EUROPEISKA
KOMMISSIONEN

Bryssel den 9.12.2020
COM(2020) 797 final

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

Första lägesrapporten om strategin för EU:s säkerhetsunion

I INLEDNING

Säkerheten är en av de saker som medborgarna oroar sig mest för, och vågen av terroristattacker i Europa på senare tid har ytterligare understrukit behovet av EU-åtgärder. Den 24 juli 2020 antog kommissionen en ***strategi för EU:s säkerhetsunion 2020–2025***[1] för att vidta åtgärder på prioriterade områden där EU kan tillföra ett mervärde till de nationella insatserna. Strategin bygger på de framsteg som tidigare gjorts inom ramen för den europeiska säkerhetsagendan 2015–2020[2] men med nytt fokus för att säkerställa att EU:s säkerhetspolitik återspeglar den föränderliga hotbilden, skapar långsiktig, hållbar resiliens, engagerar EU:s institutioner och organ, myndigheter, den privata sektorn och enskilda personer i ett helhetsgrepp över hela samhället och sammanför de många politikområden som har en direkt inverkan på säkerheten. Detta arbete genomsyras av full respekt för de grundläggande rättigheterna, eftersom unionens säkerhet enbart kan tryggas när alla litar på att deras grundläggande rättigheter inte äventyras.

Hotet från gränsöverskridande terroristnätverk är en tydlig påminnelse om att det krävs samordnade EU-åtgärder för att effektivt skydda européerna och upprätthålla våra gemensamma värden och vårt europeiska levnadssätt. Allt komplexare gränsöverskridande och sektorsövergripande säkerhetshot har uppstått, och det gör ett nära säkerhetssamarbete på alla nivåer så mycket viktigare. Detta gäller för organiserad brottslighet och narkotikahandel – men det gäller också den digitala världen, med it-angrepp och it-brottslighet som fortsätter att öka. Alla dessa utmaningar gäller även utanför våra gränser, och det finns en tydlig koppling mellan inre och yttre säkerhet. Covid-19-krisen har också riktat uppmärksamheten mot den europeiska säkerheten. Krisen har inneburit hårda prövningar för Europas kritiska infrastruktur, krisberedskap, strategiska värdekedjor och krishanteringssystem, och även för våra samhällens motståndskraft mot manipulativa ingrepp och desinformation.

Strategin för säkerhetsunionen består av fyra strategiska prioriteringar för åtgärder på EU-nivå: en framtidssäkrad säkerhetsmiljö, hantering av föränderliga hot, skydd mot terrorism och organiserad brottslighet samt ett starkt europeiskt säkerhetsekosystem. Genomförandet är centralt i strategin och det är också det centrala temat i denna rapport – ett genomförande som kräver fullt engagemang från nationella myndigheter som har det främsta ansvaret för säkerheten i EU. Den här rapporten är den första genomföranderapporten inom ramen för strategin och innebär att kommissionen har fullföljt sitt åtagande att regelbundet rapportera om framstegen[3]. Rapporten täcker perioden från den 31 oktober 2019, då den senaste lägesrapporten om säkerhetsunionen offentliggjordes under den föregående kommissionens mandatperiod[4].

II EN FRAMTIDSSÄKRAD SÄKERHETSMILJÖ

1. *Skyddad och motståndskraftig kritisk infrastruktur*

Allmänhetens vardag vilar på en allt mer sammanflätad, sammankopplad fysisk och digital infrastruktur. Den här infrastrukturen är avgörande för att ekonomin och samhället ska fungera. Utan tillförlitlig energiförsörjning, förutsägbara transporter, heltäckande hälso-

[1] COM(2020) 605 final.
[2] COM(2016) 230 final.
[3] Under utfrågningen av vice ordförande Margaritis Schinas i Europaparlamentet den 3 oktober 2019.
[4] COM(2019) 552 final.

och sjukvårdssystem och ett digitalt finansiellt nätverk skulle vår nuvarande livsstil inte vara möjlig. Covid-19-pandemin har än tydligare visat hur viktigt det är att **säkerställa resiliens i kritiska sektorer och för kritiska aktörer**. EU har insett det gemensamma intresset i att skydda kritisk infrastruktur från hot, oavsett om det rör sig om naturkatastrofer, katastrofer orsakade av människan eller terroristattacker. Den nuvarande hotbilden mot kritisk infrastruktur är omfattande. Den omfattar terrorism, hybridåtgärder, it-attacker, insiderangrepp, hot som hör ihop med ny teknik (som drönare, 5G och artificiell intelligens), klimatrelaterade utmaningar, störningar i leveranskedjorna och valpåverkan. Våra nuvarande regler behöver moderniseras och utvidgas[5]. De måste få nytt fokus från skydd till resiliens, bli mer samstämmiga och enhetliga vad gäller sektorstäckningen och inriktas på kritiska enheter som tillhandahåller samhällsviktiga tjänster.

Detta kommer att vara målet med kommande förslag för att främja den **fysiska och digitala infrastrukturens** resiliens. Det övergripande målet är att öka beredskapen både på nationell nivå och EU-nivå genom att bygga upp robust kapacitet för att förebygga, upptäcka, reagera på och mildra hot, och att vara beredda att agera i krissituationer. Den befintliga lagstiftningen har gjort det möjligt att öka och förbättra riskhanteringen i kritiska sektorer och detta arbete måste intensifieras. Ett av de främsta målen i det omarbetade direktivet om kritisk infrastruktur kommer att vara att främja en hög gemensam resiliensnivå inom ett tillräckligt antal nyckelsektorer. En uppdatering av nätverks- och informationssäkerhetsdirektivet (NIS-direktivet) syftar på samma sätt till att ge större enhetlighet i medlemsstaternas identifiering av ”leverantörer av samhällsviktiga tjänster”[6]. Trots betydande framsteg är it-säkerheten i medlemsstaterna fortfarande varierande, och syftet med översynen är att försöka öka it-säkerheten i allmänhet[7]. Resultatet kommer att bli mer omfattande och mer konsekventa strategier för den fysiska och digitala infrastrukturens resiliens.

Arbetet går allt mer mot en sådan mer sammanhängande ram och därför kommer **sektorsspecifika initiativ** att komplettera arbetet och inriktas på specifika sårbara punkter. De speciella utmaningarna vad gäller it-säkerhet inom energisektorn kommer man nu att arbeta vidare med utifrån kommissionens rekommendation från 2019[8]. Sektorns särskilda egenskaper kommer att beaktas, såsom realtidskrav, risken för kaskadeffekter och kombinationen av äldre system och ny teknik. Arbete pågår med särskilda nätföreskrifter om it-säkerhet för gränsöverskridande elflöden och för skydd av resiliens och it-säkerhet hos kritisk energiinfrastruktur. Det tematiska nätverket för skydd av kritisk energiinfrastruktur har återupptagits med nytt fokus och nya mål, och sammanträdde första gången i juni 2020 med över 100 deltagare online. Det här nätverket erbjuder en plattform som kan främja gränsöverskridande samarbete mellan operatörer av kritisk energiinfrastruktur och ägare inom energisektorn.

Som en gemensam startpunkt för medlemsstaternas samarbete med **riskberedskap inom elsektorn** fastställde det europeiska nätverket av systemansvariga för överföringssystemen för el i september 2020 det mest relevanta regionala elkrisscenariot som beskrivs i

---

5 Direktiv 2008/114/EG och direktiv (EU) 2016/1148.

6 COM(2019) 546 final. Kommissionen har också genomfört ett offentligt samråd (7 juli–2 oktober 2020) och landsbesök i alla medlemsstater för att genom möten med aktörer och myndigheter kontrollera överenstämmelsen i genomförandet av direktivet.

7 COM(2019) 546 final.

8 C(2019) 2400.

riskberedskapsförordningen[9]. Detta omfattar såväl it-attacker som pandemier och extrema väderförhållanden. Medlemsstaterna ska förbereda nationella krisscenarier och riskberedskapsplaner för att förebygga och mildra elkriser (de första utkasten ska läggas fram i april 2021). Som ett bidrag till denna process utfärdades i juni 2020 ett dokument med god praxis[10], som bygger på en noggrann granskning av hur covid-19-krisen har påverkat energisektorn. Granskningen utfördes av samordningsgrupperna för el, gas och olja, europeiska högnivågruppen för kärnsäkerhet och avfallshantering och Europeiska unionens grupp av myndigheter för olje- och gasverksamhet till havs.

Finansiella tjänster blir allt mer beroende av avancerade digitala processer, vilket innebär att det krävs ökad it-säkerhet även inom **finanssektorn**. IKT-system betraktas som en integrerad del av riskhanteringen för finansiella enheter, men detta återspeglas inte fullt ut i EU:s tillsyn över finansiella tjänster. Den 24 september 2020 antog kommissionen sin strategi för digitalisering av finanssektorn[11], med ett tydligt mål att ta itu med utmaningar och risker i samband med den digitala omställningen och främja resiliens, dataskydd och lämplig tillsyn. Detta omfattar ett lagstiftningsförslag om digital operativ resiliens[12], som ska säkerställa att det finns skyddsåtgärder som kan mildra it-attacker och andra risker[13]. Det här initiativet bidrar till en stark och dynamisk europeisk digital finanssektor och ökar därmed EU:s förmåga att stärka vårt öppna strategiska oberoende när det gäller finansiella tjänster och, i förlängningen, vår förmåga att reglera och övervaka det finansiella systemet för att skydda EU:s finansiella stabilitet.

Det omfattande ömsesidiga beroendet mellan sektorer och länder kräver i större krissituationer en samordnad insats för att säkerställa en snabb och effektiv reaktion. Det krävs också bättre förebyggande åtgärder och beredskap för liknande situationer i framtiden. I översynen av beslutet om en civilskyddsmekanism för unionen[14] har kommissionen föreslagit[15] att **resiliensmål vid katastrofer** och **resiliensplanering vid katastrofer** ska tas fram med ökat fokus på att bygga upp en mer långsiktig sektorsövergripande resiliens mot gränsöverskridande katastrofer. Den föreslagna nya strategin för att bygga upp resiliensen kompletterar arbetet med katastrofriskhantering på nationell nivå. Den 26 november nådde rådet en överenskommelse om ett förhandlingsmandat för att stärka förebyggande, beredskap och insatser vid katastrofer, utifrån kommissionens förslag av den 2 juni 2020[16].

Covid-19-pandemin har visat vilka konsekvenser hälsokriser kan få för säkerheten på EU-nivå och global nivå och framhävt vad som behöver göras för att öka beredskaps- och insatsplaneringen för epidemier och andra allvarliga gränsöverskridande hälsohot. I kommissionens paket av den 11 november 2020 om ”**Skapande av en europeisk hälsounion** – förstärkning av EU:s resiliens mot gränsöverskridande hot mot människors hälsa” beskrivs vad som behöver göras härnäst för att hantera gränsöverskridande hälsohot.

---

9 EUT L 158, 14.6.2019, s. 1.

10 *Energy security: good practices to address pandemic risks* (SWD(2020) 104).

11 https://ec.europa.eu/info/publications/200924-digital-finance-proposals_sv.

12 COM(2020) 595 final.

13 I förslaget beskrivs ett enhetligt grundscenario för IKT vad gäller riskhanteringskrav, händelserapportering till finansiella tillsynsmyndigheter, digitala tester och informationsdelning. Dessutom föreslås att tredjepartsleverantörer av kritiska IKT-tjänster ska bli föremål för tillsyn på EU-nivå.

14 Beslut nr 1313/2013/EU av den 17 december 2013 om en civilskyddsmekanism.

15 COM(2020) 220 final.

16 Förslag om ändring av beslut 1313/2013/EU om en civilskyddsmekanism – Förhandlingsmandat med Europaparlamentet

Det skulle ge en förstärkt ram för gränsöverskridande samarbete mot alla hälsohot och inbegripa tre lagstiftningsförslag: en uppgradering av lagstiftningen om allvarliga gränsöverskridande hälsohot och en förstärkning av Europeiska centrumet för förebyggande och kontroll av sjukdomar(ECDC) och av Europeiska läkemedelsmyndigheten (EMA). Med de här förslagen inrättas en robust och kostnadseffektiv ram som kan ge EU och medlemsstaterna en stabilare grund när de gäller insatser mot framtida hälsokriser.

En viktig faktor för att skydda viktiga europeiska och nationella digitala resurser är att erbjuda den kritiska infrastrukturen en kanal för **säker kommunikation**. Det kan ske med hjälp av en nätinfrastruktur för säker och störningstålig statlig satellitkommunikation, som en komponent i EU:s rymdprogram.

2. ***It-säkerhet***

Fördelarna med den digitala omställningen är tydliga, men det är också oundvikligt att den medför en ökning av potentiella sårbarheter[17]. Kritisk infrastruktur blir ofta mål för allt mer avancerade it-attacker[18]. **It-säkerheten** måste därför vara en angelägenhet inte bara för beslutsfattare utan för alla som arbetar eller kommunicerar på nätet.

För att öka tilliten till och säkerheten hos digitala produkter, processer och tjänster skapade cybersäkerhetsakten från juni 2019 **ett europeiskt ramverk för cybersäkerhetscertifiering**. Kommissionen har bett EU:s cybersäkerhetsbyrå Enisa att utarbeta två system för cybersäkerhetscertifiering, och förberedelserna är i full gång. Det här arbetet inbegriper också nationella myndigheter för cybersäkerhetscertifiering, näringslivet, konsumenter, ackrediterings-, standardiserings- och certifieringsorgan och Europeiska dataskyddsstyrelsen.

Ett av dessa system är ett system för **molntjänster** till stöd för en säker och tillförlitlig marknad för molntjänster. Det är en viktig del i **EU:s datastrategi** som antogs i februari 2020[19]. Det skulle skapa en gemensam, sektorsövergripande säkerhetsgrund för molntjänster, och bygga på högsta befintliga (europeiska och internationella) standarder,

[17] Enisa Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected.

[18] Sedan pandemin bröt ut har EU-byråerna och medlemsstaterna upptäckt en betydande ökning av it-angreppen, även mot hälso- och sjukvårdssektorn.

[19] COM(2020) 66 final.

system och praxis. Detta kommer att vara ett centralt inslag i det fria dataflödet i EU[20]. Systemet kommer också att gynna användningen av molnteknik genom att användarna, särskilt små och medelstora företag och offentlig förvaltning, får begripliga försäkringar om säkerhetsnivån när de använder molnet.

Som framhölls i EU:s strategi för en säkerhetsunion och mot bakgrund av den pågående utbyggnaden av 5G-infrastruktur i EU och det faktum att många kritiska tjänster kan bli beroende av 5G-nät, kan konsekvenserna av systemomfattande och utbredda störningar bli särskilt allvarliga. Resultatet har varit en gemensam insats från medlemsstaterna att utveckla och införa lämpliga säkerhetsåtgärder. Efter kommissionens rekommendation om **cybersäkerheten i 5G-nät** från mars 2019[21] genomförde medlemsstaterna nationella riskbedömningar som utmynnade i en samordnad EU-riskbedömningsrapport[22] där säkerhetsutmaningarna i samband med 5G-nät fastställdes. Utifrån detta offentliggjorde samarbetsgruppen för nät- och informationssäkerhet[23] den 29 januari 2020 **EU:s verktygslåda för riskreducerande åtgärder**[24] som beskriver nödvändiga strategiska och tekniska åtgärder. Verktygslådan omfattar åtgärder för att skärpa säkerhetskraven för mobilnätsoperatörer, säkerställa mångfalden bland leverantörer för enskilda mobilnätsoperatörer, bedöma leverantörernas riskprofil och tillämpa restriktioner för leverantörer som anses utgöra en hög risk. Kommissionen kommer att stödja genomförandet av verktygslådan genom att fullt ut utnyttja de befogenheter och medel som står till dess förfogande[25], inbegripet telekom- och it-säkerhetsregler, samordnad standardisering och EU-certifiering och EU:s ram för utländska direktinvesteringar[26].

Samarbetsgruppen för nät- och informationssäkerhet offentliggjorde i juli 2020 en lägesrapport om genomförandet av åtgärderna i verktygslådan[27]. Där noterades att en stor majoritet av medlemsstaterna redan har antagit eller håller på att genomföra de åtgärder som rekommenderades i verktygslådan. Åtgärder vars genomförande inte kommit så långt var bland annat att minska risken för beroendet av högriskleverantörer och utveckla strategier för att använda flera leverantörer både på företagsnivå och på nationell nivå.

