. Kommissionen kommer att främja en **industripolitik för inre säkerhet** genom att samarbeta med EU:s industrier inom viktiga sektorer (t.ex. transportknutpunkter, kritisk infrastruktur) för att ta fram säkerhetslösningar som exempelvis detektionsutrustning, biometrisk teknik och drönare, som införlivar funktioner för inbyggd säkerhet. När kommissionen **ser över EU:s upphandlingsregler** kommer den att bedöma om säkerhetsövervägandena i 2009 års direktiv om upphandling på försvars- och säkerhetsområdet[58] är tillräckliga för att tillgodose brottsbekämpande myndigheters och kritiska entiteters behov av resiliens.

Kommissionen kommer att stödja medlemsstaterna i **granskningen av utländska direktinvesteringar** och upphandling av utrustning för logistiknav för att säkerställa att kritisk infrastruktur och teknik förblir säker.

När **förordningen om krissituationer och resiliens på den inre marknaden** har börjat tillämpas kommer den att hjälpa EU att hantera kriser som stör kritiska leveranskedjor och den fria rörligheten för varor, tjänster och människor. Den kommer att möjliggöra en snabb krissamordning och identifiering av krisnödvändiga varor och tjänster och kommer att tillhandahålla en verktygslåda för att säkerställa att de finns tillgängliga. Vidare kommer kommissionen, i nära samarbete med medlemsstaterna, att föreslå att det inrättas **en beredskapsmekanism för transport- och leveranskedjan som omfattar flera organ** för att garantera ett säkert och snabbt utbyte av relevant information som är nödvändig för att förutse och motverka hot.

I och med genomförandet av förordningen om kritiska råvaror och förordningen om nettonollindustrin kommer dessutom ökad användning av kriterier för hållbarhet, resiliens och europeiskt företräde i EU:s offentliga upphandlingar att främja utvecklingen av pionjärmarknader. Stärkta handelsförbindelser, till exempel genom partnerskap om råvaror och partnerskap för ren handel och rena investeringar, kommer att bidra till att diversifiera leveranskedjorna.

Resiliens mot och beredskap för kemiska, biologiska, radiologiska och nukleära hot

Rysslands anfallskrig mot Ukraina har ökat risken för **kemiska, biologiska, radiologiska och nukleära (CBRN) hot**. För att ta itu med det potentiella förvärvet av CBRN-material och användningen av dessa som vapen kommer kommissionen att stödja medlemsstaterna och partnerländerna genom särskild utbildning och särskilda övningar. Kommissionen kommer också att stärka beredskaps- och insatskapaciteten på CBRN-området, med prioritering av hot, innovationsfinansiering för motåtgärder, rescEU-beredskapslager och medicinsk lagerhållning, inom ramen för en ny **handlingsplan för beredskap och insatser på CBRN-området**.

[56] COM(2025) 30 final.
[57] COM(2025) 85 final.
[58] Direktiv 2009/81/EG om samordning av förfarandena vid tilldelning av vissa kontrakt för byggentreprenader, varor och tjänster av upphandlande myndigheter och enheter på försvars- och säkerhetsområdet, EUT L 216, 20.8.2009.

Dessutom kommer **EU:s strategi för medicinska motåtgärder** att stödja utvecklingen av medicinska motåtgärder från forskning till tillverkning och distribution för att skydda EU mot pandemier och CBRN-hot.

Med utgångspunkt i erfarenheterna från covid-19-pandemin har EU stärkt ramen för hälsosäkerhet[59]. Kommissionen utser EU-referenslaboratorier inom folkhälsa för att stärka EU:s kapacitet och den nationella kapaciteten för övervakning och snabb upptäckt. En unionsplan för beredskap, förebyggande och insatser för hälsosäkerhet kommer att offentliggöras 2025.

Nyckelåtgärder

Kommissionen kommer att

- **se över och revidera cybersäkerhetsakten under 2025,**
- **utveckla åtgärder för att säkerställa en cybersäker användning av molntjänster,**
- **föreslå en europeisk hamnstrategi under 2025,**
- **se över EU:s upphandlingsregler för försvar och säkerhet under 2026,**
- **och presentera en ny handlingsplan för beredskap och insatser på CBRN-området under 2026.**

Dessutom kommer kommissionen att tillsammans med medlemsstaterna

- **utveckla och bygga ut den europeiska kvantkommunikationsinfrastrukturen (EuroQCI),**
- **säkerställa en effektiv tillämpning av förordningen om digitala tjänster,**
- **sträva efter att motverka att migration används som vapen,**
- **upprätta ett system för incidenter som rör luftfartsskydd,**
- **och sträva efter att inrätta en beredskapsmekanism i transport- och leveranskedjan som omfattar flera organ.**

Rådet uppmanas att

- **anta rådets rekommendation om EU:s cyberplan.**

Medlemsstaterna uppmanas att

- **införliva och fullt ut genomföra CER- och NIS 2-direktiven.**

5. Begränsa handlingsutrymmet för den grova och organiserade brottsligheten

Vi kommer att bidra till att utrota den organiserade brottsligheten genom att föreslå strängare regler för att bekämpa brottsorganisationer, bland annat vad gäller utredningar, göra unga i EU mindre sårbara för rekrytering till brottslighet och trappa upp insatserna för att strypa tillgången till kriminella verktyg och vinning av brott.

Den organiserade brottsligheten utnyttjar en föränderlig miljö och sprider sig exponentiellt. Den gynnas av avancerad teknik, är aktiv i flera jurisdiktioner och har starka förbindelser utanför EU:s gränser. Med tanke på dessa komplexa, gränsöverskridande hot är samordning och stöd på EU-nivå avgörande.

Förebyggande av brottslighet

Rekryteringen av ungdomar till organiserad brottslighet är ett växande problem i EU. Kampen mot den organiserade brottsligheten kräver att man tar itu med dess **grundorsaker** genom att

[59] Särskilt genom förordning (EU) 2022/2371 om allvarliga gränsöverskridande hot mot människors hälsa.

erbjuda utbildning och ett alternativ till ett liv i kriminalitet genom en strategi som omfattar hela samhället. Kommissionen kommer att stödja integreringen av säkerhetsöverväganden i EU:s utbildnings-, social-, sysselsättnings- och regionalpolitik. EU kommer att **främja evidensbaserade brottsförebyggande strategier**[60] som är anpassade till lokala förhållanden.

För att skydda dem som använder sig av onlinetjänster, särskilt minderåriga, mot bland annat personer som begår sexuella övergrepp mot barn eller mot människohandlare, och mot onlinerekrytering till brott eller våldsbejakande extremism, kräver åtgärder enligt **förordningen om digitala tjänster** att leverantörer av onlineplattformar som är tillgängliga för minderåriga hanterar risker och vidtar åtgärder mot olagligt innehåll, bland annat hatpropaganda. Kommissionen planerar att utfärda **riktlinjer för skydd av minderåriga** för att hjälpa leverantörer av onlineplattformar att säkerställa en hög nivå av integritet, säkerhet och trygghet för minderåriga på nätet. Riktlinjerna kommer att innehålla en uppsättning rekommendationer för alla digitala tjänster som tillhandahålls i unionen för att förbättra skyddet av minderåriga på nätet. Under 2025 planerar kommissionen också att underlätta en EU-lösning för **ålderskontroll som skyddar den personliga integriteten**, som kommer att fylla tomrummet innan den europeiska digitala identitetsplånboken lanseras slutet av 2026. Kommissionen kommer också att lägga fram en handlingsplan mot nätmobbning.

Dessutom kommer kommissionen att fortsätta att stödja ett frivilligt flerpartssamarbete med onlineplattformar och andra relevanta aktörer, bland annat genom EU:s internetforum och riktade uppförandekoder inom ramen för förordningen om digitala tjänster, såsom 2025 års uppförandekod för att motverka olaglig hatpropaganda på nätet. Målet är att öka medvetenheten, gemensamt reagera på aktuella och framväxande hot och ta fram och utbyta god praxis för begränsningsåtgärder.

På lokal nivå understryker den organiserade brottslighetens inverkan behovet av regionala lösningar för att minska sårbarheten och attraktionskraften hos olaglig verksamhet. EU:s agenda för städer kommer att ta itu med säkerhetsproblem i städer, med utgångspunkt i initiativet EU-städer mot radikalisering. Kommissionen kommer att stödja medlemsstaterna i arbetet med att förbättra säkerheten i städer och regioner genom Europeiska regionala utvecklingsfonden**.**

En starkare utbildningsgrund och kompetens ligger till grund för resilienta och sammanhållna samhällen. Unionen kommer genom **kompetensunionen** och **handlingsplanen för integration och inkludering** att sträva efter att hjälpa människor att bättre kunna motstå felaktig information och desinformation, radikalisering och rekrytering till brottslighet.

Ett centralt mål för EU är att skydda barn från alla former av våld, inbegripet brott samt fysiskt eller psykiskt våld, såväl online som offline. För att ta itu med de särskilda behoven hos särskilt utsatta grupper som exempelvis barn, som i allt högre grad exponeras för rekrytering och radikalisering, gromning och sexuella övergrepp, nätmobbning, desinformation och andra hot, kommer EU att utarbeta en **handlingsplan för skydd av barn mot brottslighet**, som ska täcka såväl det fysiska som det digitala rummet. Den kommer att innehålla en enhetlig och samordnad strategi som bygger på tillgängliga ramar och verktyg, inbegripet det framtida EU-centrumet mot sexuella övergrepp mot barn, och andra EU-organ och EU-byråer, och föreslå vägar framåt där det fortfarande kvarstår tomrum.

Upplösning av kriminella nätverk och deras medhjälpare

Kampen mot kriminella högrisknätverk, deras ledare och medhjälpare måste intensifieras. Även om den senaste tidens framgångar är betydande[61] utgör föråldrade regler och inkonsekventa

[60] https://www.eucpn.org/.
[61] Inbegripet de senaste Empact-ärendena.

definitioner av kriminella nätverk ett hinder för ändamålsenliga straffrättsliga åtgärder och gränsöverskridande samarbete. Kommissionen kommer att se över den föråldrade lagstiftningen på detta område och föreslå en förnyad **rättslig ram för organiserad brottslighet** för att stärka dessa åtgärder.

Administrativ verkställighet kan komplettera brottsbekämpningen för snabbare resultat, vilket Eppo och Europeiska byrån för bedrägeribekämpning (Olaf) har visat när det gäller att hantera **gränsöverskridande bedrägerier och brott mot EU:s ekonomiska intressen**. Bidragsfuskare fokuserar på sektorer som exempelvis förnybar energi, forskningsprogram och jordbrukssektorn[62]. Kommissionen kommer att undersöka olika sätt att samordna användningen av straffrättsliga och administrativa verktyg och stärka samarbetet med Europol, Eurojust och Eppo. Kommissionen kommer också att fortsätta att stödja en bredare tillämpning av **den administrativa strategin** för att ge lokala och andra administrativa myndigheter möjlighet att störa kriminell infiltration[63].

EU strävar efter att stärka sin rättsliga ram för bekämpning av **korruption**[64]. Europaparlamentet och rådet bör skyndsamt slutföra förhandlingarna om den uppdaterade ram för korruptionsbekämpning som föreslagits av kommissionen. Kommissionen kommer att lägga fram en EU-strategi mot korruption för att främja integriteten och stärka samordningen mellan alla berörda myndigheter och parter på detta område.

Skjutvapen är en grundförutsättning för organiserade kriminella gruppers ökade våld. Kommissionen kommer att föreslå gemensamma straffrättsliga normer för olaglig handel med skjutvapen. **EU:s nya handlingsplan mot olaglig handel med skjutvapen** kommer att inriktas på att skydda den lagliga marknaden och begränsa den brottsliga verksamheten med utgångspunkt i bättre underrättelser samt på att öka det internationella samarbetet, med särskilt fokus på Ukraina och västra Balkan.