Under de senaste månaderna har EU-institutionerna och medlemsstaterna reagerat på den förhöjda it-säkerhetsrisken som **Covid-19-krisen** har lett till. De har bland annat intensifierat informationsutbytet och öka beredskapen inför en potentiell it-kris. EU-samarbetet har intensifierats i viktiga forum (samarbetsgruppen för nät- och informationssäkerhet och nätverket av it-incidentcentrum) och genom nya former av samordnings- och informationsdelningsverktyg[28]. I september 2020 genomfördes en andra

---

20 Förordning (EU) 2018/1807.

21 COM(2019) 2335 final.

22 Rapport om EU coordinated risk assessment of the cybersecurity of 5G networks.

23 Samarbetsgruppen för nät- och informationssäkerhet inrättades för att säkerställa strategiskt samarbete och informationsutbyte mellan EU:s medlemsstater om it-säkerhet.

24 https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

25 COM(2020) 50 final.

26 Förordning (EU) 2019/452. Detta omfattar också uttryckliga hänvisningar till ”kritisk infrastruktur” (liksom ”kritisk teknik”), mer allmänt som ”faktorer som medlemsstaterna eller kommissionen får beakta” vid bedömningen av en investerings potentiella effekter.

27 Rapport om Member States’ progress in implementing the EU Toolbox on 5G Cybersecurity.

28 EU-institutioner och byråer samlades i en specialgrupp för it-säkerhet för covid-19 och lanserade en sektorsvis veckorapport om situationsmedvetenhet och analys. Enisa och Europol lanserade kampanjer om hur man kan bevara it-säkerheten under covid-19. CERT-EU har utfärdat riktlinjer för hur man upprättar säkra VPN-system. Sommaren 2019 upprättade samarbetsgruppen för nät- och

skrivbordsövning för att kontrollera den operativa nivån (Blue OLEx)[29], där ”Cyber Crisis Liaison Organisation Network” (CyCLONe) i medlemsstaterna också lanserades. Det kommer att bidra ytterligare till genomförandet av strategin för samordnade insatser vid storskaliga it-incidenter och cyberkriser[30].

I den globala cyberrymden kommer it-attacker och hot ofta från länder utanför EU. För att effektivt kunna hantera dessa hot samarbetar EU och medlemsstaterna för att öka den internationella säkerheten och stabiliteten i cyberrymden, främja ett ansvarsfullt statligt agerande, öka den globala resiliensen och öka medvetenheten om cyberhot och skadlig cyberverksamhet, även bland internationella partner[31]. Den 30 april 2020 gjorde EU:s utrikesrepresentant ett uttalande på EU:s vägnar och fördömde skadligt agerande i cyberrymden och uttryckte solidaritet med offren[32].

Den 30 juli 2020 antog rådet **EU:s första sanktioner mot cyberangrepp** mot sex enskilda personer och tre enheter som ansvarade för eller var inblandade i cyberattacker. Det gällde försöket till cyberattack mot OPCW (Organisationen för förbud mot kemiska vapen) och de attacker som är allmänt kända som WannaCry, NotPetya och Operation Cloud Hopper. Den 22 oktober 2020 antog rådet sanktioner mot två andra enskilda personer och en enhet som ansvarade för eller var inblandade i cyberattacken mot Tysklands förbundsdag. De här besluten följde efter fortlöpande signaler från EU och medlemsstaterna om behovet av att förebygga, motarbeta, avskräcka och reagera på skadlig cyberverksamhet, däribland med hjälp av de cybersanktioner som ingår i 2017 års verktygslåda för cyberdiplomati[33].

Förhandlingarna mellan medlagstiftarna om nya exportregler som begränsar försäljningen av cyberövervakningsvaror till regimer världen över som kränker de mänskliga rättigheterna[34] har också gått framåt. När dessa regler väl har antagits kommer det att leda till en mer ansvarsfull, konkurrenskraftig och transparent handel med produkter med dubbla användningsområden[35]. De föreslagna ändringarna är nödvändiga mot bakgrund av den tekniska utvecklingen och de ökande säkerhetsriskerna, och de omfattar nya kriterier för att bevilja eller avslå exporttillstånd för vissa produkter.

---

informationssäkerhet ett nytt arbetsflöde för it-säkerhet på hälsoområdet, och kommissionen och Enisa lanserade en EU-omfattande informations- och analyscentral för hälsa.

29 https://www.enisa.europa.eu/news/enisa-news/blue-olex-2020-the-european-union-member-states-launch-the-cyber-crisis-liaison-organisation-network-cyclone.

30 C(2017) 6100.

31 EU främjar den strategiska ramen för konfliktförebyggande, stabilitet och samarbete i cyberrymden, inbegripet genom EU:s deltagande i FN:s diskussioner om cyberfrågor. Två viktiga processer är den öppna arbetsgruppen om utvecklingen på området information och telekommunikation i samband med internationell säkerhet och gruppen med regeringsexperter på området för främjande av staters ansvarsfulla agerande i cyberrymden. Bland frågorna ingår påverkan från internationell rätt, genomförandet av avtalade icke-bindande frivilliga normer för staters ansvarsfulla agerande, förtroendeskapande åtgärder samt en utveckling av genomförandet genom riktad kapacitetsuppbyggnad.

32 https://www.consilium.europa.eu/sv/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/.

33 Rådsbeslut (Gusp) 2020/1127, 2020/1537 och 2020/651 som ingår i 9916/17.

34 COM(2016) 616 final. Syftet med kommissionens förslag är att ändra och omarbeta förordning (EG) nr 428/2009 som upprättade en gemenskapsordning för kontroll av export, överföring, förmedling och transitering av produkter med dubbla användningsområden.

35 Det rör sig om en stor grupp varor, material, programvara och teknik som kan användas för såväl civila som militära syften.

3. Skydd av offentliga platser

Som angavs i EU:s Agenda för terroristbekämpning[36] är skyddet av offentliga platser, genom uppbyggnad av resiliensen mot säkerhetshot, fortfarande en avgörande komponent i arbetet mot en ändamålsenlig och verklig säkerhetsunion. Kommissionen samarbetar med en mängd offentliga och privata aktörer för att ta fram vägledning och ge praktiskt stöd och finansiering[37], i enlighet med **Handlingsplan till stöd för skyddet av offentliga platser**[38] från **2017** och samlingen med god praxis för skydd av offentliga platser[39] från 2019. Som angavs i EU:s agenda om terrorismbekämpning kommer kommissionen att intensifiera sitt stöd till lokala och regionala myndigheter eftersom de spelar en nyckelroll när det gäller att skydda offentliga platser och förebygga radikalisering. Detta ska bland annat omfatta ett EU-protokoll om säkerhet och resiliens för städer, och grundläggande principer och mål för lokala myndigheter på dessa områden.

Eftersom terroristattacker allt mer riktas mot **gudstjänstlokaler** har särskild tonvikt lagts på samarbete mellan myndigheter och religiösa ledare och församlingar, för att öka medvetenheten om säkerhet och hjälpa till att genomföra god praxis och utbildning i församlingarna. Enkla åtgärder kan utgöra skillnaden mellan liv och död. I oktober 2019 blev en synagoga i Halle mål för en terroristattack. En förstärkt dörr, en SOS-knapp och säkerhetskameror bidrog till att rädda liv.

För att ytterligare öka säkerheten på offentliga platser, framför allt gudstjänstlokaler, satte kommissionen 2020 in 20 miljoner euro till projekt som leds av berörda aktörer.

Kommissionen arbetar också med att hantera **nya risker på offentliga platser**, bland annat **obemannade luftfartygssystem** (drönare). Drönare kan ge betydande ekonomiska möjligheter och sysselsättningsmöjligheter men de utgör också en stor risk på offentliga platser, för kritisk infrastruktur och andra känsliga platser, som fängelser. Risken har mildrats med nya EU-bestämmelser[40] på det här området, genom att säkerheten för drönaroperationer har förbättrats. Från och med januari 2021 ska drönaroperatörer registreras hos nationella myndigheter. Detta system kan kompletteras med ett **regelverk för U-space**, Europas trafikledningssystem för obemannad trafik[41], för att ge säkrare drönaroperationer. Tillsammans kommer dessa åtgärder att försvåra för enskilda personer att flyga drönare inom restriktionsområden och bidra till att identifiera och åtala brottslingar.

Kommissionen arbetar också för att stödja brottsbekämpare, aktörer inom kritisk infrastruktur, arrangörer av massevenemang och andra berörda parter för att motverka icke-samarbetsvilliga användare av drönare. Man arbetar exempelvis med Europeiska unionens byrå för luftfartssäkerhet för att ta fram **god praxis för att hjälpa flygplatsaktörer** att reagera på otillåtna drönarincidenter, underlätta mer harmoniserade

---

[36] COM(2020) 795 final.

[37] 2019 års inbjudan att lämna projektförslag om skydd inom ramen för Fonden för inre säkerhet omfattade ”Secu4All” som ska utveckla ett omfattande utbildningsprogram för lokala myndigheter för att ge invånarna en säker stadsmiljö, och ”DroneWISE” som ska stärka beredskapen för en första insats mot fientliga obemannade luftfartyg. Under 2020 kommer en ny inbjudan som omfattar 12 miljoner euro att offentliggöras om skydd av offentliga platser.

[38] COM(2017) 612 final.

[39] SWD(2019) 140.

[40] Kommissionens genomförandeförordning (EU) 2019/947.

[41] Kommissionen kan föreslå en genomförandeförordning i detta syfte, som skulle antas genom ett granskningsförfarande med deltagande av flygsäkerhetskommittén.

testinsatser för motåtgärder runt omkring i EU och ta fram en praktisk handbok för aktörer, med fokus på tätorter.

Kommissionens gemensamma forskningscentrum arrangerade i oktober 2020 en **digital höstskola för skydd av offentliga platser** som samlade över 200 stadsplanerare och offentliga och privata operatörer inom offentliga platser. Utbildningen omfattade en mängd olika ämnen, t.ex. hur man kan skydda sig mot bombdåd och fordonsattacker, minska hoten från fientliga drönare i tätorter och använda övervaknings- och detektionsteknik.

Kommissionen har också fortsatt att aktivt stödja **partnerskapet för säkerhet på offentliga platser,** med start i januari 2019 inom ramen för EU-agendan för städer, som har offentliggjort sin nya handlingsplan[42] för att hantera säkerheten i tätorter på olika förvaltningsnivåer. Åtgärderna omfattar bland annat utformningen av en ram för ett självbedömningsverktyg, rekommendationer för beslutsfattande, styrning och finansiering på flera nivåer, innovation med smarta lösningar och smart teknik, däribland begreppet inbyggd säkerhet, säkerhet genom förebyggande och säkerhet genom social inkludering. Partnerskapet går nu in i genomförandefasen.

Genom den fjärde ansökningsomgången för innovativa åtgärder i städerna tillhandahölls stöd för att förbättra säkerheten på offentliga platser på lokal nivå. Tre städer har valts ut och testar nya lösningar på området säkerhet i städer (Pireus i Grekland, Tammerfors i Finland och Turin i Italien), med medel från Europeiska regionala utvecklingsfonden.

När det gäller beredskap har kommissionen också tagit fram en europeisk ram för att förbättra beredskapen och insatserna vid incidenter med många brännskadade, där hela Europas kapacitet för vård av brännskadade patienter utnyttjas genom samarbete på EU-nivå. Europeiska unionens civilskyddsmekanism kan utnyttjas för att stödja ett stort antal patienter med allvarliga brännskador med tillgång till specialsängar för brännskadade på särskilda behandlingscentrum, experter på bedömning av brännskador och medicinsk evakueringskapacitet.

[42] Handlingsplanen har antagits och finns på Futurium: https://ec.europa.eu/futurium/en/security-public-spaces/security-public-spaces-partnership-final-action-plan-0.

III HANTERA FRAMVÄXANDE HOT

1. It-relaterad brottslighet

Brottslingar utnyttjar ofta brister i it-säkerheten. Detta har blivit tydligare än någonsin under covid-19-krisen. Antalet ”klassiska” it-brott med hjälp av sabotageprogram och utpressningsprogram (dvs. stöld av personuppgifter och betalningsuppgifter eller utpressning av offer) har ökat, liksom spridningen av nya webbplatser som lockar användare att installera sabotageprogram. It-attacker mot hälso- och forskningsinfrastruktur har inträffat, där man har låst IKT-system som har låsts upp endast mot en lösensumma eller mot tillgång till information om vaccinutvecklingen[43]. En avsevärd ökning av sexuella övergrepp mot barn och material om sexuella övergrepp mot barn har också noterats[44].

För effektiva insatser mot it-brottslighet krävs ett starkt ramverk för förundersökning och lagföring. Ett viktigt första steg är fullt införlivande och genomförande av direktivet om **angrepp mot informationssystem**[45]. Kommissionen övervakar åtgärderna i Bulgarien, Italien, Portugal och Slovenien efter att överträdelseförfaranden inleddes 2019. Det krävs också framsteg för genomförandet av **direktivet om bekämpande av sexuella övergrepp mot barn**[46] från 2011. De områden som fortfarande kräver insatser är förebyggande, materiell straffrätt, stöd och skyddsåtgärder för barn som fallit offer för övergrepp. Sedan 2018 har kommissionen inlett överträdelseförfaranden mot 25 medlemsstater[47].

Den 24 juli 2020 antog kommissionen en **EU-strategi för en effektivare bekämpning av sexuella övergrepp mot barn**[48], som syftar till att vidta effektiva åtgärder på EU-nivå för att bekämpa brottet sexuella övergrepp mot barn. En särskild ny utmaning har tillkommit eftersom vissa kommunikationstjänster på nätet, såsom e-post och meddelandetjänster, från den 21 december 2020 omfattas av direktivet om integritet och elektronisk kommunikation och därmed omfattas av de reviderade definitionerna i den europeiska kodexen för elektronisk kommunikation. Till följd av detta finns det en klar risk för att leverantörer av de tjänster som utför viktig frivilligverksamhet i syfte att upptäcka, hantera och rapportera sexuella övergrepp mot barn på internet i dag måste upphöra med detta. Kommissionen har därför föreslagit en **förordning**[49] för att denna frivilligverksamhet ska kunna fortsätta under vissa villkor, tills en långsiktig lagstiftningslösning är på plats. Kommissionen arbetar på ett förslag till sådan lösning och den planeras att antas under 2021.

En **it-försvarsallians under covid-19** har upprättats av det europeiska nätverket för centrum för it-säkerhet och kompetensnav för innovation och insatser, för att utveckla innovativa strategier för att motverka covid-19-relaterade brott. I april 2020 upprättades en

---

43 Hotbildsbedömning av internetstödd organiserad brottslighet (Iocta) 2020, oktober 2020

44 Report on Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic, Europol, 19.6.2020.

45 Direktiv 2013/40/EU.

46 Direktiv 2011/93/EU.

47 Spanien, Portugal, Italien, Nederländerna, Sverige, Malta, Litauen, Slovakien, Bulgarien, Rumänien, Tyskland, Österrike, Belgien, Tjeckien, Estland, Grekland, Finland, Frankrike, Kroatien, Ungern, Irland, Luxemburg, Lettland, Polen och Slovenien.

48 COM(2020) 607 final.

49 COM(2020) 568 final.

särskild covid-plattform inom ramen för EIC[50], som kopplar samman civilsamhälle, innovatörer, partner och investerare i hela EU för att utveckla innovativa lösningar.

För att lagföringen av brottslingar ska bli effektivare, och med tanke på hur viktig elektronisk information och elektronisk bevisning är i brottsutredningar, bör polisen och straffrättsliga myndigheter snabbt få tillgång till sådan information och bevis till sina förundersökningar. Detta fastställdes i det gemensamma uttalandet från EU:s inrikesministrar den 13 november 2020[51]. Europol, Eurojust och det europeiska rättsliga nätverket offentliggjorde den 1 december 2020 sin andra lägesrapport SIRIUS EU om elektronisk bevisning. I rapporten belyses den ökade betydelsen av elektronisk bevisning i brottsutredningar[52]. Europaparlamentet har ännu inte fastställt någon ståndpunkt om kommissionens förslag om **gränsöverskridande tillgång till elektronisk bevisning**[53] från april 2018, så förhandlingarna mellan medlagstiftarna har ännu inte inletts. Förseningar i antagandet av dessa förslag hindrar polisens och de rättsliga myndigheternas arbete och komplicerar de pågående satsningarna att upprätta kompatibla regler för gränsöverskridande tillgång till e-bevisning genom internationella förhandlingar[54].