Olagligt handlad pyroteknik som används vid brott kräver åtgärder för att förbättra förebyggandet och spårbarheten. Kommissionen håller för närvarande på att utvärdera direktivet om pyrotekniska artiklar och kommer också att överväga **straffrättsliga påföljder för olaglig handel med pyrotekniska artiklar**.

Följ pengarna

Att **följa pengarna** är avgörande för att bekämpa organiserad brottslighet och terrorism, men det är fortfarande mycket svårt. Kopplingen mellan organiserad brottslighet och penningflöden kräver intensiva och kombinerade insatser för att stoppa kriminella nätverks tillgång till finansieringskällor och bättre skydda människor, företag och offentliga budgetar.

EU har intensifierat sina ansträngningar genom de nya reglerna för bekämpning av penningtvätt, inbegripet inrättandet av **EU:s myndighet för bekämpning av penningtvätt och finansiering av terrorism (Amla)**[65]. Samarbete mellan Amla, Olaf, Eppo, Eurojust och Europol är avgörande för att genomföra effektiva finansiella utredningar. Kommissionen

[62] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

[63] https://administrativeapproach.eu/sites/default/files/page/files/eu-jha-council-9-10-june-conclusions-administrative-approach-org-crime.pdf.

[64] Förslag till Europaparlamentets och rådets direktiv om bekämpande av korruption, om ersättande av rådets rambeslut 2003/568/RIF och konventionen om kamp mot korruption som tjänstemän i Europeiska gemenskaperna eller Europeiska unionens medlemsstater är delaktiga i och om ändring av Europaparlamentets och rådets direktiv (EU) 2017/1371, COM(2023) 234 final, Bryssel, 3.5.2023.

[65] https://www.amla.europa.eu/index_sv.

kommer att stödja inrättandet av **partnerskap**, både sådana som underlättar samarbete mellan olika organ och sådana som involverar den privata sektorn.

För att omintetgöra de ekonomiska motiv som ligger bakom den organiserade brottsligheten är det viktigt att beslagta tillgångar och förverka vinning av brott. De nyligen antagna skärpta reglerna om **återvinning och förverkande av tillgångar**[66] bör införlivas av medlemsstaterna utan dröjsmål och utnyttjas fullt ut. För att bekämpa parallella finansiella system som kringgår EU:s ram för bekämpning av penningtvätt, inbegripet kryptobaserade system, krävs också innovativa åtgärder, utbyte av bästa praxis mellan medlemsstaterna och ökat stöd från Europol och Eurojust. Kommissionen kommer att undersöka genomförbarheten av ett nytt EU-omfattande system för att spåra vinning från organiserad brottslighet och finansiering av terrorism, och även uppmuntra snabba och utökade informationsflöden från **finansunderrättelseenheter** till brottsbekämpande myndigheter. Kommissionen kommer att undersöka olika sätt att täppa till kryphål och stödja medlemsstaternas kapacitetsuppbyggnad och kommer att fortsätta stärka samarbetet med tredjeländer som utnyttjas av brottslingar för illegal bankverksamhet.

Bekämpning av allvarliga brott

Förutom att upplösa kriminella nätverk krävs riktade insatser för att bekämpa allvarliga brott. För att stärka vår förmåga att bekämpa **internetbedrägerier** – som orsakar mycket stor ekonomisk skada[67] – kommer kommissionen att stödja förebyggande åtgärder och effektivare brottsbekämpande åtgärder och samarbeta med medlemsstaterna och berörda parter för att stödja och skydda offren, bland annat genom att hjälpa dem att få tillbaka sina pengar. Dessa insatser kommer att formaliseras i en **handlingsplan mot internetbedrägerier**.

Med utgångspunkt i EU:s strategi för bekämpande av **sexuella övergrepp mot barn**[68] 2020–2025 kommer kommissionen att stödja medlagstiftarna i arbetet med att slutföra de två lagstiftningsförslagen[69] för att förebygga och bekämpa sexuella övergrepp mot barn på nätet och göra de brottsbekämpande åtgärderna mot sexuella övergrepp mot barn och sexuellt utnyttjande av barn effektivare. I och med de tillfälliga regler som gäller fram till april 2026 är det viktigt att inrätta en permanent rättslig ram, och kommissionen uppmanar medlagstiftarna att inleda förhandlingar om utkastet till förordning om fastställande av regler för att förebygga och bekämpa sexuella övergrepp mot barn. Medlagstiftarna uppmanas också att gå vidare mot förhandlingar om direktivet om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och material med sexuella övergrepp mot barn, som kommer att fastställa minimiregler om fastställande av brottsrekvisit och påföljder på området sexuell exploatering av barn.

Hälften av EU:s farligaste kriminella nätverk är inblandade i våldsam **olaglig narkotikahandel**. Även om EU nyligen har stärkt sin kamp mot denna brottslighet[70], särskilt genom att utvidga mandatet för **Europeiska unionens narkotikamyndighet**, krävs ytterligare åtgärder. Kommissionen kommer att ha ett nära samarbete med medlemsstaterna för att föreslå en ny **narkotikastrategi för EU**. Den kommer också att se över den **rättsliga ramen för narkotikaprekursorer** och föreslå en **europeisk handlingsplan mot narkotikahandel** för att störa smugglingsvägar och affärsmodeller**.** Det **offentlig-privata partnerskapet inom ramen för den europeiska hamnalliansen** om stärkt hamnskydd kommer att utvidgas till att omfatta

[66] Europaparlamentets och rådets direktiv (EU) 2024/1260 av den 24 april 2024 om återvinning av tillgångar och förverkande, EUT L, 2024/1260, 2.5.2024.
[67] Global Anti-Scam Report 2024.
[68] COM(2020) 607 final
[69] COM(2022) 209 final och COM(2024) 60 final.
[70] COM(2023) 641 final.

mindre hamnar och inlandshamnar och säkerställa att reglerna om sjöfartsskydd efterlevs. Kommissionen är medveten om de allvarliga lokala konsekvenserna av narkotikahandeln och kommer att fortsätta att stödja en balanserad, evidensbaserad och tvärvetenskaplig narkotikapolitik med beredskap för plötsliga inflöden av narkotika, särskilt av syntetiska opioider.