På internationell nivå deltar kommissionen på EU:s vägnar i de pågående förhandlingarna om det andra tilläggsprotokollet till Europarådets **Budapestkonvention om it-brottslighet**. Det här protokollet kan ge behöriga brottsbekämpande myndigheter förstärkta, kraftfulla verktyg för gränsöverskridande samarbete i fråga om utredning och lagföring av it-brott och andra grova brott, inbegripet direkt samarbete med tjänsteleverantörerna. Eftersom de flesta av dessa förbättrade och förstärkta samarbetsmöjligheter kommer att bygga på utbyte av personuppgifter är det viktigt att det framtida protokollet ger tillräckligt skydd av data, inte bara med tanke på grundläggande rättigheter utan också för att säkerställa rättssäkerhet, ömsesidigt förtroende och ändamålsenlighet i det operativa brottsbekämpningssamarbetet.

Förhandlingarna bör slutföras under 2021. Förutom mandatet från rådet (rättsliga och inre frågor) förra året förhandlar kommissionen samtidigt om ett **avtal mellan EU och USA om gränsöverskridande tillgång till elektronisk bevisning**. Detta skulle komplettera de föreslagna interna EU-bestämmelserna för direkt gränsöverskridande samarbete med tjänsteleverantörer, genom att lagkonflikter undanröjs och gemensamma regler och skyddsåtgärder införs. Formella förhandlingar inleddes den 25 september 2019 och många

---

50 Kommission anordnade tillsammans med Europeiska innovationsrådet och medlemsstaterna ett pan-europeiskt EUvsVirus-hackaton + Matchathon https://covid-eic.easme-web.eu/.

51 Gemensamt uttalande från EU:s inrikesministrar om den senaste tidens terroristattacker i Europa, 13.11.2020,
12634/20.

52 Enligt rapporten skedde en markant ökning av antalet gränsöverskridande förfrågningar från myndigheter i EU till leverantörer av onlinetjänster under 2019, och en stor majoritet av dem kom från Tyskland (37,7 % av förfrågningarna), Frankrike (17,9 %) och Storbritannien (16,4 %). Förfrågningar om tillgång till elektroniska uppgifter fördubblades i Polen och närmare tredubblades i Finland. Dessutom ökade de akuta begärandena om utlämnande av uppgifter med närmare 50 % på ett år.

53 COM(2018) 226 final och COM(2018) 225 final.

54 FN:s generalförsamling antog den 27 december 2019 resolution 74/247 ”Countering the use of information and communications technologies for criminal purposes” som upprättade en öppen ad hoc-mellanstatlig expertkommitté som har till uppgift att utarbeta en övergripande internationell konvention om it-brottslighet. EU stöder inte att nya internationella rättsliga instrument skapas om it-brottslighet, eftersom Budapestkonventionen redan erbjuder ett omfattande multilateralt rättsligt ramverk. I juli 2020 enades FN:s medlemsstater om att skjuta upp de första stegen. EU bidrog till processen på grundval av en gemensam ståndpunkt (dok.7677/2/20).

förhandlingsrundor har redan ägt rum. Resultaten av förhandlingarna beror i hög grad på vilka framsteg som görs i fråga om interna e-bevisningsregler.

Med avseende på **lagring och användning av uppgifter för brottsbekämpningsändamål**, följdes den tidigare domen *Tele2 mot Watson*[55] från 2016 upp av kommissionen genom expertsamråd med relevanta tjänsteleverantörer, polisen och rättsliga myndigheter, civilsamhället, dataskyddsmyndigheter, den akademiska världen och EU-byråer. Synpunkter inkom också genom en undersökning om datalagringspraxis hos leverantörer av elektroniska kommunikationstjänster och brottsbekämpande myndigheters behov av och praxis att få tillgång till uppgifter, identifiering av relevanta tekniska utmaningar och en översyn av de nationella rättsliga ramarna[56]. Det här arbetet har visat att det är nödvändigt att brottsbekämpande myndigheter får tillgång till data för att effektivare kunna utföra sitt arbete.

Den 6 oktober 2020 avkunnade domstolen domar[57] avseende den nationella lagstiftningen i Belgien, Frankrike och Förenade kungariket om lagring, överföring och tillgång till icke-innehållsdata för ändamål rörande brottsbekämpning och nationell säkerhet. Kommissionen kommer att bedöma vilka alternativ som finns för att säkerställa att terrorister och andra brottslingar ska kunna identifieras och spåras upp, samtidigt som EU-rätten följs så som den tolkas av domstolen, även med hänsyn till andra pågående mål i domstolen i denna fråga.

En annan viktig del i bekämpningen av it-brott har varit att säkerställa tillgången till och korrektheten i registreringsinformation för domännamn på internet (**Whois-data**) i linje med insatserna från Internet Corporation for Assigned Names and Numbers (ICANN). Diskussionerna syftar till att säkerställa att legitima aktörer som ansöker om tillgång, däribland polisen och it-säkerhetsaktörer, ska kunna få effektiv tillgång till allmän registreringsinformation för toppdomäner, med full respekt för tillämpliga dataskyddsregler. De slutliga rekommendationerna om en ny Whois-policy offentliggjordes den 10 augusti 2020 och håller för närvarande på att ses över, innan ett beslut ska fattas av styrelsen för ICANN. Kommissionen ska undersöka slutsatserna av översynen och om de i tillräcklig grad tar hänsyn till dataskydd och allmänintresse när det gäller att ge brottsbekämpande myndigheter och cybersäkerhetsoperatörer faktisk tillgång.

2. Modern brottsbekämpning

Ny teknik håller på att omforma i princip alla områden i samhället, däribland säkerheten, och det innebär att polisen och rättsväsendet måste få möjlighet att hålla jämna steg med utvecklingen. För att öka säkerhet och trygghet är det viktigt att integrera artificiell intelligens, stordata och högpresterande datorsystem i säkerhetspolitiken utan att försvaga det effektiva skyddet av grundläggande rättigheter.

Kommissionen arbetar med ett antal viktiga arbetsområden[58]. Den 25 november 2020 föreslog kommissionen[59] lagen om dataförvaltning, ett regelverk för att underlätta delning och återanvändning av personuppgifter och andra uppgifter för innovations- och

---

55 Dom i de förenade målen C-203/15 och C-698/15, *Tele2 Sverige AB och Watson m.fl.*, 21 december 2016.

56 https://data.europa.eu/doi10.2837/26288

57 Domar i mål C-623/17, Privacy International, och i de förenade målen C-511/18, La Quadrature du Net m.fl., C-512/18, French Data Network m.fl., och C-520/18, Ordre des barreaux francophones et germanophone m.fl.

58 Inklusive EU:s datastrategi (se ovan).

59 COM(2020) 767 final.

utvecklingsändamål. Detta omfattar näringslivet och offentliga organ via virtuella eller fysiska sektorsdataområden. Det skulle ge nationella brottsbekämpande myndigheter tillgång till data som lagras i andra dataområden för sina egna innovationsändamål. Tillgång till data som lagras av nationella brottsbekämpande myndigheter och säkerhetsmyndigheter skulle däremot endast bli tillgängliga om det är tillåtet enligt EU-rätten eller nationell lagstiftning. Om enskilda registrerade personer frivilligt gör sina uppgifter tillgängliga för det allmänna bästa, kan nationella brottsbekämpande myndigheter och säkerhetsmyndigheter också utnyttja det, men enbart för vetenskaplig forskning.

Arbete pågår också med att förbereda det nya initiativet om **artificiell intelligens (AI),** efter offentliggörandet av vitboken om AI[60]. I vitboken beskrivs de möjligheter som AI-tekniken erbjuder för ökad säkerhet och välbefinnande för invånarna och samhället som helhet, men där identifieras också ett antal risker, som it-hot, personliga säkerhetsrisker eller förlust av uppkopplingen. I de offentliga samråden är deltagarnas främsta oro risken för att AI kränker grundläggande rättigheter och att AI kan leda till diskriminerande resultat[61]. I meddelandet *Att skapa förtroende för människocentrerad artificiell intelligens*[62] betonade kommissionen behovet att göra AI-systemen motståndskraftiga mot såväl uppenbara angrepp som mer subtila försök att manipulera data eller själva algoritmerna, och att riskreducerande åtgärder vidtas.

Kryptering spelar en grundläggande roll när det gäller att få stark it-säkerhet och ändamålsenligt skydd av grundläggande rättigheter, såsom integritet, inbegripet telehemlighet vid kommunikation, och skydd av personuppgifter och för att skapa förtroende för tjänster och produkter som bygger på krypteringsteknik, som lösningar för digital identitet. Samtidigt kan kryptering användas för att dölja brott från brottsbekämpningen och rättsväsendet, och på så sätt göra det svårare att utreda, upptäcka och lagföra brott. Medlemsstaterna i rådet har efterlyst lösningar som gör det möjligt för brottsbekämpande och rättsliga myndigheter att få laglig tillgång till digital bevisning, med full respekt för integritet, dataskydd och garantier för rättvisa rättegångar[63]. Kommissionen kommer att samarbeta med medlemsstaterna för att identifiera juridiska, operativa och tekniska lösningar för att få laglig tillgång till elektronisk information i krypterade miljöer som upprätthåller kommunikationssäkerheten.

Praktiska åtgärder omfattar bland annat en **dekrypteringsplattform** hos Europol som ska hjälpa brottsbekämpande myndigheter att få laglig tillgång till krypterade uppgifter i objekt som beslagtagits under brottsutredningar[64]. Europeiska utbildningsgruppen för it-brottslighet har tagit fram pilotutbildningsmoduler som kommer att bidra till arbetet i Europeiska unionens byrå för utbildning av tjänstemän inom brottsbekämpning (Cepol). Ett nätverk av medlemsstaternas krypteringsexperter har upprättats för att dela bästa praxis och sakkunskap och för att stödja utvecklingen av en verktygslåda med tekniska och praktiska instrument.

Systemet för digitalt utbyte av elektroniska bevis kommer att erbjuda ett verktyg för säkert, snabbt och effektivt gränsöverskridande utbyte av europeiska utredningsorder, begäranden om ömsesidig hjälp och bevisning i digitalt format. Detta kan successivt utökas

[60] COM(2020) 65 final.

[61] Av uppgiftslämnarna anser 90 respektive 87 % att dessa farhågor är viktiga eller mycket viktiga.

[62] COM(2019) 168 final.

[63] ST 13084 2020 – Rådets resolution om kryptering – Säkerhet genom kryptering och säkerhet trots kryptering.

[64] Det här projektet med en budget på 6 miljoner euro stöds också av kommissionens gemensamma forskningscentrum.

till andra straffrättsliga samarbetsinstrument och dess framtida tillämpningsområde kommer att fastställas i ett lagstiftningsförslag om digitalisering av förfaranden för rättsligt samarbete som planeras till 2021[65].

3. Bekämpa olagligt innehåll på nätet

Radikalisering som leder till våldsbejakande extremism och terrorism är ett mångfacetterat och gränsöverskridande fenomen som har kunnat utnyttja internets snabba tillväxt. Internet används fortfarande för att radikalisera och rekrytera mottagliga grupper. I juli tog Europols enhet för anmälan av internetinnehåll bort 2 000 länkar till terroristrelaterat innehåll – däribland manualer och handledningar om hur man genomför en attack. Internet spelade en viktig roll för radikaliseringen och marknadsföringen av de brott som begicks av dem som var inblandade i attackerna i Frankrike och i Österrike, och beläggen för det belyser ytterligare behovet av en tydlig rättslig ram för att förhindra spridning av terroristrelaterat innehåll på nätet, samtidigt som effektiva skyddsåtgärder för de grundläggande rättigheterna måste upprätthållas. Förhandlingarna mellan Europaparlamentet och rådet om förslaget till **förordning om terrorisminnehåll online**[66] har intensifierats under de senaste veckorna. För att kunna motverka terrorismrelaterat innehåll, däribland innehåll som bidrar till radikalisering, är det viktigt att dessa förhandlingar avslutas med att ett nytt och ändamålsenligt instrument inrättas för beslut om avlägsnande av gränsöverskridande terrorisminnehåll inom högst en timmes tid från det att ordern har mottagits.

Fram till dess fortsätter **EU:s internetforum** att fungera som katalysator för åtgärder, och erbjuder en viktig plattform för medlemsstaterna och näringslivet för att förhindra spridning av terroristrelaterat innehåll på nätet och motverka radikaliserande budskap. Forumet håller på att ta fram en referensförteckning över förbjudna symboler och grupper i medlemsstaterna, som skulle kunna ligga till grund för plattformens innehållsmoderering.

EU:s internetforum har utvidgat sin verksamhet till att också omfatta **sexuella övergrepp mot barn på internet**. Forumet ska tillhandahålla en gemensam plats för utbyte av bästa praxis och identifiering av hinder för både privata och offentliga aktörer, för att öka den ömsesidiga förståelsen och hitta lösningar tillsammans. Det gör det också möjligt med politisk samordning på hög nivå för att maximera effekten och ändamålsenligheten i satsningen. En teknisk expertprocess har inrättats inom ramen för EU:s internetforum bestående av företrädare för den akademiska världen, näringslivet, myndigheter och civilsamhällets organisationer för att kartlägga och preliminärt bedöma möjliga tekniska lösningar för att upptäcka och anmäla sexuella övergrepp på barn i helt krypterad elektronisk kommunikation. Sådana tekniska lösningar bör inte försvaga krypteringen. Den här metoden kompletterar andra delar i kampen mot sexuella övergrepp mot barn, både online och offline, som beskrivs ovan.

Kommissionen har också fortsatt att dela med sig av EU:s expertis och erfarenheter som part i den oberoende rådgivande kommittén till det nyligen inrättade **globala internetforumet för terrorismbekämpning** och, tillsammans med Microsoft, som ledare för arbetsgruppen för krishantering. Tillsammans med Europol fortsatte kommissionen att stödja medlemsstaterna i genomförandet av **EU:s krisprotokoll.** EU-enheten för anmälan av innehåll på internet stod värd för en andra skrivbordsövning den 23 november 2020, för

[65] Meddelandet *Digitalisering av rättskipningen i Europeiska unionen: En verktygslåda med möjligheter*, COM(2020) 710 final, 2.12.2020.

[66] COM(2018) 640 final.

att utarbeta riktlinjer för att förbättra de operativa insatserna och samordningen i realtid mellan medlemsstaterna och leverantörer av onlinetjänster.

I juni 2020 offentliggjorde kommissionen resultaten av den senaste övervakningen av genomförandet av **uppförandekoden för att motverka olaglig hatpropaganda på nätet**[67]. Den visade att i genomsnitt bedömer it-företagen inom 24 timmar 90 % av flaggat innehåll och tar bort 71 % av innehåll som bedöms vara olaglig hatpropaganda. Den visade dock också brister i insynen och återkopplingen till användarna. Genomförandet av uppförandekoden under de senaste fyra åren har också bidragit till reflektioner om hur olagligt innehåll på nätet ska hanteras samtidigt som yttrandefriheten skyddas i det kommande förslaget till en lag om digitala tjänster. I 2020 års tal om tillståndet i unionen meddelade ordförande Ursula von der Leyen också att senast i slutet av 2021 ska kommissionen föreslå att förteckningen över brott på EU-nivå enligt artikel 83.1 i fördraget om Europeiska unionens funktionssätt ska utökas med hatbrott och hatpropaganda[68].

4. *Hybridhot*

Med tanke på hybridhotens föränderliga karaktär inrättade rådet i juli 2019 en **övergripande arbetsgrupp för förstärkning av resiliens och motverkande av hybridhot**. Dess främsta syfte är att stödja strategisk och horisontell samordning bland medlemsstaterna på området staters och samhällens resiliens, förbättra den strategiska kommunikationen och motverka desinformation. Arbetet har omfattat en uppföljning av undersökningarna om hybridrisker[69], och även tittat närmare på hybridhot och desinformation i närliggande partnerländer. Verksamheten i den övergripande arbetsgruppen presenterades i årsrapporten som antogs den 14 september 2020.

I december 2019 antog rådet ”Slutsatser om kompletterande insatser för förstärkning av motståndskraft och motverkande av hybridhot”[70], och uppmanade till en övergripande säkerhetsstrategi för att motverka hybridhot, som fungerar mer strategiskt, samordnat och enhetligt inom alla relevanta politikområden. Två uppföljningsåtgärder vidtogs i juli 2020. Först förberedde kommissionen och utrikestjänsten en **kartläggning av åtgärder och dokument som rör EU:s insatser mot hybridhot**[71]. Kartläggningen ger en övergripande inventering av åtgärder för att motverka hybridhot på EU-nivå och motsvarande policydokument. Den fungerar som utgångspunkt för att skapa en begränsad digital plattform som enda kontaktpunkt för alla åtgärder, all politik och alla lagstiftningsdokument som rör hybridhot, liksom relevanta studier. Sedan undersöktes i den senaste **årsrapporten om att motverka hybridhot**[72] genomförandet som omfattar lägesbild, uppbyggnad av resiliens, beredskap och krishantering, samt internationellt samarbete och särskilt samarbete mellan EU och Nato när det gäller att motverka hybridhot. Även om vissa framsteg noteras i rapporten vad gäller samordning på EU-nivå, kräver den helt nya omfattningen och mångfalden av hybridhot i dag ytterligare åtgärder på

---

67 https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en.

68 Beskrivs också mer detaljerat i hbtqi-jämlikhetsstrategi för 2020–2025 (COM(2020) 698).

69 Åtgärd 1 i 2016 års gemensamma ram för att motverka hybridhot, se JOIN/2016/018.

70 Rådets slutsatser 14972/19.

71 SWD(2020) 152 Joint Staff Working Document, *Mapping of measures related to enhancing resilience and countering hybrid threats*.

72 SWD(2020) 153 Joint Staff working document, *Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats*.

EU-nivå för att integrera den externa och interna dimensionen i ett smidigt flöde och stödja medlemsstaternas satsningar för att motverka hybridhot och stärka sin resiliens.

Parallellt pågår arbete med genomförandet av de åtgärder som fastställs i den nya säkerhetsstrategin för att integrera hybridhänsyn i det politiska beslutsfattandet, utveckla en begränsad onlineplattform, fastställa utgångsvärden för sektorspecifik motståndskraft mot hybridhot och effektivisera informationsflödena för att ytterligare öka omvärldsuppfattningen[73]. Detta bygger på **EU:s gemensamma enhet för hybridhot** som inrättades inom ramen för EU:s underrättelse- och lägescentral (EU Intcen), EU:s främsta kontaktpunkt för hybridhotbedömningar. Enheten har hittills utarbetat över 180 skriftliga rapporter om hybridhot och cyberhot. Ett av enhetens projekt är **Analys av hybridtendenser**[74] som bland annat tillhandahåller återkommande analyser av nya aktörers hybridverksamhet, information om utländsk underrättelseverksamhet mot EU:s medlemsstater, institutioner, partner och intressen och information om statliga och icke-statliga hybridaktörers utnyttjande av covid-19-pandemin.

Samarbetet EU-Nato inom ramen för Warszawa- och Brysselförklaringarna 2016 och 2018 har ytterligare intensifierats, vilket belystes i den femte lägesrapporten från juni 2020, med samverkan mellan personal och konkreta resultat på områdena hybridhot, cyberförsvar och kapacitetsuppbyggnad[75]. Det är viktigt att utveckla en gemensam metod för arbetet med utgångsvärden för resiliens mot hybridhot inom alla sektorer, för att motverka risken för splittrade och överlappande strategier, verktyg och åtgärder. Det europeiska kompetenscentrumet för motverkande av hybridhot i Helsingfors deltog också i detta samarbete. Samarbetet med Nato har intensifierats under covid-19-krisen, bland annat om pandemirelaterad desinformation och för att motverka fientlig informationsverksamhet.

I allmänhet har covid-19-pandemin framhävt de snabbt föränderliga riskerna med **desinformation** och den verkliga risken för människors liv[76]. Den 10 juni 2020 antog kommissionen och utrikesrepresentanten ett **gemensamt meddelande om covid-19 och desinformation**[77] för att framhålla de särskilda riskerna med desinformation om covid-19 och vilka åtgärder som bör vidtas. Detta omfattade åtgärder av de stora onlineplattformarna för att utveckla strategier för att motverka hotet, intensifierad övervakning av plattformarnas verksamhet liksom ett särskilt samarbete genom utrikestjänstens system för tidig varning. Pandemin har lett till ökade insatser för att bekämpa desinformation, och till ökad medvetenhet hos allmänheten. Under första halvan av 2020 har 1963 nya fall av Kremlvänlig desinformation lagts till i den offentliga databasen **EUvsDisinfo**, varav närmare en tredjedel rörde covid-19-infodemin. Från mitten av mars till slutet av april 2020 besökte över 10 000 personer varje dag webbplatsen och det totala antalet besökare

[73] Den 26 november 2020 förslog det gemensamma forskningscentrumet en ny ram för att öka medvetenheten om hot: https://ec.europa.eu/jrc/en/news/jrc-framework-against-hybrid-threats

[74] Analysen av hybridtendenser är ett verktyg som ska användas tillsammans med nationella system för att övervaka omfattningen av och intensiteten i hybridhot på områden som politik/diplomati, försvar, ekonomi, information, underrättelser, it, samhälle, energi och infrastruktur.

[75] Samarbete mellan personal på området it-säkerhet och cyberförsvar har ytterligare intensifierats genom arbete med konsekventa begrepp och doktriner, övningar, informationsutbyte och ömsesidiga briefingar.

[76] Till de verkliga konsekvenser hör bland annat en anlagd brand i teleinfrastruktur och vilseledande hälsoinformation med direkta konsekvenser.

[77] JOIN(2020) 8, Gemensamt meddelande: Gripa in mot covid-19-desinformation – Kolla fakta.

ökade med 400 % jämfört med samma period 2019. EU:s insatser omfattade riktade informationskampanjer[78] och gav faktainformation om pandemin.

Erfarenheterna från detta har beaktats vid utarbetandet av **EU:s handlingsplan för demokrati** som antogs den 2 december 2020[79]. I den beskrivs de första stegen mot att förstärka resiliensen för EU:s demokratiska struktur genom att främja fria och rättvisa val, arbeta för fria och oberoende medier och bekämpa desinformation. Den sista aspekten kommer att bygga på 2018 års handlingsplan mot desinformation[80] som grund för ökade EU-åtgärder för att bekämpa desinformation och för att engagera nyckelaktörer i civilsamhället och det privata näringslivet. Den förebådar också nästa steg med **uppförandekoden om desinformation**, efter bedömningen av kodens ändamålsenlighet i september 2020[81]. Koden har varit ett viktigt och nödvändigt steg mot att skapa ett mer öppet och ansvarsfullt ekosystem av onlineplattformar, men skulle kunna bli ännu effektivare med enhetliga definitioner, konsekventare genomförande och fler åtgärder för att hantera specifika områden såsom riktade budskap på individnivå (micro-targeting). Ett annat viktigt verktyg som EU nu har till sitt förfogande är **det europeiska observatoriet för digitala medier,** som är i drift sedan juni 2020. Det sammanför viktiga aktörer som arbetar med desinformation, som faktagranskare och forskare.

IV SKYDDA EU FRÅN TERRORISM OCH ORGANISERAD BROTTSLIGHET

1. *Terrorism och radikalisering*

Den senaste tidens attacker har återigen visat att terroristhotet i EU fortfarande är akut. Efter mordet på en lärare i Conflans-Sainte-Honorine den 16 oktober 2020 dödades ytterligare tre personer i kyrkan Notre-Dame i Nice den 29 oktober. Den 2 november dödades fyra människor vid en terroristattack i Wien och 23 skadades. Den 13 november antog rådet ett gemensamt uttalande av EU:s inrikesministrar om den senaste tidens terroristattacker i Frankrike och Österrike[82]. Dessa aktuella jihadistinspirerade attacker sammanfaller med ett växande hot från våldsbejakande högerextremister och andra former av terrorism.

För att ytterligare stödja EU-länderna i kampen mot terrorism och radikalisering antar kommissionen i dag en **EU-agenda för terrorismbekämpning**[83]. Agendan bygger på befintliga strategier och instrument och kommer att stärka EU:s insatser för att bättre förutse hot och risker, förebygga radikalisering och våldsbejakande extremism, skydda människor och infrastruktur (bland annat genom säkerhet vid de yttre gränserna) och effektivt följa upp attacker. I agendan beskrivs också hur man kan gå vidare för att förbättra brottsbekämpningen och det rättsliga samarbetet, samt användningen av teknik och utbyte av relevant information i hela EU, även för dem som utför kontroller vid de yttre gränserna. Genomförandet och efterlevnaden av lagstiftningen måste prioriteras.

---

78 Till exempel lanserades kampanjen ”Tänk efter innan du delar” för att ge råd om hur man kan begränsa spridningen av desinformation till unga målgrupper och informationsförmedlare i EU:s östliga partnerskapsländer. Den hade över 500 000 visningar på sociala medier.

79 COM(2020) 790 final.

80 JOIN(2018) 36 Gemensamt meddelande, Handlingsplan mot desinformation.

81 SWD(2020) 180.

82 Gemensamt uttalande från EU:s inrikesministrar om den senaste tidens terroristattacker i Europa, 13.11.2020,
12634/20.

83 COM(2020) 795 final.

Förebyggande är avgörande i kampen mot terrorism. EU:s insatser för att **förebygga radikalisering** bygger på de solida erfarenheter som hittills gjort med stöd till yrkesverksamma på fältet och till beslutsfattare. Den 24 november antog kommissionen en ny **handlingsplan för integration och inkludering**[84]. I kampen mot radikalisering är det mycket viktigt att försöka föra samman olika grupper i samhället. Ett mer sammanhållet och inkluderande samhälle kan bidra till att förhindra spridning av extremistiska ideologier som kan leda till terrorism och våldsam extremism. Stödet till **nätverket för kunskapsspridning om radikalisering** omfattar ytterligare ett kontrakt på 30 miljoner euro i januari 2020 för de kommande fyra åren av hjälp till yrkesverksamma på fältet, samt extra stöd till beslutsfattare och forskare. Dessa och andra instrument, såsom **EU:s internetforum**, kommer att göra det möjligt för kommissionen att ta itu med de prioriterade åtgärder som lyfts fram i de strategiska riktlinjerna för 2021, som utvecklats tillsammans med medlemsstaterna, om en samordnad EU-strategi för förebyggande av radikalisering. De kompletteras med åtgärder i agendan för terrorismbekämpning för att motverka extremistiska ideologier på nätet, öka insatserna i fängelser och för rehabilitering och återanpassning, även för utländska terroriststridande. Dessutom ska stödet till lokala aktörer stärkas och våra samhällen göras mer motståndskraftiga.

Direktivet om bekämpande av terrorism[85], som antogs i mars 2017, är det viktigaste straffrättsliga instrumentet på EU-nivå för att bekämpa terrorism. Det fastställer miniminormer för att definiera terroristbrott och terrorismrelaterade brott, och likaså för påföljder, samtidigt som det ger offer för terrorism rätt till skydd, stöd och hjälp. Den 30 september 2020 antog kommissionen en rapport[86] med en bedömning av de åtgärder som medlemsstaterna har vidtagit för att följa direktivet. Slutsatsen är att införlivandet i nationell lagstiftning har bidragit till att stärka medlemsstaternas straffrättsliga system i fråga om terrorism och de rättigheter som offer för terrorism har, men att det fortfarande finns luckor. Till exempel straffbelägger inte alla medlemsstater i sin nationella lagstiftning alla de gärningar som anges i direktivet som terroristbrott, och inte alla har infört bestämmelserna om straffbeläggning av resor för terrorismändamål och finansiering av terrorism samt stöd till offer. En utvärderingsrapport om direktivet kommer att antas senare under 2021.

EU fortsätter att arbeta för att hjälpa medlemsstaterna att motverka terroristattacker och stödja genomförandet av bestämmelserna. Förordningen om saluföring och användning av **sprängämnesprekursorer** som antogs i juni 2019[87] kommer att börja tillämpas den 1 februari 2021. För att hjälpa nationella myndigheter och den privata sektorn att genomföra förordningen offentliggjorde kommissionen i juni 2020 en uppsättning riktlinjer[88]. Dessutom inrättade kommissionen i juni 2020 ett program[89] för att övervaka förordningens resultat och effekter.

I november 2019 uppmanade kommissionen medlemsstaterna att bedöma genomförandet av 2017 års handlingsplan för att förbättra beredskapen mot **kemiska, biologiska, radiologiska och nukleära säkerhetsrisker (CBRN-säkerhetsrisker)**[90]. Den

[84] COM(2020) 758.
[85] Direktiv (EU) 2017/541.
[86] COM(2020) 619.
[87] Förordning (EU) 2019/1148.
[88] Kommissionens tillkännagivande – Riktlinjer för genomförandet av förordning (EU) 2019/1148 om saluföring och användning av sprängämnesprekursorer, EUT C 210, 24.6.2020, s. 1.
[89] SWD(2020) 114 final.
[90] COM(2017) 610 final.

övergripande slutsatsen var att en majoritet av åtgärderna har genomförts. I början av 2020 upprättade kommissionen i samarbete med nationella experter en förteckning över högriskkemikalier som ger anledning till oro. Denna låg sedan till grund för kontakter med utrustningstillverkare i syfte att förbättra detektionskapaciteten. Nyligen inledde kommissionen en undersökning för att se om det är möjligt att begränsa tillgången till vissa av dessa kemikalier. Arbete pågår också som en del av unionens civilskyddsmekanism, och ytterligare kapacitet för att ingripa mot CBRN-säkerhetsrisker diskuteras med medlemsstaterna inom områdena dekontaminering, detektion, övervakning samt lagring.

Den 12 oktober 2020 beslutade rådet att förlänga sitt sanktionssystem mot spridning och användning av kemiska vapen med ett år[91], så att EU kan införa restriktiva åtgärder mot personer och enheter som deltar i utvecklingen och användningen av kemiska vapen. Den 14 oktober 2020 antog rådet restriktiva åtgärder mot sex personer och en enhet som varit inblandade i mordförsöket på Aleksej Navalnyj, som den 20 augusti 2020 förgiftades med ett nervgift av typen *novitjok* i Ryssland[92].

Finansiell information är också avgörande för att identifiera terroristnätverk, eftersom terrorister är beroende av finansiering för resor, utbildning och utrustning, och insatser för **finansiera kampen mot terrorism** är avgörande för terrorismbekämpningsutredningar. Några av de viktigaste åtgärderna är utnyttjandet av befintliga verktyg och underrättelser till deras fulla potential, korrekt genomförande av internationellt överenskomna standarder och hantering av de utmaningar som ny teknik och plattformar för sociala medier[93] löpande medför (se nedan).

Transportnätet har varit och fortsätter att vara ett mål för terrorism. EU:s insatser omfattar en riskbaserad bedömningsmetod för att skydda luftfartssektorn[94]. Konfliktområden utgör en allvarlig risk för den civila luftfarten, och utbyte av information och riskbedömning är avgörande för att minska riskerna[95]. EU:s informationssystem för **riskbedömning av konfliktområden** ses som bästa praxis, och internationella standarder för informationsutbyte har införlivats i EU-lagstiftningen[96]. På grundval av de erfarenheter som gjorts på området civil luftfart har kommissionen utvidgat den riskbedömningsbaserade strategin till andra transportsätt. Genomförandet av EU:s **handlingsplan för järnvägssäkerhet**[97] pågår, och kan bygga på sakkunskap från EU-plattformen för järnvägspassagerare, en specialiserad expertgrupp som inrättats av kommissionen. På sjöfartsområdet tillämpas den riskbedömningsbaserade metoden allmänt, och kommissionen samarbetar med medlemsstaterna och berörda parter för att öka passagerarnas säkerhet. Detta har införlivats i **EU:s strategi för sjöfartsskydd** och dess **handlingsplan**, som reviderades 2018. Den omfattar även en säkerhets- och

[91] Rådets beslut (Gusp) 2020/1466 av den 12 oktober 2020 om ändring av beslut (Gusp) 2018/1544.

[92] Rådets beslut (Gusp) 2020/1482 av den 14 oktober 2020 och rådets genomförandeförordning (EU) 2020/1480.

[93] Enligt vad som fastställdes av EU i november 2019 vid ministerkonferensen ”No Money For Terror” om finansiering av terrorismbekämpning, som Australien stod värd för.

[94] Den integrerade riskbedömningsprocessen för luftfartsskydd i EU stöder beslutsprocessen på området flygfraktsäkerhet, standarder för luftfartsskydd och risker för den civila luftfarten i konfliktområden.

[95] Den tragiska nedskjutningen av Ukraine International Airlines flyg 752 den 8 januari 2020 visade återigen vikten av informationsutbyte och riskbedömning för säkerheten inom den civila luftfarten.