För att bekämpa exploatering av människor har EU antagit nya regler[71] och kommer att införa en **förnyad EU-strategi mot människohandel** (2026–2030) som omfattar alla skeden från förebyggande till lagföring, med fokus på stöd till offer på både EU-nivå och internationell nivå.

I kampen mot **smuggling av migranter** kommer kommissionen att leda insatserna tillsammans med viktiga partner genom den nya globala alliansen mot smuggling av migranter, i samarbete med Europol, Eurojust och Frontex, även på nätet. Kommissionens förslag om bekämpning av smuggling av migranter[72] bör antas och genomföras utan dröjsmål. Dessutom har kommissionen, efter antagandet av **verktygslådan för transportföretag**[73], ökat de uppsökande kontakterna med utländska myndigheter och företag och kommer att fortsätta att samarbeta med luftfartsindustrin och civila luftfartsorganisationer[74] för att öka medvetenheten om smuggling av migranter med flyg[75].

Miljöbrott hotar miljön, folkhälsan och ekonomierna på lång sikt. Kommissionen kommer att stödja medlemsstaterna i genomförandet av miljöbrottsdirektivet[76] och stärka operativa nätverk och åtgärder på detta område[77]. Det är mycket viktigt med en sträng kontroll av efterlevnaden. Dessutom kommer Europarådets nyligen antagna konvention om straffrättsliga sanktioner till skydd för miljön[78] att bidra till att säkerställa kraftfulla och jämförbara insatser för att bekämpa miljöbrott, både i och utanför Europa.

Straffrättsliga åtgärder

Brottslighet och terrorism kan påverka alla, vilket gör det nödvändigt att stödja och skydda **brottsoffrens** rättigheter för att minska skadan och öka den övergripande säkerheten och förtroendet för myndigheterna. Med utgångspunkt i direktivet om brottsoffers rättigheter kommer kommissionen att införa en ny **EU-strategi för brottsoffers rättigheter**.

EU:s straffrättsliga system behöver effektiva verktyg för att hantera framväxande hot. För att uppnå detta har kommissionen lanserat ett **högnivåforum om framtiden för EU:s straffrätt**. Detta forum sammanför medlemsstaterna, Europaparlamentet, EU:s byråer och organ och andra berörda parter. Dess mål är att diskutera olika sätt att säkerställa att våra straffrättsliga system förblir effektiva, rättvisa och motståndskraftiga mot bakgrund av föränderliga utmaningar, samtidigt som det rättsliga samarbetet och det ömsesidiga förtroendet stärks, bland annat genom digitalisering[79].

---

[71] Direktiv (EU) 2024/1712 av den 13 juni 2024 om ändring av direktiv 2011/36/EU om förebyggande och bekämpande av människohandel och om skydd av dess offer, EUT L, 2024/1712, 24.6.2024.
[72] COM(2023) 755 final och COM(2023) 754 final.
[73] *Toolbox addressing the use of commercial means of transport to facilitate irregular migration to the EU*.
[74] Inbegripet Internationella civila luftfartsorganisationen (Icao).
[75] Kommissionen kommer också att stödja slutförandet av förordningen om åtgärder mot transportföretag som underlättar eller ägnar sig åt människohandel eller smuggling av migranter, COM(2021) 753 final.
[76] Europaparlamentets och rådets direktiv (EU) 2024/1203 av den 11 april 2024 om skydd för miljön genom straffrättsliga bestämmelser, EUT L, 2024/1203, 30.4.2024.
[77] EU:s nätverk för genomförande och upprätthållande av miljölagstiftningen (Impel), det europeiska nätverket för miljöåklagare, EnviCrimeNet och Europeiska unionens miljödomarförening.
[78] Expertkommittén för miljöskydd genom straffrättsliga bestämmelser – Europarådets kommitté för brottsfrågor.
[79] Särskilt genom inrättandet av e-Codex och det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister avseende tredjelandsmedborgare (Ecris-TCN).

Nyckelåtgärder

Kommissionen kommer att

- **lägga fram ett lagstiftningsförslag om moderniserade regler om organiserad brottslighet under 2026,**
- **lägga fram ett lagstiftningsförslag om översyn av den rättsliga ramen för narkotikaprekursorer under 2025,**
- **lägga fram ett lagstiftningsförslag om gemensamma straffrättsliga normer för olaglig handel med skjutvapen under 2025,**
- **bedöma behovet av att se över direktiven om pyrotekniska artiklar och om explosiva varor för civilt bruk,**
- **bedöma behovet av att ytterligare stärka den europeiska utredningsordern och den europeiska arresteringsordern,**
- **lägga fram en ny EU-strategi mot människohandel under 2026,**
- **lägga fram en ny EU-strategi för brottsoffers rättigheter under 2026,**
- **lägga fram en EU-handlingsplan för skydd av barn mot brottslighet senast 2027,**
- **lägga fram en europeisk handlingsplan mot narkotikahandel under 2025,**
- **lägga fram EU:s nya handlingsplan mot olaglig handel med skjutvapen under 2026,**
- **successivt utvidga den europeiska hamnalliansen från och med 2025,**
- **anta riktlinjer enligt förordningen om digitala tjänster för skydd av minderåriga under 2026**
- **och lägga fram en EU-handlingsplan mot nätmobbning under 2026.**

Medlemsstaterna uppmanas att

- **fullt ut införliva de nya reglerna om återvinning och förverkande av tillgångar senast i slutet av 2026 och utnyttja dem fullt ut,**
- **genomföra den administrativa strategin i kampen mot kriminell infiltration,**
- **inrätta offentlig-privata partnerskap mot penningtvätt**
- **och införliva och fullt ut genomföra direktivet för att förebygga och bekämpa våld mot kvinnor och våld i hemmet.**

Europaparlamentet och rådet uppmanas att

- **gå vidare mot förhandlingar om förordningen om fastställande av regler för att förebygga och bekämpa sexuella övergrepp mot barn och direktivet om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och material med sexuella övergrepp mot barn**
- **och slutföra förhandlingarna om direktivet om bekämpande av korruption.**

6. Bekämpande av terrorism och våldsbejakande extremism

Vi kommer att införa en övergripande agenda för terrorismbekämpning för att förebygga radikalisering, säkra onlinemiljöer och offentliga platser, strypa finansieringskanalerna och vidta svarsåtgärder vid eventuella attacker.