[96] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R1583

[97] COM(2018) 470 final.

försvarsdimension. Detta anges i den senaste genomföranderapporten, som antogs och offentliggjordes den 23 oktober 2020[98].

Europol ger stöd till medlemsstaterna i utredningar som rör terrorism genom det **europeiska centrumet mot terrorism**. Medlemsstaternas begäranden om operativt stöd till det europeiska centrumet mot terrorism fortsatte att öka i antal, och centrumet deltar nu i nästan alla större terrorismbekämpningsutredningar. Under 2019 stödde Europol totalt 632 olika insatser på området terrorismbekämpning. Medlemsstaternas utredare har också visat en ökande uppskattning av detta arbete, från en nöjdhetsnivå på 8/10 under 2018 till 9,1/10 under 2019. Centrumet har sammanlagt samordnat 18 insatsdagar under 2019[99].

Eurojust har också gett stöd till 116 terrorismutredningar under 2019 och 2020. Det pågående arbetet kommer att utmynna i ett lagstiftningsförslag om informationsutbyte vid fall av digital gränsöverskridande terrorism, för att utveckla det register för bekämpning av terrorism som inleddes 2019[100] samt för att utvidga arbetet kring höger- och vänsterextremistgrupper.

Senast den 30 juli 2020 förnyade rådet EU:s förteckning över de personer, grupper och enheter som omfattas av restriktiva åtgärder i syfte att bekämpa terrorism. Den senaste förteckningen omfattar 14 personer och 21 enheter. Samma dag införde rådet restriktiva åtgärder mot en person inom ramen för sanktionssystemet för terrorismbekämpning mot Isil/Daish/al-Qaida. För närvarande är fem personer enskilt uppförda på förteckningen enligt detta system, som förnyades med ett år den 19 oktober 2020[101].

En viktig fråga i terrorismbekämpningspolitiken är de hot som **utländska terroriststridande** för närvarande utgör i Syrien och Irak. Med full respekt för medlemsstaternas primära behörighet i dessa frågor kan stöd och samarbete på EU-nivå hjälpa medlemsstaterna att hantera gemensamma utmaningar: lagföring av personer som har begått terroristbrott, förhindrande av oupptäckt inresa till Schengenområdet och återintegrering och rehabilitering av återvändande utländska terroriststridande. Kommissionen har till exempel ett nära samarbete med medlemsstaterna och viktiga partnerländer för att se till att bevis från slagfältet delas och används effektivt för identifiering, upptäckt vid EU:s gränser och lagföring. 2020 års memorandum om bevis från slagfältet[102], som offentliggjorts av Eurojust, visar att det visserligen är svårt att få fram sådana uppgifter och se till att de uppfyller kriterierna för tillåten bevisning, men att de kan bidra till att ställa misstänkta terrorister inför rätta.

Kommissionen understöder också en dialog med medlemsstaterna och humanitära aktörer för att ge en heltäckande och faktabaserad översikt över situationen i de nordöstra syriska lägren där europeiska familjemedlemmar till utländska terroriststridande finns. Särskild uppmärksamhet ägnas åt barnens situation i de syriska lägren. Kommissionen hjälper också medlemsstaterna att utbyta erfarenheter om nationella åtgärder och mekanismer för att bättre hantera **rehabilitering och återintegrering** av återvändande utländska terroriststridande samt barn. Nätverket för kunskapsspridning om radikalisering genomför

---

98 Rapport från kommissionens avdelningar, Europeiska utrikestjänsten och Europeiska försvarsbyrån om genomförandet av den reviderade EU-strategin för sjöfartsskydd, SWD(2020) 252.

99 Konsoliderad årlig verksamhetsrapport för 2019, Europol, 9.6.2020.

100 Registret förvaltas av Eurojust dygnet runt och ger proaktivt stöd till nationella rättsliga myndigheter. Sådan centraliserad information ska hjälpa åklagare att samordna sig mer aktivt och att identifiera misstänkta personer eller nätverk som utreds i specifika fall med potentiella gränsöverskridande konsekvenser.

101 Rådsbeslut (Gusp) 2020/1132, 2020/1126 och 2020/1516.

102 https://www.eurojust.europa.eu/eurojust-memorandum-battlefield-evidence-0

också studiebesök och ger skräddarsydda råd för att bättre kunna hantera svårigheterna med dömda återvändande personer, särskilt efter deras frigivning från fängelset, samt familjers och lokalsamhällens roll i återintegreringsinsatserna.

Partnerskap för terrorismbekämpning och samarbete med tredjeländer och partner i EU:s grannskap är också avgörande för att förbättra säkerheten inom EU och bättre koppla samman de inre och yttre dimensionerna av EU:s säkerhetspolitik. Rådet har efterlyst en ytterligare förstärkning av EU:s externa engagemang[103] i kampen mot terrorism med fokus på västra Balkan, Nordafrika och Mellanöstern, Sahelregionen, Afrikas horn och Asien. I detta arbete utnyttjar man maximalt alla verktyg för yttre åtgärder, bland annat dialoger på hög nivå om terrorismbekämpning och nätverket av 17 **experter på terrorismbekämpning/säkerhet**[104] vid EU:s delegationer, vilket tillhandahåller löpande stöd, underlätta samarbetet och främjar kapacitetsuppbyggnaden. För närvarande pågår en diskussion om möjligheten att stärka och utvidga detta nätverk.

Den gemensamma handlingsplanen för terrorismbekämpning för **västra Balkan** från 2018 och de åtföljande bilaterala överenskommelser som undertecknades 2019 med varje partner[105] är inriktade på en region av central betydelse för gemensamma säkerhetsmål och för skyddet av människor som lever i EU. Vid ministerforumet för rättsliga och inrikes frågor mellan EU och länderna på västra Balkan den 22 oktober 2020 bekräftade EU och partnerna på västra Balkan sitt åtagande att genomföra målen i den gemensamma handlingsplanen även efter 2020[106]. Samarbetet med västra Balkan omfattar hantering av det pågående återvändandet för utländska terroriststridande och deras familjemedlemmar samt en ytterligare integrering i insatser mot radikalisering. EU upprätthåller också regelbundna kontakter om terrorismbekämpning med **Mellanöstern, Nordafrika och Centralasien**[107]. Arbetet med **Centralasien** har inriktats på kemiska, biologiska, radiologiska och nukleära hot. Den gemensamma samarbetskommittén för **EU och Gulfstaternas samarbetsråd** sammanträdde den 25 juni 2020 och behandlade frågor som motverkande av radikalisering och bekämpning av terrorismfinansiering och penningtvätt samt it-säkerhet och samarbete med Europol. I slutet av 2019 samarbetade EU med Nato med den första revisionen någonsin av kemiska, biologiska, radiologiska och nukleära hot i en av Gulfstaterna. I slutet av 2019 hade totalt cirka 465 miljoner euro avsatts för pågående projekt om terrorismbekämpning och förebyggande av våldsbejakande extremism utanför EU, en ökning med 15 % jämfört med föregående år.

EU har också fortsatt att fördjupa samarbetet med **Förenta nationerna** om terrorismbekämpning[108], särskilt med FN:s kontor för terrorismbekämpning och det

---

[103] Rådets slutsatser (8868/20) om EU:s yttre åtgärder för att förebygga och bekämpa terrorism och våldsbejakande extremism (16 juni 2020).

[104] Algeriet, Bosnien och Hercegovina (regionalt för västra Balkan), Tchad (regionalt för Sahel), Etiopien (förbindelse med Afrikanska unionen), Indonesien (regionalt för Sydostasien och förbindelser med Asean-ARF), Irak, Jordanien, Kenya (regionalt för Afrikas horn), Kirgizistan (regionalt för Centralasien), Libanon, Libyen, Marocko, Nigeria, Pakistan, Saudiarabien, Tunisien och Turkiet.

[105] Serbien, Nordmakedonien, Bosnien och Hercegovina, Kosovo*, Albanien och Montenegro.

[106] Gemensamt pressuttalande: https://www.consilium.europa.eu/en/press/press-releases/2020/10/23/joint-press-statement-eu-western-balkans-ministerial-forum-on-justice-and-home-affairs/pdf

[107] Åtgärder mot terrorism betonades till exempel i den nya EU-strategin för Centralasien.

* Denna beteckning påverkar inte ståndpunkter om Kosovos status och är i överensstämmelse med FN:s säkerhetsråds resolution 1244/1999 och med Internationella domstolens utlåtande om Kosovos självständighetsförklaring.

[108] Under 2019 undertecknades en ram för samarbete mellan EU och FN om terrorismbekämpning https://eeas.europa.eu/sites/eeas/files/2019042019_un-eu_framework_on_counter-terrorism.pdf .

verkställande direktoratet för terrorismbekämpning, bland annat genom årliga högnivådialoger och senast genom aktivt deltagande i FN:s virtuella vecka mot terrorism sommaren 2020. Kommissionen har också noga följt överläggningarna om en översyn av definitionen av terroristbrott i **Europarådets** konvention om förebyggande av terrorism, och uppmuntrat till en nära anpassning till definitionerna i EU-lagstiftningen. Ett fortsatt gott samarbete mellan **Nato** och EU kan också noteras på området terrorismbekämpning och kemiska, biologiska, radiologiska och nukleära material. Det omfattar informationsutbyte om kapacitetsuppbyggnad för att undvika dubbelarbete och säkerställa komplementaritet.

2. Bekämpa organiserad brottslighet

Den organiserade brottsligheten ökar, blir allt mer gränsöverskridande och utspelar sig allt mer på nätet.

Europol, hotbildsbedömningar avseende den grova organiserade brottsligheten (Socta 2017)

Kommissionens åtgärder har omfattat kampen mot narkotika, olagliga skjutvapen, ekonomisk brottslighet, olaglig import av kulturföremål, människohandel och miljöbrott, och har understött medlemsstaternas brottsbekämpande och rättsliga myndigheter samt partner i grannskapet. Samarbetet med tredjeländer – särskilt i grannskapet, t.ex. västra Balkan – och internationella organisationer, däribland FN:s kontor mot narkotika och brottslighet[109] har också varit av avgörande betydelse[110].

Under 2019 mottog och behandlade **Europols centrum för grov och organiserad brottslighet** nästan 55 000 operativa bidrag, vilket är en ökning med 12 % jämfört med 2018. Centrumet gav stöd till länder i 726 fall[111]. Det är också mycket viktigt att i alla medlemsstater fullt ut införliva EU:s rättsliga ram mot organiserad brottslighet[112], som syftar till att harmonisera medlemsstaternas lagar om straffbeläggande av gärningar som har samband med deltagande i en kriminell organisation, och fastställer påföljder för dessa brott. Kommissionen har inlett en studie för att analysera olika sätt att förbättra denna lagstiftning. Ytterligare åtgärder för att intensifiera kampen mot organiserad brottslighet i EU kommer att sammanföras i den EU-agenda mot organiserad brottslighet som ska antas under första kvartalet 2021.

---

[109] En högnivådialog mellan EU och UNODC ägde rum den 8 december 2020.

[110] I slutet av 2019 avsattes cirka 830 miljoner euro till pågående insatser mot organiserad brottslighet utanför EU.

[111] Konsoliderad årlig rapport för 2019, Europol, juni 2020.

[112] Rambeslut 2008/841/RIF.

Frysning och förverkande av vinning av brott hör till de effektivaste sätten att bekämpa organiserad brottslighet. Det nya **europeiska centrumet för bekämpning av finansiell och ekonomisk brottslighet** (EFECC), som inrättades vid Europol i juni 2020, kommer att stärka det operativa stödet till medlemsstaterna och EU-organ på området för finansiell och ekonomisk brottslighet och främja systematisk användning av finansiella utredningar. I syfte att stödja EU:s insatser för effektivare identifiering, frysning och förverkande av tillgångar som härrör från brott antog rådet i juni 2020 slutsatser om förstärkta finansiella utredningar för att bekämpa grov och organiserad brottslighet[113]. Under 2021 kommer kommissionen att se över lagstiftningen om frysning och förverkande av vinning av brott[114] och om kontor för återvinning av tillgångar[115].

Kampen mot organiserad brottslighet kräver skyddsåtgärder för att säkerställa att brottsbekämpande verksamhet kan fungera effektivt inom väsentliga gränser, såsom skydd av personuppgifter. Dataskyddsdirektivet från 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott[116] skyddar den grundläggande rätten till uppgiftsskydd när personuppgifter används av straffrättsliga myndigheter för brottsbekämpande ändamål. Det säkerställer att personuppgifter om brottsoffer, vittnen och misstänkta är vederbörligen skyddade, och underlättar gränsöverskridande samarbete i kampen mot brottslighet och terrorism. Tidsfristen för införlivandet av dataskyddsdirektivet för brottsbekämpning löpte ut den 6 maj 2018. I dag har de flesta medlemsstaterna antagit lagstiftning som införlivar direktivet. Några överträdelseförfaranden pågår dock fortfarande[117]. Kommissionen håller för närvarande på att bedöma om de nationella införlivandelagarna är förenliga med direktivet.

Kampen mot olaglig narkotika

I juli 2020 antog kommissionen en ny **EU-agenda och handlingsplan mot narkotika 2021-2025**[118], som bygger på de nuvarande EU-strategierna för narkotika[119]. Här fastställs den politiska ramen och prioriteringarna för de kommande fem åren. Agendans främsta fokus är följande: 1) Förbättrade säkerhetsåtgärder mot olaglig handel med narkotika, från organiserade kriminella grupper till förvaltningen av de yttre gränserna och olaglig distribution och produktion. 2) Utökat förebyggande arbete, bland annat genom att öka medvetenheten om de skadliga effekterna av droger, i synnerhet kopplingarna mellan narkotikamissbruk, våld och andra former av brottslighet. 3) Bekämpning av narkotikarelaterade skador genom tillgång till behandling, risk- och skademinskning och ett balanserat tillvägagångssätt avseende narkotikaproblemet i fängelser. Den 30 november 2020 antog kommissionen också en utvärdering av EU:s politik för narkotikaprekursorer som visar att det krävs ytterligare åtgärder för att förhindra att organiserade kriminella

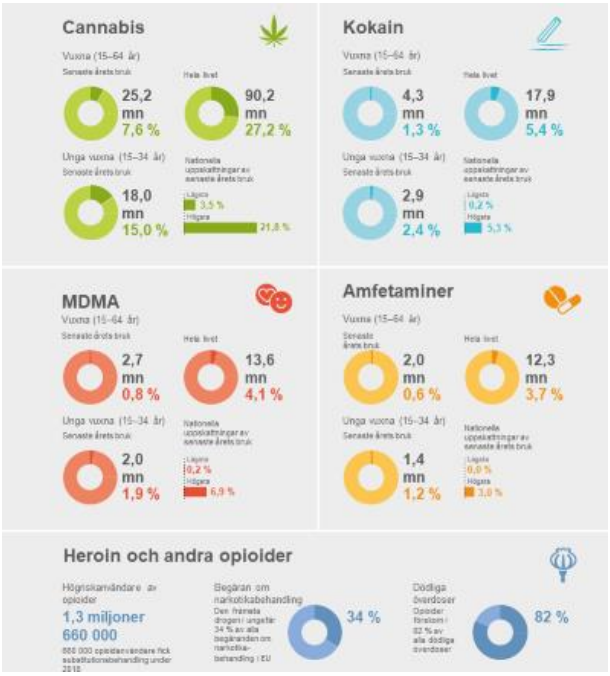
[113] Rådets slutsatser 8927/20.
[114] Direktiv 2014/42/EU.
[115] Rådets beslut 2007/845/RIF.
[116] Direktiv (EU) 2016/680 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott.
[117] Tre medlemsstater (Tyskland, Slovenien och Spanien) har ännu inte anmält ett fullständigt införlivande trots överträdelseförfaranden. Kommissionen väckte talan vid domstolen i ett ärende om bristande införlivande och riktade i maj 2020 kompletterande motiverade yttranden till de två andra medlemsstaterna för att de inte hade införlivat direktivet fullt ut.
[118] COM(2020) 606.
[119] EU:s narkotikastrategi 2013–2020 och EU:s handlingsplan mot narkotika 2017–2020.

grupper i EU får tillgång till de kemikalier de behöver för att framställa olaglig syntetisk narkotika[120].