Terrorhotnivån i EU är fortsatt hög. Detta är nära kopplat till spridningseffekterna av geopolitiska händelser, ny teknik och nya metoder för finansiering av terrorism. Vi måste se till att EU är väl rustat att förutse hot, förebygga radikalisering (både offline och online), skydda allmänheten och offentliga platser mot attacker och effektivt vidta svarsåtgärder vid eventuella attacker. En **ny EU-agenda för att förebygga och bekämpa terrorism och våldsbejakande extremism** kommer att presenteras under 2025 för att fastställa EU:s kommande åtgärder. I

linje med den nya agendan kommer EU och västra Balkan att underteckna den nya **gemensamma handlingsplanen** för förebyggande och bekämpande av terrorism och våldsbejakande extremism under 2025.

Förebyggande av radikalisering och skydd av människor på nätet

I likhet med kampen mot organiserad brottslighet börjar kampen mot terrorism och våldsbejakande extremism med **att ta itu med dess grundorsaker**. **EU:s kunskapsnav om förebyggande av radikalisering** kommer att öka sitt stöd till yrkesverksamma och beslutsfattare med en ny **omfattande verktygslåda med förebyggande åtgärder** för att möjliggöra tidig identifiering och tidiga insatser som är inriktade på utsatta personer, särskilt minderåriga. Radikalisering sker ofta i fängelser och för att hjälpa medlemsstaterna att ta itu med detta problem kommer kommissionen att utfärda nya rekommendationer.

Terrorister och våldsbejakande extremister använder onlineplattformar för att sprida terrorisminnehåll och skadligt innehåll, samla in medel och rekrytera. Utsatta användare, särskilt minderåriga, radikaliseras på nätet i alarmerande takt. **Förordningen om terrorisminnehåll online** har varit avgörande för att motverka spridningen av terrorisminnehåll online och göra det möjligt att snabbt avlägsna det allra mest vidriga och farliga materialet[80]. Kommissionen håller för närvarande på att utvärdera hur den fungerar och kommer att bedöma hur denna ram bäst kan stärkas.

EU:s krisprotokoll för gemensamma och snabba insatser av brottsbekämpande myndigheter och teknikindustrin vid terrorattentat kommer att ändras för att säkerställa skalbarhet och flexibilitet för att hantera terrorattackernas växande onlinedimension. EU:s internetforum kommer även fortsättningsvis att vara den främsta vägen till frivilligt samarbete med teknikindustrin för att bekämpa terrorisminnehåll och skadligt innehåll på nätet. Dessutom deltar kommissionen i internationella initiativ såsom Christchurch Call Foundation och det globala internetforumet för terrorismbekämpning.

Bekämpning av finansiering av terrorism

Terrorister finansierar sin verksamhet med gräsrotsfinansieringskampanjer, kryptotillgångar, neobanker eller plattformar för internetbetalning. Brottsbekämpande myndigheter måste upptäcka och utreda dessa finansiella flöden. Detta kräver medel, verktyg och sakkunskap. **Nätverket av finansiella utredare med inriktning på terrorismbekämpning** spelar en viktig roll. Kommissionen kommer att undersöka möjligheten att skapa ett **nytt EU-omfattande system för att spåra finansiering av terrorism** som omfattar transaktioner inom EU och Sepa-transaktioner, överföringar av kryptotillgångar, internetbetalningar och elektroniska överföringar, som ett komplement till TFTP-avtalet mellan EU och USA.

EU:s budget måste **skyddas mot missbruk som syftar till att främja radikala/extremistiska åsikter** i medlemsstaterna. I den reviderade **budgetförordningen** ingår nu fällande dom för ”uppmaning till diskriminering, hat eller våld” som skäl för uteslutning från EU-finansiering. Kommissionen kommer att fortsätta att undersöka det bästa sättet att fullt ut utnyttja verktygslådan, även när den väljer ut potentiella stödmottagare. Skyddet av EU:s budget bygger också på ett starkt samarbete och informationsutbyte med nationella myndigheter, EU-byråer och EU-organ.

[80] Fram till den 31 december 2024 hade 1 426 avlägsnandeorder utfärdats för att avlägsna terrorisminnehåll eller spärra åtkomsten till detta, varav de allra flesta riktade sig mot jihadistiskt terrorisminnehåll men även mot högerextremt terrorisminnehåll.

Skydd mot attacker

Utöver investeringar i förebyggande av radikalisering är en viktig del av skyddet av allmänheten att begränsa möjligheterna för terrorister och kriminella att genomföra attacker. Det krävs åtgärder både när det gäller de verktyg som terrorister använder och för att skydda dem som riskerar att bli måltavlor för attacker.

Utöver åtgärder mot skjutvapen kommer kommissionen också att **se över reglerna** om **sprängämnesprekursorer** så att de även ska omfatta högriskkemikalier. **Offentliga platser** är fortfarande de vanligaste målen för terrorattacker, särskilt för ensamagerande. För att skydda allmänheten kommer **EU:s rådgivande säkerhetsskyddsprogram** att stärkas för att genomföra sårbarhetsanalyser av offentliga platser, kritisk infrastruktur och högriskevenemang på begäran av medlemsstaterna och med finansiering genom EU:s budget inom ramen för Fonden för inre säkerhet. EU kommer att sträva efter att öka den tillgängliga finansieringen för skydd av offentliga platser. Kommissionen erbjuder stöd till myndigheter och privata aktörer i medlemsstaterna genom särskild vägledning och särskilda verktyg, såsom kunskapsnavet om skydd av offentliga platser[81], och 70 miljoner euro har redan gjorts tillgängligt för skyddet av offentliga platser sedan 2020.

Kommissionen kommer också att undersöka möjligheten att införa krav på att organisationer ska överväga eller tillämpa säkerhetsåtgärder på allmänt tillgängliga platser genom att samarbeta med lokala myndigheter och privata partner.

Med tanke på de uppenbara sårbarheterna kommer **EU:s strategi för att bekämpa antisemitism och främja judiskt liv (2021–2030)** att fortsätta att vägleda kommissionens åtgärder för att skydda den judiska befolkningsgruppen. Kommissionen kommer också att se till att det finns lämpliga verktyg för att stödja medlemsstaterna i kampen mot **antimuslimskt hat**.

Användningen av **drönare** för spionage och attacker utgör ett allt större säkerhetsproblem. Kommissionen kommer att utveckla en **harmoniserad provningsmetod för system för drönarbekämpning**, inrätta ett **kompetenscentrum för drönarbekämpning** och bedöma behovet av att harmonisera medlemsstaternas lagar och förfaranden[82].

Utländska terroriststridande

För att identifiera utländska terroriststridande som återvänder eller reser in vid EU:s yttre gränser behövs uppgifter om personer som utgör ett terroristhot. I detta syfte kommer kommissionen, tillsammans med Europol, att stärka sitt **samarbete med viktiga tredjeländer för att erhålla personuppgifter och biometriska uppgifter om personer som kan utgöra ett terroristhot**, däribland utländska terroriststridande, som sedan kan föras in i Schengens informationssystem i full överensstämmelse med tillämpliga rättsliga ramar på EU-nivå och nationell nivå. Det är därför mycket viktigt att medlemsstaterna använder alla befintliga verktyg. Detta inbegriper införande av all relevant information i **Schengens informationssystem**, förbättrade biometriska kontroller och obligatoriska systematiska kontroller av alla personer vid EU:s yttre gränser[83]. Dessutom kommer de **gemensamma riskindikatorer** som tagits fram av Frontex att fortsätta att stödja medlemsstaternas gränskontrollmyndigheter när det gäller att identifiera och bedöma risken för misstänkta resor som görs av potentiella utländska terroriststridande.

[81] Kunskapsnavet om skydd av offentliga platser.
[82] Uppföljning av uppsättningen nyckelåtgärder i 2023 års meddelande om bekämpning av potentiella hot från drönare, COM(2023) 659 final.
[83] I full överensstämmelse med kodexen om Schengengränserna och screeningförordningen.

För att säkerställa att medlemsstaterna bibehåller tillgången till **bevis från slagfältet** som samlats in av FN:s utredningsgruppför att stödja irakiska myndigheter gällande ansvarsutkrävande av brott begångna av Daesh (Unitad) för lagföring av utländska terroriststridande kommer kommissionen, tillsammans med Eurojust, att bedöma möjligheten att lagra dessa bevis i Eurojusts databas över bevis för de allvarligaste internationella brotten. Dessutom kommer det nya **rättsliga terrorismbekämpningsregistret** att fortsätta att hjälpa medlemsstaternas rättsväsenden att snabbt identifiera gränsöverskridande kopplingar i terrorismärenden.

Nyckelåtgärder

Kommissionen kommer att

- **anta en ny EU-agenda för att förebygga och bekämpa terrorism och våldsbejakande extremism under 2025,**
- **underteckna en ny gemensam handlingsplan för förebyggande och bekämpande av terrorism och våldsbejakande extremism tillsammans med västra Balkan under 2025,**
- **utveckla en ny omfattande verktygslåda med förebyggande åtgärder tillsammans med EU:s kunskapsnav,**
- **utvärdera tillämpningen av förordningen om terrorisminnehåll online under 2026,**
- **ändra EU:s krisprotokoll under 2025,**
- **lägga fram ett lagstiftningsförslag om översyn av förordningen om saluföring och användning av sprängämnesprekursorer under 2026**
- **och undersöka genomförbarheten av ett nytt EU-omfattande system för att spåra finansiering av terrorism.**

Medlemsstaterna uppmanas att

- **förbättra de biometriska kontrollerna och genomföra obligatoriska systematiska kontroller vid EU:s yttre gränser**
- **och fullt ut använda det rättsliga terrorismbekämpningsregistret.**

7. EU som en stark global aktör inom säkerhet

För att öka EU:s säkerhet kommer vi att främja det operativa samarbetet genom partnerskap med viktiga regioner som exempelvis våra utvidgnings- och grannskapspartner, Latinamerika och Medelhavsområdet. EU:s säkerhetsintressen kommer att beaktas i det internationella samarbetet, bland annat genom att utnyttja EU:s verktyg och instrument.

De senaste åren har visat på de inneboende kopplingarna mellan EU:s yttre och inre säkerhet. Rysslands anfallskrig mot Ukraina, konflikten i Gaza, situationen i Syrien och uppblossande konflikter runt om i världen har haft allvarliga spridningseffekter på EU:s inre säkerhet. För att motverka den globala instabilitetens konsekvenser för EU:s inre säkerhet **måste unionen aktivt försvara sina säkerhetsintressen** genom att ta itu med yttre hot, störa smugglingsvägar och skydda korridorer av strategiskt intresse, såsom handelsvägar. EU kommer samtidigt att fortsätta att vara en stark allierad till partnerländerna och samarbeta för att stärka den globala säkerheten och bygga upp ömsesidig motståndskraft mot hot.

Under de senaste åren har EU vidtagit betydande åtgärder för att stärka sitt säkerhetssamarbete. EU har upprättat operativa avtal om brottsbekämpning och rättsligt samarbete samt andra typer av arrangemang med partnerländer. Unionen strävar aktivt efter att upprätta ytterligare internationella avtal, i linje med rådets förhandlingsdirektiv, och mot

initiativ för kapacitetsuppbyggnad, som främjas av EU:s byråer och organ. Instrumentet Europa i världen spelar också en avgörande roll i att stärka säkerheten med partnerländerna.

Den **regelbaserade världsordningen** är en hörnsten vad gäller att stärka den globala säkerheten. Säkerhetsdialoger, inbegripet tematiska dialoger, är avgörande för att stärka dessa insatser. Genomförandet av den **strategiska kompassen för säkerhet och försvar**, tillsammans med bilaterala och multilaterala ramar för samarbete såsom stabiliserings- och associeringsavtal och associeringsavtal, och samarbete med organisationer som FN och Nato, är avgörande för att utveckla effektiva säkerhetslösningar. EU kommer att fortsätta att spela sin roll i multilaterala forum[84] och kommer att stärka sitt samarbete med relevanta internationella och regionala organisationer och ramar, däribland Nato, Förenta nationerna, Europarådet, Interpol, G7, OSSE och det civila samhället.