EU har också finansierat konkreta projekt för att stärka kampen mot narkotika, t.ex. civilsamhällesforumet mot narkotika. Den europeiska narkotikarapporten 2020 från Europeiska centrumet för kontroll av narkotika och narkotikamissbruk, som offentliggjordes den 22 september 2020[121], visar den senaste utvecklingen när det gäller narkotikamissbruk och marknadsutvecklingar i EU, Turkiet och Norge. Den visar på en ökning av kokaintillgången, med rekordhöga beslag på 181 ton, en nästan fördubbling av heroinbeslag till 9,7 ton och hög tillgång på narkotika med hög renhetsgrad i EU. Där undersöks också de nya syntetiska opioider som dykt upp och som vållar särskilda hälsoproblem, och de utmaningar som orsakas av covid-19-pandemin.

Arbetet mot narkotika fortskrider på flera olika nivåer. **Lagstiftningspaketet om nya psykoaktiva ämnen** antogs hösten 2017[122] och blev fullt tillämpligt i november 2018. Fem medlemsstater är fortfarande föremål för överträdelseförfaranden[123]. Den första delegerade akten för att definiera ett nytt psykoaktivt ämne (isotonitazen) som narkotika har nu antagits[124].

På den **internationella arenan** har EU varit aktivt i FN:s narkotikakommission[125], särskilt för att uppdatera förteckningen över nya psykoaktiva ämnen[126] och för att omförteckna cannabis och cannabisrelaterade ämnen[127]. Två nya dialoger om narkotika med Kina och Iran har godkänts av rådet[128], och Europeiska centrumet för kontroll av narkotika och narkotikamissbruk har gått vidare med samarbetsavtal med tredjeländer[129].



Kampen mot ekonomisk brottslighet

Ny lagstiftning har antagits för att stärka kampen mot ekonomisk brottslighet och penningtvätt. Direktivet för att underlätta användning av finansiell information och andra uppgifter för att förebygga,

[120] COM(2020) 768 final, 30.11.2020.
[121] European Drug Report 2020: Trends and Developments, EMCDDA, 22.9.2020.
[122] Förordning (EU) 2017/2101 och direktiv (EU) 2017/2103,
[123] Österrike, Finland, Irland, Portugal och Slovenien.
[124] C/2020/5897. EUT L 379, 13.11.2020, s. 55.
[125] Ett styrande organ för FN:s drog- och brottsbekämpningsbyrå (UNODC).
[126] COM(2019) 631.
[127] COM(2019) 624 och COM(2020) 659.
[128] Toppmötet mellan EU och Kina den 16–17 juli 2018 i Peking resulterade i en överenskommelse om att inleda en årlig dialog mellan EU och Kina om narkotika. Formerna för den framtida dialogen bekräftades av Coreper den 30 oktober 2019. Rådet godkände inledandet av en ny dialog mellan EU och Iran om narkotika den 5 mars 2020.
[129] Kommissionens yttrande om utkastet till samarbetsavtal med Kosovo, antaget den 14 april 2020, och för Serbien antaget den 16 december 2019.

upptäcka, utreda eller lagföra vissa brott antogs 2019 och gav brottsbekämpande myndigheter och kontor för återvinning av tillgångar åtkomst till nationella centraliserade bankkontoregister i syfte att bekämpa grov brottslighet. Direktivet syftar också till att förbättra samarbetet mellan brottsbekämpande myndigheter och finansunderrättelseenheter och underlätta informationsutbytet mellan dessa enheter. I juni 2020 offentliggjorde kommissionen rapporten ”Återvinning av tillgångar och förverkande: Åtgärder för att se till att brott inte lönar sig”[130]. I den redogjordes för möjligheterna till större harmonisering av systemen för återvinning av tillgångar[131] för att modernisera EU-lagstiftningen om återvinning av tillgångar och stärka de nationella myndigheternas kapacitet att bekämpa organiserad brottslighet. Ytterligare analys av återvinning av tillgångar har inletts genom en extern studie. Förordningen om ömsesidigt erkännande av beslut om frysning och beslut om förverkande[132] kommer att tillämpas från och med den 19 december 2020 och kommer att avsevärt förbättra samarbetet mellan medlemsstaterna.

I maj 2020 antog kommissionen en **handlingsplan för en övergripande unionspolitik för förebyggande av penningtvätt och finansiering av terrorism**[133] i syfte att stärka EU-ramen. Den 5 november antog rådet slutsatser om bekämpning av penningtvätt och finansiering av terrorism[134] och uppmanade särskilt kommissionen att arbeta för antagandet av ett enhetligt regelverk, inrättandet av en oberoende tillsynsmyndighet och samordningen av finansunderrättelseenheter. I linje med rådets slutsatser om förstärkta finansiella utredningar[135] undersöker kommissionen också behovet av att koppla samman centraliserade bankkontoregister, vilket avsevärt skulle påskynda tillgången till information om bankkonton för finansunderrättelseenheter och brottsbekämpning. Parallellt med detta fortsätter ansträngningarna för att se till att medlemsstaterna effektivt genomför de senaste EU-standarderna. Reglerna i det 5:e penningtvättsdirektivet syftar till att säkerställa ökad insyn i företagens ägarstrukturer. Tidsfristen för införlivande löpte ut den 1 januari 2020 och kommissionen har inlett överträdelseförfaranden mot 16 medlemsstater[136]. En annan viktig åtgärd är den nya kontantkontrollförordningen[137] som antogs i oktober 2018 och börjar tillämpas den 3 juni 2021. Den ska förbättra det befintliga systemet för kontroller av kontanta medel som förs in i eller ut ur EU, och tillämpningsföreskrifter håller på att utarbetas.

På det externa planet fortsätter insatserna för att stödja partnerländerna i kampen mot penningtvätt och finansiering av terrorism. I detta sammanhang spelar utrikestjänsten och EU:s delegationer en nyckelroll för att främja och stödja det politiska engagemanget med tredjeländer och internationella organisationer såsom arbetsgruppen för finansiella åtgärder (FATF).

Som ett komplement till detta arbete har kommissionen lanserat en global facilitet för att ge stöd till partnerländer utanför EU som vill inrätta effektiva ramar för bekämpning av penningtvätt och finansiering av terrorism i enlighet med internationella standarder. 20

[130] COM(2020) 2017.
[131] Inbegripet bedömningen av direktiv 2014/42/EU och rådets beslut 2007/845/RIF.
[132] Förordning (EU) 2018/1805.
[133] C(2020) 2800 final.
[134] Rådets slutsatser 12608/20.
[135] Rådets slutsatser 8927/20.
[136] Belgien, Cypern, Estland, Förenade kungariket, Grekland, Irland, Luxemburg, Nederländerna, Polen, Portugal, Rumänien, Slovakien, Slovenien, Spanien, Tjeckien, Ungern och Österrike.
[137] Förordning (EU) 2018/1672.

miljoner euro har avsatts för detta, och syftet är också att uppmuntra samarbete mellan finansiella och rättsliga aktörer på nationell, regional och internationell nivå.

Bekämpa korruption

Korruption är ett brott i sig och en viktig möjliggörande faktor för organiserad brottslighet. Den nyligen inrättade **rättsstatsmekanismen**[138] ska regelbundet övervaka och bedöma förebyggandet och bekämpningen av korruption och medlemsstaternas rättsliga ramar. Den första EU-omfattande rapporten om rättsstatsprincipen antogs den 30 september 2020[139]. Den visade att många medlemsstater har höga standarder för rättsstatsprincipen, men stora utmaningar kvarstår. Rapporten omfattar alla medlemsstater med objektiva och faktiska årliga bedömningar, i syfte att löpande utveckla en större medvetenhet om och förståelse för utvecklingen i de enskilda medlemsstaterna, för att kunna identifiera risker, utveckla möjliga lösningar och rikta stödet i ett tidigt skede. **Europeiska åklagarmyndigheten** ska hantera brott mot EU-budgeten, för närvarande i de 22 deltagande EU-länderna. Den kommer att ha befogenhet att utreda, lagföra och väcka talan mot dem som är ansvariga för brott mot EU:s budget, t.ex. bedrägeri, korruption eller allvarliga gränsöverskridande momsbedrägerier. Europeiska åklagarmyndigheten ska inleda sin verksamhet under första kvartalet 2021[140].

Kommissionen håller för närvarande på att bedöma införlivandet i nationell lagstiftning av bestämmelserna i **direktivet om bekämpande genom straffrättsliga bestämmelser av bedrägeri som riktar sig mot unionens finansiella intressen**[141] och har inlett överträdelseförfaranden mot de medlemsstater som inte har anmält ett fullständigt införlivande[142]. Under 2021 kommer kommissionen att anta en rapport om i vilken utsträckning medlemsstaterna har vidtagit de åtgärder som krävs för att följa direktivet.

Bekämpa olaglig handel med kulturföremål

Huvudsyftet med **förordningen om införsel och import av kulturföremål**[143], som antogs i juni 2019, är att stoppa import till unionen av kulturföremål som olagligen exporterats från ursprungslandet. För att säkerställa ett korrekt genomförande förbereder kommissionen för närvarande antagandet av genomförandebestämmelser, bland annat ett centraliserat elektroniskt system för import av kulturföremål, som kommer att möjliggöra lagring och utbyte av information mellan medlemsstaterna och nödvändiga importformaliteter[144]. En allmän regel om förbud kommer att träda i kraft i slutet av 2020 och ge medlemsstaternas tullmyndigheter rättsliga möjligheter att kontrollera och agera vid transporter som kan innehålla kulturföremål som olagligen exporterats från ursprungslandet.

---

[138] Den europeiska rättsstatsmekanismen erbjuder ett förfarande för dialog om rättsstatsprincipen mellan kommissionen och medlemsstaterna, rådet och Europaparlamentet samt nationella parlament, det civila samhället och andra berörda parter. Rättsstatsrapporterna är kärnan i detta samarbete.

[139] COM(2020) 580.

[140] Rådets genomförandebeslut om utnämning av europeiska åklagare trädde i kraft den 29 juli 2020. De europeiska åklagarna höll sitt första möte den 28 september 2020. Europeiska åklagarmyndigheten kommer snart att ingå samarbetsavtal med Europol, Eurojust och Olaf.

[141] Direktiv (EU) 2017/1371.

[142] Överträdelseförfaranden pågår fortfarande mot Österrike, Irland och Rumänien.

[143] Förordning (EU) 2019/880

[144] Det elektroniska systemet ska vara klart senast den 28 juni 2025. Kommissionen har antagit en första lägesrapport om utvecklingen av det elektroniska systemet för import av kulturföremål. [COM(2020) 342].

Bekämpa olaglig handel med skjutvapen

Den 24 juli 2020 offentliggjorde kommissionen en **ny EU-handlingsplan för 2020–2025 mot olaglig handel med skjutvapen**[145]. Vid en ministerkonferens på hög nivå mellan EU:s och västra Balkans utrikes- och inrikesministerier den 31 januari 2020 underströks behovet av ökade insatser för att bekämpa olaglig handel med skjutvapen. Handlingsplanen innehåller särskilda åtgärder för att förbättra den rättsliga kontrollen av skjutvapen, kunskapen om det skjutvapenrelaterade hotet, brottsbekämpningssamarbete och internationellt samarbete med fokus på sydöstra Europa. Kommissionen vidtog åtgärder för att se till att det direktiv om kontroll av förvärv och innehav av vapen som antogs i maj 2017[146] införlivas fullt ut av medlemsstaterna. Tio medlemsstater har dock ännu inte anmält att direktivet har införlivats fullt ut[147], och en stor majoritet av medlemsstaterna har inte införlivat den tillhörande genomförandelagstiftningen. Kommissionen har därför inlett överträdelseförfaranden[148] Kommissionen håller också på att göra en detaljerad bedömning av de anmälda införlivandeåtgärderna och kommer att rapportera om genomförandet av direktivet under första halvåret 2021. Kommissionen har även börjat undersöka om den rättsliga ramen för import, export och transitering av skjutvapen[149] behöver moderniseras.

Bekämpa människohandel

I strategin för säkerhetsunionen betonades behovet av att utveckla ett nytt strategiskt tillvägagångssätt för att utrota människohandel inom ramen för agendan

[145] COM(2020)608: denna nya handlingsplan integrerar det fransk-tyska initiativet för västra Balkan, ”Färdplan för en hållbar lösning på olagligt innehav och missbruk av samt olaglig handel med handeldvapen och lätta vapen och ammunition till dessa på västra Balkan senast 2024 ”.

[146] Direktiv (EU) 2017/853. Två genomförandedirektiv av den 16 januari 2019 om tekniska specifikationer för märkning och för signal- och larmvapen var också av stor betydelse.

[147] Dessa är Danmark, Cypern, Luxemburg, Polen, Slovenien, Slovakien, Spanien, Sverige, Tjeckien och Ungern.

[148] 25 förfaranden pågår om detta direktiv (Belgien, Bulgarien, Cypern, Danmark, Estland, Finland, Frankrike, Grekland, Irland, Lettland, Litauen, Luxemburg, Malta, Nederländerna, Polen, Portugal, Rumänien, Slovenien, Slovakien, Spanien, Sverige, Tjeckien, Tyskland, Ungern och Österrike, samt mot Förenade kungariket) och 34 förfaranden löper avseende genomförandedirektiven (direktiv 2019/68 – Belgien, Bulgarien, Cypern, Finland, Grekland, Irland, Italien, Kroatien, Luxemburg, Polen, Rumänien, Slovenien, Spanien, Sverige, Tjeckien, Tyskland, Ungern och Österrike, samt mot Förenade kungariket; direktiv 2019/69 – Bulgarien, Cypern, Finland, Grekland, Irland, Italien, Kroatien, Luxemburg, Nederländerna, Polen, Rumänien, Spanien, Sverige, Slovenien, Tjeckien och Ungern, samt Förenade kungariket).

[149] Reglerat av förordning (EU) nr 258/2012.

mot organiserad brottslighet. Dessutom offentliggjorde kommissionen i oktober 2020, i enlighet med artikel 20 i direktivet mot människohandel[150], sin tredje rapport om de framsteg som gjorts i kampen mot människohandel[151].
Här visas framsteg när det gäller transnationellt samarbete, gränsöverskridande brottsbekämpning och operativa rättsliga åtgärder, men också inrättandet av nationella och transnationella mekanismer för vidareslussning av offer för människohandel och utveckling av kunskapsbasen om människohandel. Medlemsstaterna använder sig i allt högre grad av EU-organ för att utbyta information, genomföra gemensamma åtgärder och gemensamma utredningsgrupper för att bekämpa människohandel både inom och utanför EU[152]. Det operativa samarbetet har gett påtagliga resultat, särskilt inom ramen för den europeiska sektorsövergripande plattformen mot brottshot: under 2019 har detta arbete resulterat i 825 gripanden, 8 824 identifierade misstänkta och identifieringen av 1 307 potentiella offer, däribland 69 barn. 94 organiserade kriminella grupper som var inblandade i dessa brott identifierades eller upplöstes och 1,5 miljoner euro i tillgångar har frysts på bankkonton, företag och webbdomäner. På EU:s dag mot människohandel den 18 oktober 2020 offentliggjorde kommissionen en studie om människohandelns kostnader, och en annan om nationella och gränsöverskridande mekanismer för vidareslussning[153].

Smuggling av migranter

Det europeiska centrumet för människosmuggling har rapporterat en fortsatt ökning av **smuggling av migranter**, främst i västra Balkan och grannländerna, och med sekundära förflyttningar i hela EU. Under 2019 bidrog Europol till att identifiera 14 218 misstänkta som är aktiva inom människohandel[154]. I maj 2020 inrättade Eurojust fokusgruppen för åklagare för människosmuggling som ett viktigt nav för att regelbundet sammanföra de viktigaste rättsliga aktörerna på nationell nivå i EU:s medlemsstater och stödja deras gemensamma operativa insatser[155].

Bekämpa miljöbrott

Miljöbrott omfattar handlingar som överträder miljölagstiftningen och orsakar eller kan orsaka betydande skada eller risk för miljön och människors hälsa[156]. De viktigaste **miljöbrottsområdena** är olagliga utsläpp eller utsläpp av ämnen i luft, vatten eller mark, olaglig handel med vilda djur och växter, olaglig handel med ozonnedbrytande ämnen och olaglig transport eller dumpning av avfall. Den nyligen genomförda utvärderingen av direktivet om miljöbrott[157] visade att framstegen med att utveckla en europeisk ram inte

[150] EUT L 101, 15.4.2011, s. 1.
[151] COM (2020) 661 final, kompletterad med en studie om insamling av uppgifter om människohandel i EU 2017–2018.
[152] Exempelvis samarbetade Europeiska arbetsmyndigheten med Europol för att bekämpa människohandel i EU för alla former av utnyttjande, inbegripet sexuellt utnyttjande och arbetskraftsexploatering, samt alla former av handel med barn. Detta är också ett erkännande av ILO:s protokoll till konventionen om tvångsarbete (P29). Detta protokoll är en grundläggande arbetsnorm som fastställer att tvångsarbete är ett brott och behandlar förebyggande, skydd av offer, ersättning och internationellt samarbete kring nuvarande former av tvångsarbete, även i samband med människohandel.
[153] Studier av de ekonomiska, sociala och mänskliga kostnaderna för människohandel och en översyn av hur medlemsstaternas nationella och gränsöverskridande mekanismer för vidareslussning fungerar, finns på https://ec.europa.eu/anti-trafficking
[154] Europeiska centrumet för människosmuggling, 4:e årsrapporten, 15.5.2020.
[155] http://www.eurojust.europa.eu/press/PressReleases/Pages/2020/2020-05-29.aspx
[156] Europaparlamentets och rådets direktiv om skydd för miljön genom straffrättsliga bestämmelser, 2008/99/EG.
[157] SWD(2020) 259 final.

fått några större effekter på fältet, till exempel när det gäller bättre gränsöverskridande samarbete och mer likvärdiga villkor när det gäller påföljder i alla medlemsstater. Framför allt hade det inte lett till fler fällande domar och mer avskräckande påföljder i medlemsstaterna. Det har därför beslutats att direktivet ska ses över före utgången av 2021.

Den 29–30 oktober 2019 anordnade Eurojust tillsammans med det europeiska nätverket av åklagare för miljö (ENPE) en konferens om internationellt samarbete och samarbete i kampen mot miljöbrott (”International collaboration & co-operation in the fight against environmental crime”) för att öka medvetenheten och främja gränsöverskridande samarbete om miljöbrott bland åklagare och andra rättstillämpare inom och utanför EU.

Den handlingsplan mot olaglig handel med vilda djur och växter som antogs 2016 håller för närvarande på att utvärderas. En särskild åtgärd är ett projekt som pågår fram till januari 2021 och som är inriktat på olaglig handel med vilda djur och växter i och via EU med hjälp av internet- och paketleveranstjänster, i syfte att motverka och upplösa nätverk för it-brottslighet avseende vilda djur och växter[158].

V. ETT STARKT EUROPEISKT SÄKERHETSEKOSYSTEM

En genuin och effektiv säkerhetsunion måste vara något som alla i samhället verkar för. Myndigheter, polis, privata sektorn, utbildningssektorn och medborgarna måste själva vara engagerade, rustade och ordentligt sammankopplade med varandra för att bygga upp beredskap och resiliens för alla, framför allt för de mest utsatta grupperna, brottsoffer och vittnen.

1. Samarbete och informationsutbyte

Ett av de viktigaste bidrag som EU kan ge för att skydda medborgarna är att hjälpa dem som ansvarar för säkerheten att få ett bra samarbete. Samarbete och informationsutbyte är kraftfulla verktyg när man ska bekämpa brott och terrorism, hantera hot mot it-säkerheten och skipa rättvisa. Ett antal verktyg har införts för att stödja informationsutbyte mellan brottsbekämpande och rättsliga myndigheter.

I dag antar kommissionen ett reviderat mandat för **Europol**[159] för att genomföra ett antal riktade förbättringar i dess arbete. På så sätt kommer Europol att bättre kunna hantera den föränderliga karaktären hos brott som begås via internet och ekonomiska brott. Det kommer att stärka samarbetet med den privata sektorn och anpassa dataskyddsbestämmelserna till befintliga EU-bestämmelser.

Europol och andra EU-byråer som Frontex, Cepol och Eurojust har med stöd av kommissionen fortsatt att utveckla EU:s policycykel avseende organiserad och grov internationell brottslighet, den s.k. **Europeiska sektorsövergripande plattformen mot brottshot** (Empact)[160]. Samarbetet inom Empact har fortsatt visa sig vara ett effektivt verktyg mot organiserad brottslighet i hela Europa, exempelvis under ”gemensamma

[158] https://wwf.be/fr/wildlife-cybercrime/

[159] COM (2020) 796 final.

[160] Empact är EU:s verktyg för polissamarbete för att hantera de största hoten mot EU:s säkerhet genom att stärka samarbetet mellan berörda avdelningar i medlemsstaterna, EU:s institutioner och EU-byråer samt tredjeländer och organisationer. Empact samlar olika aktörer (sektorsövergripande arbetsmetod) för att förbättra och stärka samarbetet mellan medlemsstaterna, EU:s institutioner och EU-byråerna samt tredjeländer och organisationer, däribland den privata sektorn.

insatsdagar" i september, oktober och november 2020[161]. Detta är ett tydligt bevis på värdet av samarbete. Det stödde också mindre kvantifierbara mål som en förbättrad underrättelsebild, utbildning och kapacitetsuppbyggnad, förebyggande, samarbete med partner utanför EU och kampen mot internetbrott[162]. I den oberoende utvärderingen av EU:s policycykel 2018–2021/Empact 2020[163] konstaterades att den har visat sig vara allt mer relevant och effektiv när det gäller att hantera de mest akuta hoten från organiserade kriminella grupper. Mervärde tillkommer i form av en samarbetsplattform som gör att medlemsstaterna kan nå bättre resultat mot grov och organiserad brottslighet än om de hade varit tvungna att hantera dessa frågor på egen hand. Utvärderingen uppmärksammade också möjligheter och gav rekommendationer att ytterligare utveckla detta synnerligen användbara samarbetsverktyg under nästa cykel 2022–2025.

Kommissionen kommer under 2021 att lansera ett initiativ till **en EU-kod för polissamarbete**, för att effektivisera, förbättra, utveckla, modernisera och underlätta samarbetet mellan berörda nationella byråer. Detta kommer att bli ett viktigt stöd till medlemsstaterna i deras kamp mot grov och organiserad brottslighet och terrorism.

Samarbete behövs också mellan **polisen och andra centrala brottsbekämpande myndigheter**, och med organ som tullen. EU:s **tullverksamhet** har en viktig uppgift när det gäller att säkra de yttre gränserna och säkerheten för leveranskedjan, och bidrar därmed till Europeiska unionens inre säkerhet. Nya och föränderliga hot berör de viktigaste kopplingarna mellan tullen och de brottsbekämpande myndigheterna, framför allt tullkontrollernas värde när det gäller att upptäcka och förebygga och tullens ledande roll när det gäller varor. Kommissionen har stöttat och uppmuntrat samarbete mellan tullen och Europol[164], vilket får direkt inverkan på insatser på områden som skjutvapen, miljöbrott, kriminell finansiering och it. Tullmyndigheterna deltar för närvarande i flera Europol-ledda insatser mot grov och internationell organiserad brottslighet[165] samt i Cepols utbildningar. Denna verksamhet bidrar till att främja och utveckla ytterligare samarbete mellan olika organ och förbättra samspelet mellan de främsta aktörerna.

Starka och effektiva informationssystem är oumbärliga för att nå bättre informationsutbyte mellan rättsvårdande och brottsbekämpande myndigheter i hela EU. **Schengens informationssystem (SIS)** har också förstärkts med uppdaterade regler som riktas mot eventuella brister genom att ytterligare varningskategorier införs, förteckningen utökas över föremål som varningar kan införas för och nya typer av data som kan införas[166].

---

[161] Empact Gemensamma insatsdagar: "Operation BOSPHORUS", 1 776 skjutvapen beslagtogs (2–11 november), "JADs Mobile 3": över 350 stulna bilar och över 1 000 stulna bildelar återtogs. (12–13 oktober), "JADs against human trafficking for labour exploitation", 715 potentiella offer för arbetskraftsexploatering identifierades (14–20 september). "JADs against crime in southeast Europe", 51 vapen av olika typer och 47 kilo narkotika av olika slag (september).

[162] Alla detaljerade faktablad med siffror, per EMPACT EU:s brottsprioritering, finns här: https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf, Dok 7623/20 5.5.2020.

[163] En oberoende utvärdering planerades i rådets slutsatser av den 27 mars 2017 om en fortsättning av EU:s policycykel avseende organiserad och grov internationell brottslighet för perioden 2018–2021 (7704/17).

[164] Se exempelvis Customs Cooperation Working Party (CCWP) Action Plan (handlingsplanen för arbetsgruppen för tullsamarbete). Till de främsta områden för 2020–2021 hör en ökad närvaro av tulltjänstemän vid Europols sambandskontor, direktåtkomst för tullmyndigheterna till Europols nätapplikation för säkert informationsutbyte (Siena), bättre representation av tulltjänstemän i Europols nationella enheter och medverkan från polis- och tullchefer i Europeiska polischefernas konvent.

[165] Moms- och punktskattebedrägerier, olaglig handel med skjutvapen, miljöbrott, kriminell finansiering, kamp mot sexuella övergrepp mot barn.

[166] Förordning (EU) 2018/1860, förordning (EU) 2018/1861 och förordning (EU) 2018/1862

De nya reglerna trädde i kraft den 28 december 2018 och ska vara helt operativa senast i december 2021[167].

Under 2019 kompletterades **det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister (Ecris)** med ytterligare ett system som möjliggör ett effektivt utbyte av uppgifter från kriminalregister om tredjelandsmedborgare som dömts i EU (Ecris-TCN-systemet). Arbetet med den tekniska utvecklingen och genomförandet av detta nya centraliserade system pågår för närvarande, och det förväntas tas i bruk 2023.

Den 24 juli 2020 antog kommissionen rapporten om översynen av direktivet om passageraruppgifter (PNR)[168], med en granskning av de första två årens tillämpning av PNR-direktivet[169]. Den visar att utvecklingen av det EU-omfattande PNR-systemet har kommit en bra bit på väg. Användningen av PNR-uppgifter är av avgörande betydelse i kampen mot terrorism, grova brott och organiserad brottslighet och har redan gett påtagliga resultat. Det är bara en medlemsstat som ännu inte har meddelat fullt införlivande till kommissionen[170]. Den 3 december 2020 sände kommissionen ett motiverat yttrande för underlåtenhet att anmäla fullt införlivande av direktivet.

Den 9 september 2020 offentliggjorde kommissionen utvärderingen av **direktivet om förhandsinformation om passagerare** från 2004[171]. I utvärderingen framhålls ett antal brister och inkonsekvenser, som kommer att beaktas vid den kommande översynen av den nuvarande rättsliga ramen. Ett annat viktigt instrument som är föremål för ytterligare granskning är **Prümbesluten**[172], som ska beaktas mot bakgrund av den operativa, tekniska och forensiska utvecklingen och utvecklingen inom dataskydd.

Samarbetet måste nå utanför EU och inbegripa **viktiga tredjeländer i kampen mot terrorism och organiserad brottslighet**. Den 13 maj 2020 godkände rådet att förhandlingar inleddes med Nya Zeeland om utbyte av personuppgifter mellan Europol och Nya Zeeland. Förhandlingar pågår med Turkiet, men inga framsteg har gjorts i förhandlingarna med Algeriet, Egypten, Israel, Jordanien, Libanon, Marocko och Tunisien om utbyte av personuppgifter för bekämpning av grov brottslighet och terrorism. Den 19 november 2020 antog kommissionen dessutom en rekommendation till rådets beslut om bemyndigande att inleda förhandlingar om avtal mellan Europeiska unionen och tio tredjeländer om samarbete mellan Eurojust och dessa tredjeländer om utbyte av personuppgifter[173].

När det gäller **internationellt samarbete om utbyte av PNR-uppgifter** i syfte att bekämpa terrorism och grova brott, godkände rådet att förhandlingar inleds med Japan om undertecknande av ett PNR-avtal[174]. Samtidigt håller de **gemensamma utvärderingarna av de befintliga avtalen EU–USA och EU–Australien** på att slutföras. Kommission har

[167] SIS kommer också att uppdateras i enlighet med den föreslagna ändringen av Europolförordningen (COM(2020) XXX).
[168] COM(2020) 305 final.
[169] Direktiv (EU) 2016/681.
[170] Slovenien.
[171] SWD(2020) 174.
[172] Prümramen möjliggör automatisk överföring av DNA, fingeravtryck och registreringsuppgifter för fordon mellan brottsbekämpande myndigheter. En inledande konsekvensbedömning har offentliggjorts.
[173] De föreslagna tredjeländerna är Algeriet, Armenien, Bosnien och Hercegovina, Egypten, Israel, Jordanien, Libanon, Marocko, Tunisien och Turkiet, COM (2020) 743 final.
[174] 18 februari 2020.

också inlett en process för att se över sin nuvarande övergripande strategi för överföring av PNR-uppgifter till tredjeländer[175].

Kommissionen arbetar också med FN för att öka partnerländernas kapacitet att förebygga, upptäcka, utreda och lagföra terroristbrott och annan grov brottslighet, genom att samla in och analysera passageraruppgifter, både API- och PNR-uppgifter.

Kommissionen inledde en process för att underlätta överföring av PNR-uppgifter i enlighet med EU:s rättsliga krav inom ramen för de nya PNR-standarder[176] som antagits av Internationella civila luftfartsorganisationen (Icao)[177]. Den 23 juni 2020 antog Icao-rådet de nya standardbestämmelserna och rekommendationerna om PNR[178] och dess avtalsslutande parter har till och med den 30 januari 2021 på sig att informera Icao om eventuella skillnader mellan sina nationella bestämmelser och de nya standarderna och rekommendationerna.

2. Betydelsen av starka yttre gränser

Modern och effektiv förvaltning av de yttre gränserna är avgörande för att garantera EU-medborgarnas säkerhet. Om alla relevanta aktörer engageras för att göra mesta möjliga av säkerheten vid gränsen och får lämpliga verktyg, kan det få en verklig effekt på förebyggandet av gränsöverskridande brottslighet och terrorism. I den nya migrations- och asylpakten[179] belystes också behovet av kraftfull och rättvis förvaltning av de yttre gränserna, inbegripet kontroller av identitet, hälsa och säkerhet. Det ingår i den övergripande strategin och visar hur politiken för migration, asyl, integrering och gränsförvaltning är beroende av framsteg på alla fronter.

I den nya pakten understryks att ett effektivt Schengenområde är oumbärligt för migrationspolitiken och att det också har djupgående konsekvenser för säkerheten. Detta diskuterades vid det första Schengenforumet den 30 november 2020. Företrädare för medlemsstaterna och Europaparlamentet var eniga om vikten av ett effektivt Schengen för medborgarna när det gäller fri rörlighet men också säkerhet. Den här processen kommer att bidra till en ny Schengenstrategi som ska läggas fram under 2021. Utvärderings- och övervakningsmekanismen för Schengen är ett viktigt verktyg för att säkerställa ömsesidigt förtroende och för att garantera ett bättre och enhetligt genomförande av Schengenregelverket, däribland dess säkerhetsaspekter. Detta var ett viktigt tema i den rapport som antogs den 25 november[180], med en lägesrapport för genomförandet av Schengenregelverket, och en bedömning av hur utvärderings- och övervakningsmekanismen fungerar.

Förordningarna om interoperabilitet[181] är utformade för att befintliga och nya eller uppgraderade EU-informationssystem för säkerhet och gräns- och migrationshantering ska samverka på ett smartare och effektivare sätt. Interoperabilitet mellan EU:s

[175] Roadmap on the external dimension of the EU policy on Passenger Name Records, tillgänglig på: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12531-External-dimension-of-the-EU-policy-on-Passenger-Name-Records-

[176] Rådets beslut (EU) 2019/2107.

[177] Säkerhetsrådets resolution 2396 (2017).

[178] Benämnd som ändring 28 till bilaga 9 (Underlättande) till konventionen angående internationell civil luftfart (Chicagokonventionen).

[179] COM(2020) 609 final.

[180] SWD(2020)327 final.

[181] Förordning (EU) 2019/817 och förordning (EU) 2019/818.

informationssystem kommer att ge effektivitet och ändamålsenlighet i kontrollerna vid de yttre gränserna och bidra till att förebygga olaglig invandring och till en hög säkerhetsnivå. Den kommer att utgöra ett värdefullt extra verktyg för brottsbekämpande myndigheter och gränsmyndigheter[182]. Medlemsstaterna, de Schengenassocierade länderna och de berörda unionsbyråerna (eu-Lisa, Europeiska gräns- och kustbevakningsbyrån och Europol) måste vara redo, och kommissionen övervakar förberedelserna och beredskapen för att se till att ett fullständigt genomförande uppnås före utgången av 2023.

Medlagstiftarna slöt den 8 december 2020 ett preliminärt avtal om förslaget att **uppdatera informationssystemet för viseringar**[183].