Regionalt samarbete

Det är prioriterat att som en politisk och geostrategisk nödvändighet fortsätta EU:s orubbliga stöd till **Ukraina** och stärka säkerheten och motståndskraften i **EU:s utvidgningsländer**. Stödet till EU:s säkerhet bör gå hand i hand med en **påskyndad integrering av kandidatländerna** i den **europeiska säkerhetsordningen**, parallellt med konsolideringen av deras regionala samarbete. Kommissionen kommer att använda EU:s utvidgningspolitik för att stödja kandidatländernas och de potentiella kandidatländernas kapacitet att reagera på hot, öka det operativa samarbetet och informationsutbytet och säkerställa anpassning till EU:s principer, lagstiftning och verktyg. Instrumentet för stöd inför anslutningen (IPA III) samt Ukrainafaciliteten, Moldavienfaciliteten och faciliteten för reformer och tillväxt för västra Balkan är avgörande för att stärka säkerheten i både kandidatländer och potentiella kandidatländer.

EU kommer också att ytterligare integrera **grannskapspartner** i den europeiska säkerhetsordningen. Genom den **nya pakten för Medelhavsområdet** och den kommande **strategin för Svartahavsregionen** kommer unionen att sträva efter att fortsätta att bygga upp regionalt samarbete och bilaterala strategiska övergripande partnerskap med en säkerhetsdimension, när så är relevant, med regelbundna säkerhetsdialoger på hög nivå. Det operativa samarbetet med Nordafrika, **Mellanöstern och gulfstaterna** kommer att stärkas, särskilt när det gäller terrorismbekämpning, bekämpning av penningtvätt, olaglig handel med skjutvapen samt produktion av och olaglig handel med narkotika, särskilt kaptagon**.**

För att ta itu med den ökade terroristverksamheten och brottsliga verksamheten och dess potentiella spridningseffekter i **Afrika söder om Sahara, särskilt Sahel, Afrikas horn och Västafrika**, kommer EU att stärka stödet till Afrikanska unionen, de regionala ekonomiska gemenskaperna och länderna i regionen. I linje med EU:s strategi för sjöfartsskydd[85] kommer EU att stärka samarbetet i **Guineabukten, Röda havet och Indiska oceanen** för att bekämpa människohandel och sjöröveri, genom att stödja samarbete inom Afrika och regionalt samarbete, och med stöd av EU:s samordnade närvaro till havs och Centrumet för analys av maritim underrättelseverksamhet beträffande narkotika (MAOC-N).

EU kommer att stärka det operativa samarbetet med **Latinamerika och Karibien** för att upplösa och lagföra kriminella högrisknätverk och störa olaglig verksamhet och smugglingsvägar samt stärka ramarna för samarbete, såsom den latinamerikanska kommittén för inre säkerhet och samordnings- och samarbetsmekanismen för narkotika mellan EU och

[84] Det globala forumet för terrorismbekämpning, den globala koalitionen mot Daesh, det globala internetforumet för terrorismbekämpning, Christchurch Call Foundation, den globala koalitionen för att hantera syntetiska narkotikahot.
[85] JOIN(2023) 8 final.

Celac. Logistiknavens motståndskraft samt partnerskap och strategier för följ pengarna-principen kommer att prioriteras. EU kommer att ytterligare stödja utvecklingen av organisationen för polisiärt samarbete i Latinamerika och Västindien (Ameripol), som är tänkt att bli den regionala motsvarigheten till Europol, och stärka det rättsliga samarbetet mellan medlemsstaterna och regionen. EU kommer också att samarbeta med **Sydasien och Centralasien** kring gemensamma säkerhetsproblem i samband med terrorism, olaglig handel med olagliga varor, inbegripet narkotika, människohandel och smuggling av migranter.

Dessutom kommer EU att stödja regionala samarbetsramar i tredjeländer för att ytterligare hjälpa dem att stoppa olaglig handel vid källan, i linje med principen om delat ansvar för hela den kriminella leveranskedjan. EU kommer dessutom att göra sin del för att stärka säkerheten vid logistiknav utomlands genom att samordna **gemensamma inspektioner i tredjeländers hamnar**.

Operativt samarbete

Global Gateway kommer att stödja hållbara infrastrukturprojekt av hög kvalitet inom sektorerna för digital teknik, klimat och energi, transport, hälso- och sjukvård, utbildning och forskning. Kommissionen kommer nu, när så är relevant, att inkludera säkerhetsöverväganden i framtida investeringar inom ramen för Global Gateway. Detta kommer att inbegripa initiativ som är avgörande för EU:s och dess partnerländers strategiska oberoende, såsom infrastrukturprojekt som omfattar säkerhetsbedömningar och riskreducerande åtgärder.

Kommissionen kommer att eftersträva ytterligare **avtal mellan EU och tredjeländer om samarbete med Europol och Eurojust**, särskilt med latinamerikanska länder.

Dessutom är ett proaktivt deltagande av tredjeländer i **Empact** ett av de effektivaste sätten att stärka det operativa samarbetet. EU kommer att fortsatt uppmuntra tredjeländer, särskilt i västra Balkan, det östra grannskapet, Afrika söder om Sahara, Nordafrika, Mellanöstern, Latinamerika och Karibien, att delta i ramen. Ett annat verktyg för att intensifiera samarbetet med tredjeländer i kampen mot brottslighet är de operativa arbetsgrupperna mellan medlemsstaterna som samordnas av Europol, där tredjeländer kan delta. Kommissionen strävar också efter att slutföra förhandlingarna om det internationella avtalet mellan **EU och Interpol**[86] för att säkerställa en mer enhetlig strategi för globala säkerhetshot och kampen mot gränsöverskridande brottslighet.