Viss viktig lagstiftning måste dock fortfarande uppdateras. Europaparlamentet måste komma fram till att det är redo att samarbeta med rådet om ändringarna[184] av EU-systemet för reseuppgifter och resetillstånd (Etias)[185].

Kopplingarna mellan relevanta informationssystem för analys av säkerhetsrisken är avgörande för att öka vår säkerhet. En prioritering i handlingsplanen av den 28 september 2020 för att ta tullunionen till nästa nivå[186] är att förbättra **samarbetet mellan tull- och gränsförvaltningsmyndigheter** och att skapa synergier mellan deras **informationssystem** med relevanta skyddsåtgärder, däribland lagstiftning om skyddet av personuppgifter och integritet. I en preliminär bedömning som kommissionen genomfört tillsammans med polis- och tullexperter från medlemsstaterna, rekommenderas särskilt en sammankoppling av Schengens informationssystem (SIS) och Europoluppgifter med tullens importkontrollsystem (ICS2)[187], och en genomförbarhetsstudie kommer nu att inledas.

Förordningen om en europeisk gräns- och kustbevakning[188] trädde i kraft i december 2019 och utgör en grundlig omställning av EU:s kapacitet och verktyg för att stärka unionens yttre gränser. Detta kan avsevärt öka gränsernas bidrag till säkerheten. Det nya mandatet stärker Frontex förmåga att stödja medlemsstaterna i förvaltningen av de yttre gränserna och återvändanden, och ökar möjligheterna till samarbete med tredjeländer. Arbete pågår med att säkerställa att den europeiska gräns- och kustbevakningens permanenta kår är redo för sin första utplacering från och med den 1 januari 2021.

I juni 2019 införde EU **strängare säkerhetsnormer för id-kort** för att underlätta EU-medborgarnas fria rörlighet och samtidigt minska identitetsbedrägerier[189]. Medlemsstaterna är från och med augusti 2021 skyldiga att börja utfärda identitetshandlingar och uppehållstillstånd i enlighet med de nya säkerhetsnormerna. De flesta av dem håller för närvarande på att anpassa sina dokumentutformningar efter kraven i förordningen.

3. Förstärkt forskning och innovation på säkerhetsområdet

[182] Befintliga system: Schengens informationssystem (SIS), Informationssystemet för viseringar (VIS), och framtida system: In- och utresesystem, EU-system för reseuppgifter och resetillstånd (Etias), det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister för tredjelandsmedborgare (Ecris-TCN) Etias, Ecris-TCN) .

[183] COM(2019) 12

[184] COM(2019) 3 final och COM(2019) 4 final.

[185] Förordning (EU) 2018/1240 och förordning (EU) 2018/1241.

[186] COM(2020) 581 final.

[187] System med förhandsinformation om gods används för tidig bedömning av säkerhetsrisker för all förflyttning av varor över den yttre gränsen.

[188] Förordning 2019/1896.

[189] Förordning 2019/1157.

Forskning om säkerhet och främjande av innovation är grunden för en samordnad EU-lösning på komplexa utmaningar, och möjliggör konkreta åtgärder för att minska risker. Säkerheten är ett av fyra fokusområden under 2018–2020 inom arbetsprogrammet **Horisont 2020**[190], vilket utgör 50 % av den totala offentliga finansieringen av säkerhetsforskning i EU. Efter 2019 års ansökningsomgångar för säkerhetsforskning inom Horisont 2020 valdes 42 projekt ut och fick totalt 253 miljoner euro i EU-finansiering. Arbetet kommer att omfatta att skydda infrastruktur, öka katastrofresiliensen, bekämpa brottslighet och terrorism, säkra de yttre gränserna och förbättra den digitala säkerheten. Den preliminära budgeten för projekt under 2020 uppgår till 265 miljoner euro. Detta omfattar en ansökningsomgång med 20 miljoner euro om artificiell intelligens, till stöd för europeiska brottsbekämpande organ för att öka deras AI-kapacitet, eliminera kunskapsklyftor på AI-området och främja samarbete. Arbete som förbereds inom ramen för det nya forskningsprogrammet Horisont Europa kommer att stödja genomförandet av EU:s strategi för en säkerhetsunion och gränsförvaltnings- och säkerhetsdimensionen i den nya migrations- och asylpakten, EU:s politik för katastrofriskreducering och EU:s strategi för sjöfartsskydd[191].

EU-finansierad säkerhetsforskning har också visat sig vara effektiv när det gäller att främja samarbete och stödja säkerhetspersonal under covid-19-pandemin[192]. Stödet omfattar verktyg för gemensam bedömning och utredning av epidemiologiska risker och risker för brott samt en hotbildsbedömning.

För att säkerställa spridningen av **innovativa projekt** måste EU:s byråer integreras med befintlig forskning och innovation inom säkerhetsområdet. Efter RIF-rådet i oktober 2019 håller EU:s byråer och kommissionens gemensamma forskningscentrum, utifrån sina befintliga rättsliga mandat, på att inrätta en **europeisk innovationsknutpunkt för inre säkerhet** som ska fungera som ett samarbetsnätverk för deras innovationslaboratorier. Knutpunkten kommer vara en samordningsmekanism som ska stödja de deltagande enheterna när det gäller utbyte av information och kunskap, lansering av gemensamma projekt och spridning av resultat och tekniska lösningar som är relevanta för den inre säkerheten[193].

Europeiska centrumet för cybersäkerhet inom näringsliv, teknik och forskning och nätverket av nationella samordningscentrum är Europas svar för att stödja innovation och industripolitik inom it-säkerhet. Syftet är att stärka den europeiska it-säkerhetskapaciteten, skydda vår ekonomi och vårt samhälle från cyberattacker, upprätthålla forskningens kvalitet och stärka EU:s konkurrenskraft. Trepartsmöten pågår.

[190] EU har anslagit cirka 91 miljoner euro till projekt som förbättrar skyddet av infrastruktur, däribland mot kombinerade cyberhot och fysiska hot, förbättrad och snabb insats vid incidenter och bättre informationsutbyte.

[191] Under Horisont Europa kommer kluster 3 särskilt att stödja kommissionens politiska prioriteringar: Främjande av vår europeiska livsstil, den europeiska gröna given och ett Europa rustat för den digitala tidsåldern.

[192] Åtgärder inom Horisont 2020 som stöder insatser under pandemin finns på: https://www.researchgate.net/publication/341287556.

[193] Den 21 februari 2020 bekräftade ständiga kommittén för operativt samarbete i frågor som rör den inre säkerheten uppdragsbeskrivningen, de främsta funktionerna, uppgifterna och styrningen av EU:s innovationsknutpunkt för inre säkerhet.

4. Kompetens och ökad medvetenhet

Om vi ska kunna bygga ett mer motståndskraftigt samhälle med bättre beredskap i företag, förvaltningar och hos enskilda personer är det mycket viktigt med medvetenhet om säkerhetsfrågor och kompetens att hantera eventuella hot. Det är också viktigt att brottsoffer kan utöva sina rättigheter.

Brottsbekämpande och rättsväsende

De covid-19-relaterade restriktionerna har i hög grad påverkat Cepol, som tvingades ställa in all planerad närutbildning från mars 2020. De här särskilda omständigheterna har också orsakat en ökad efterfrågan på onlinetjänster. Under årets första fyra månader noterade byrån en ökning på 30 % i virtuella aktiviteter och en ökning på 100 % av nätanvändarna. Till de prioriterade utbildningsområdena för 2019–2021[194] hör kampen mot olaglig invandring, terrorismbekämpning, människohandel, it-brottslighet och sexuella övergrepp mot barn. Kommissionen förbereder för närvarande en utvärdering av Cepol som ska vara färdig i juli 2021.

Allmänheten

Kampanjen #SaferInternet4EU lanserades på Safer Internet Day 2018. Aktiviteterna har nått ut till närmare 63 miljoner personer i EU under de senaste två åren och omfattar utmärkelser, stöd till lärare och it-hygien. Nätverket av centrum för ett säkrare internet erbjöd över 1 800 nya resurser som bland annat omfattar falska nyheter, nätmobbning, integritetsfrågor, gromning och it-hygien.

Oktober 2020 var den åttonde **Europeiska månaden för cybersäkerhet**, som främjar nätsäkerheten inom EU. Årets kampanj kretsade kring säkerhetsfrågor som rör digitaliseringen av vårt dagliga liv – aktuellare än någonsin på grund av covid-19-pandemin. Kampanjen uppmuntrar människor att tänka efter innan de klickar (”Think Before U Click”) och lyfter fram olika teman för it-säkerhet som gör det lättare att identifiera och hantera it-hot. 2021 års europeiska utmaning för it-säkerhet i Prag håller på att förberedas.

Ett viktigt verktyg som hjälper offer för it-brott är No More Ransom[195]. Det är ett kostnadsfritt dekrypteringsverktyg som hjälper offer att slå tillbaka utan att betala hackarna. Verktyget stöds av Europols it-brottscentrum och firade sitt fjärde år i juli 2020. Sedan lanseringen har det registrerat över 4,2 miljoner besökare från 188 länder och förhindrat att uppskattningsvis 632 miljoner dollar i lösensummor hamnat i brottslingarnas fickor.

Den 1 juli 2020 lade kommissionen fram den **europeiska kompetensagendan**[196] för hållbar konkurrenskraft, social rättvisa och motståndskraft. Den sätter upp ambitiösa kvantitativa mål för att förbättra den nuvarande kompetensen och utbildningen i nya färdigheter som ska uppnås under de kommande fem åren. Det omfattar också insatser för att öka antalet utexaminerade inom naturvetenskap, teknik, ingenjörsvetenskap, humaniora och matematik som behövs inom sådana spetsområden som it-säkerhet. Den 10 november 2020 lanserade kommissionen kompetenspakten under den femte upplagan av Europeiska veckan för yrkesutbildning 2020. Pakten främjar gemensamma åtgärder för att maximera effekten av investeringar i att förbättra befintlig kompetens och utbildning med nya

[194] Bedömning av de strategiska behoven av utbildning i EU 2018–2021, EU-STNA report, CEPOL.
[195] https://www.nomoreransom.org/.
[196] COM(2020)274.

färdigheter. Tillsammans med pakten har det första europeiska kompetenspartnerskapet aviserats på tre områden: fordonsindustrin, mikroelektronik samt flyg- och rymdteknik och försvar.

Den 30 september 2020 antog kommissionen ett antal politiska strategier som kommer att få stor betydelse för utvecklingen av EU:s långsiktiga säkerhetskompetens. **Handlingsplanen för digital utbildning 2021–2027**[197] kommer att driva på ett högpresterande ekosystem för digital utbildning med ökad kompetens för den digitala omställningen[198]. Ett meddelande om det **Europeiska området för utbildning** senast 2025[199] antogs samma dag, med grundläggande och digitala färdigheter som huvudtema. Ett meddelande om ett nytt **europeiskt område för forskning och innovation**[200] visar hur Europas forsknings- och innovationsområden ska kunna förbättras och påskynda EU:s omställning till digitalt ledarskap och bekämpa könsrelaterat våld i alla former inom forsknings- och innovationsorganisationen.

Erasmus+-programmet bidrar också till att bekämpa radikalisering genom projekt mot radikalisering, våldsbejakande extremism, socialt utanförskap, felaktig information och falska nyheter[201]. Ett exempel är projektet för förebyggande av radikalisering i fängelser som syftar till att öka kompetensen hos personal i främsta ledet för att identifiera, rapportera och tolka signaler om radikalisering och reagera på rätt sätt[202]. Projektet No Hate BootCamp hjälpte ungdomsledare att bli ambassadörer för ”nej till hatpropaganda” i sina lokalsamhällen.

Kommissionen själv försöker engagera allmänheten i diskussionerna om EU:s säkerhetspolitik. Åtgärder på EU-nivå har gjorts mer synliga och tillgängliga för medborgarna genom den nya **webbplatsen om EU:s säkerhetsstrategi**[203]. Många **offentliga samråd** har genomförts där medborgarna har fått möjlighet att direkt påverka utformningen av politiken.

Alla brottsoffer har rätt till stöd och skydd, men offren för de allra grövsta brotten, som terrorism eller sexuellt utnyttjande av barn, kräver särskild uppmärksamhet. Den 24 juni 2020 antog kommissionen sin första **EU-strategi för brottsoffers rättigheter (2020–2025)**[204]. Den riktar sig till offer för alla slags brott men särskilt till de mest utsatta, däribland offer för terrorism, barn som fallit offer för sexuellt utnyttjande och offer för människohandel. Den 22 september 2020 anordnade kommissionen en högnivåkonferens om brottsoffers rättigheter och då invigdes **plattformen för brottsoffers rättigheter**, som ska främja en mer övergripande strategi för detta[205]. Kommissionen har också utnämnt sin

[197] COM(2020) 624 final.
[198] https://ec.europa.eu/education/sites/education/files/document-library-docs/deap-communication-sept2020_en.pdf.
[199] COM(2020) 625 final.
[200] COM(2020) 628 final.
[201] Hittills har omkring 80 projekt som rör radikalisering finansierats, över 100 projekt om att förebygga och bekämpa nätmobbning och över 100 om utbildning för kritisk och etisk användning av internet i syfte att bekämpa desinformation på nätet.
[202] http://www.r2pris.org/.
[203] https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union-strategy_sv.
[204] COM(2020)258 final.
[205] Plattformen ska för första gången sammanföra de viktigaste aktörerna på EU-nivå, däribland det europeiska nätverket för brottsoffers rättigheter, EU-nätverket av nationella kontaktpunkter för skadestånd, EU:s samordnare för kampen mot terrorism, relevanta byråer som Eurojust, Europeiska

första **samordnare för brottsoffers rättigheter**, till stöd för konsekvens och ändamålsenlighet i politiken för brottsoffers rättigheter.

När det gäller **offer för terrorism** inrättades i januari 2020 EU:s expertcentrum för terrorismens offer, som ska erbjuda expertis, vägledning och stöd till nationella myndigheter och brottsofferorganisationer. Det främjar utbyten av bästa praxis och sakkunskap över gränserna mellan personer som arbetar med dessa frågor och specialister. Det är inte utformat för att erbjuda direkt hjälp till särskilda offer för terrorism, utan för att stödja nationella strukturer när det gäller att erbjuda professionell hjälp och stöd, däribland riktlinjer som ska offentliggöras under 2020. EU-centrumet är ett pilotprojekt som ska pågå i två år. Rådets ordförandeskap arbetar med att stödja detta med ett nätverk av nationella kontaktpunkter för offer för terrorism.

VI SLUTSATS

Strategin för EU:s säkerhetsunion infördes för att tillhandahålla ett övergripande och dynamiskt tillvägagångssätt. Terroristattackerna på senare tid har återigen visat att EU måste kunna reagera och att vi måste stärka vår resiliens och beredskap genom modernisering och effektiv spridning av de verktyg vi har till vårt förfogande. De har också visat att alla aktörer måste engagera sig fullt ut i en gemensam strategi, så att medlemsstaterna, EU-institutionerna, den privata sektorn, ideella organisationer och medborgarna själva kan bidra till att bygga upp en säkerhetsbas som är tillräckligt stark och flexibel för att ge resultat. Denna enhetliga och konsekventa strategi är också det bästa sättet att se till att våra grundläggande rättigheter skyddas som en del av främjandet av vår europeiska livsstil.

Den här rapporten visar att många arbetsflöden pågår, men också att vi måste hålla takten uppe. Målet för EU-agendan för terrorismbekämpning som presenterades i dag är att stärka den europeiska ramen för terroristbekämpning genom att fastställa vilka åtgärder som krävs: att föregripa och förebygga terrorism, att skydda medborgarna och infrastrukturen och att vara redo att regera, med beaktande av kopplingen mellan inre och yttre säkerhet. Vi har redan mer samarbete, fler satsningar mot radikalisering och fler verktyg för att beröva terrorister deras medel för en attack. Nu måste vi gå ett steg längre. Avgörande för det är att säkerställa att nya regler antas för att ta itu med terrorisminnehåll på nätet, och här är ett avtal under det här året en viktig prioritering. Kommissionen uppmanar också medlemsstaterna att påskynda genomförandet av all överenskommen lagstiftning. Det är ett gemensamt ansvar att garantera EU-medborgarnas säkerhet, och en kollektiv ambition för ett säkrare Europa måste vara ett gemensamt åtagande.

unionens byrå för grundläggande rättigheter, Europeiska unionens byrå för utbildning av tjänstemän inom brottsbekämpning och Europeiska jämställdhetsinstitutet och civilsamhället.