Unionen måste vara närvarande på plats inom ramen för Team Europe-strategin. Specialiserad personal från EU och medlemsstaterna spelar en avgörande roll för att säkerställa att unionens yttre åtgärder är väl underbyggda, samordnade och lyhörda. För att ta denna strategi till nästa nivå kommer kommissionen, med stöd av unionens höga representant för utrikes frågor och säkerhetspolitik, att stärka **sambandsnätverken** och underlätta utplaceringen av regionala **sambandspersoner för Europol och Eurojust**, i linje med medlemsstaternas operativa behov.

EU kommer att eftersträva ett närmare samarbete kring operativ brottsbekämpning och rättsligt samarbete, främja informationsutbyte i realtid och gemensamma insatser genom **gemensamma utredningsgrupper** i tredjeländer med stöd av Europol och Eurojust. Kommissionen kommer också att stödja medlemsstaterna i inrättandet av **gemensamma samkörningscentrum** som sammanför experter och lokala brottsbekämpande myndigheter i strategiska tredjeländer.

Verktyg inom ramen för den gemensamma utrikes- och säkerhetspolitiken (Gusp)

Uppdragen inom den gemensamma säkerhets- och försvarspolitiken (GSFP) kommer också att utnyttjas till sin fulla potential för att bättre kartlägga och hantera externa hot mot EU:s inre säkerhet, i enlighet med de mandat som rådet fastställt. För att bygga upp

[86] Rådets beslut (EU) 2021/1312 av den 19 juli 2021 och rådets beslut (EU) 2021/1313 av den 19 juli 2021.

tredjeländers kapacitet kommer unionens höga representant för utrikes frågor och säkerhetspolitik och kommissionen att stödja GSFP-åtgärder med särskilda finansieringsinstrument och utforska alla lämpliga finansieringsvägar.

EU:s restriktiva åtgärder är ett väletablerat Gusp-verktyg som också används i kampen mot terrorism. På grundval av förslag från unionens höga representant för utrikes frågor och säkerhetspolitik, medlemsstaterna eller kommissionen skulle rådet kunna bedöma hur de autonoma EU-sanktionerna (EU:s terroristförteckning) skulle kunna göras mer effektiva, operativa och smidiga. Dessutom skulle de kunna överväga att undersöka ytterligare restriktiva åtgärder mot kriminella nätverk, i linje med Gusp-målen.

Viseringspolitik och informationsutbyte

EU:s viseringspolitik är ett viktigt verktyg för samarbete med tredjeländer och för att säkra våra gränser genom att kontrollera inresor till EU och fastställa villkoren för dem. Kommissionen kommer att fullt ut integrera **säkerhetsöverväganden i EU:s viseringspolitik** genom en kommande EU-strategi för viseringspolitik. Kommissionen kommer att samarbeta med medlagstiftarna för att anta förslaget om att se över och effektivisera upphävandemekanismen, särskilt vid specifika fall av missbruk av det viseringsfria systemet[87]. Tredjeländer kommer att uppmuntras att utbyta information om personer som kan utgöra säkerhetshot, som kommer att föras in i EU:s informationssystem och databaser.

För att uppnå politisk samordning och insatser i tidigare led och möjliggöra ett effektivare, snabbare och smidigare samarbete kommer kommissionen att sträva efter att inrätta **dataflödesarrangemang** och undersöka sätt att **förbättra informationsutbytet** för brottsbekämpande ändamål och gränsförvaltning med betrodda tredjeländer i enlighet med grundläggande rättigheter och dataskyddsregler.

Nyckelåtgärder

Kommissionen kommer att

- **ingå internationella avtal mellan EU och prioriterade tredjeländer om samarbete med Europol och Eurojust,**
- **uppmuntra partnerländernas deltagande i Empact för att bekämpa organiserad brottslighet och terrorism,**
- **stödja EU:s byråer och organ vad gäller att upprätta och stärka samarbetsarrangemang med partnerländer,**
- **ytterligare beakta säkerhetsöverväganden i EU:s viseringspolitik genom den kommande EU-strategin för viseringspolitik**
- **och stärka informationsutbytet med betrodda tredjeländer för brottsbekämpande ändamål och gränsförvaltning.**

Kommissionen kommer att i samarbete med unionens höga representant för utrikes frågor och säkerhetspolitik

- **använda civila uppdrag inom den gemensamma säkerhets- och försvarspolitiken (GSFP) fullt ut**
- **och samordna gemensamma inspektioner i tredjeländers hamnar senast 2027.**

Kommissionen kommer att i samarbete med unionens höga representant för utrikes frågor och säkerhetspolitik och medlemsstaterna

- **stärka sambandsnätverken och samarbetet inom ramen för Team Europe-strategin**

[87] COM(2023) 642.

- **och inrätta gemensamma operativa grupper och samkörningscentrum i tredjeländer från och med 2025.**

Europaparlamentet och rådet uppmanas att

- **slutföra förhandlingarna om översynen av upphävandemekanismen.**

8. Slutsats

I en osäker värld måste EU förbättra sin förmåga att förutse, förebygga och reagera på säkerhetshot.

Det är inte tillräckligt att enbart reagera på kriser när de uppstår. Vi måste öka vår medvetenhet och få en fullständig bild av hoten allteftersom de utvecklas. Vi måste dessutom se till att våra verktyg och resurser är tillräckliga.

De omfattande åtgärder som beskrivs i denna strategi kommer att bidra till att skapa ett starkare EU i världen: ett EU som kan förutse, planera för och se till sina egna säkerhetsbehov, som effektivt kan reagera på hot mot den inre säkerheten och ställa förövarna till svars, och som skyddar sina öppna, fria och välmående samhällen och demokratier.

Detta kräver en ny inställning till inre säkerhet. Vi kommer att sträva efter att främja en ny säkerhetskultur i EU, där säkerhetsöverväganden beaktas i all lagstiftning och politik och i alla program – hela vägen från planering till genomförande – och där samarbete över olika politikområden gör det möjligt för oss att bryta ny mark.

Detta är ingen uppgift för enskilda institutioner, stater eller aktörer. Det är Europas gemensamma sak.