EUROPEISKA
KOMMISSIONEN

Bryssel den 24.7.2020
COM(2020) 605 final

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

Strategi för EU:s säkerhetsunion

I. Inledning

I kommissionens politiska riktlinjer klargörs att vi inte kan lämna någon möda ospard när det gäller att skydda allmänheten i EU. Säkerheten är inte bara en förutsättning för personlig trygghet utan också för grundläggande rättigheter och för tilliten till och dynamiken i vår ekonomi, vårt samhälle och vår demokrati. Människorna i EU står i dag inför en föränderlig säkerhetsmiljö, som påverkas av framväxande hot och andra faktorer som klimatförändringar, befolkningsutveckling och politisk instabilitet bortom våra gränser. Globaliseringen, den fria rörligheten och den digitala omställningen skapar välstånd, förenklar våra liv och stimulerar innovation och tillväxt. Men dessa fördelar är oupplösligt förenade med risker och kostnader. De kan manipuleras av terrorister, organiserad brottslighet, narkotikahandlare och människosmugglare som alla utgör direkta hot mot allmänheten och vår europeiska livsstil. Cyberattacker och cyberbrottslighet fortsätter att växa. Säkerhetshoten blir också allt mer komplexa: de gynnas av möjligheterna att verka gränsöverskridande och av sammankopplingarna, de drar fördel av den suddiga gränsen mellan den fysiska och den digitala världen och utnyttjar sårbara grupper och sociala och ekonomiska skillnader. Attacker kan komma med ett ögonblicks varsel och efterlämna små eller inga spår. Både statliga och andra aktörer kan sätta in olika hybridhot[1], och det som händer utanför EU kan få kritiska konsekvenser för säkerheten inom EU.

Covid-19-krisen har också ändrat hur vi ser på säkerhetshot och säkerhetspolitik. Den har visat på behovet av att garantera säkerhet i både den fysiska och digitala miljön. Den har understrukit betydelsen av öppet strategiskt oberoende i våra leveranskedjor i fråga om varor, tjänster, infrastruktur och teknik av kritisk betydelse. Den har stärkt behovet av att engagera alla sektorer och personer i en gemensam satsning på att göra EU bättre förberett, mer resilient och med bättre verktyg för att reagera när det behövs.

Allmänheten kan inte skyddas enbart genom medlemsstaternas egna insatser. Det har aldrig varit viktigare att bygga vidare på våra starka sidor för att arbeta tillsammans, och EU har aldrig haft större möjligheter att bidra. EU kan föregå med gott exempel genom att stärka sin krishantering och verka inom och utanför sina gränser för att bidra till global stabilitet. Även om medlemsstaterna har huvudansvaret för säkerheten, har förståelsen för att en medlemsstats säkerhet är allas säkerhet ökat de senaste åren. EU kan sätta in en tvärvetenskaplig och integrerad reaktion som hjälper säkerhetsaktörer i medlemsstaterna med de verktyg och den information de behöver[2].

EU kan också se till att säkerhetspolitiken fortsätter att vara förankrad i våra gemensamma europeiska värden – respekt och upprätthållande av rättsstatsprincipen, jämlikhet[3], grundläggande rättigheter, insyn, ansvarsutkrävande och demokratisk kontroll – så att politiken har medborgarnas förtroende. EU kan skapa en fungerande och verklig säkerhetsunion, där enskildas fri- och rättigheter värnas. Säkerhet och respekt för de grundläggande rättigheterna är inte motstridiga mål, utan hänger samman med och kompletterar varandra. Våra värden och grundläggande rättigheter måste utgöra

[1] Definitionerna av hybridhot varierar, men går ut på att ringa in blandningen av tvångsmedel och undergrävande verksamhet, konventionella och okonventionella metoder (diplomatiska, militära, ekonomiska, tekniska m.m.), som kan sättas in på ett samordnat sätt av statliga eller andra aktörer för att nå ett visst mål (men håller sig under tröskeln för öppet krig). Se JOIN(2016) 18 final.

[2] Exempelvis tjänster från EU:s rymdprogram som Copernicus, innefattande jordobservationsdata och -tillämpningar som kan bidra till gränsbevakning, sjöfartsskydd, polisverksamhet, bekämpning av piratverksamhet, avskräckning från narkotikasmuggling samt krishantering.

[3] *En jämlikhetsunion: jämställdhetsstrategi för 2020–2025*, COM(2020) 152.

säkerhetspolitikens grund, där nödvändighets-, proportionalitets- och legalitetsprinciperna iakttas, och med garantier för ansvarsutkrävande och rättslig prövning, och samtidigt möjliggöra verkningsfulla åtgärder till skydd för individerna, särskilt de mest utsatta.

Det finns redan omfattande rättsliga, praktiska och kompletterande verktyg, men de måste stärkas och användas bättre. Stora framsteg har gjorts för att förbättra informationsutbyte och underrättelsesamarbete med medlemsstaterna och för att begränsa utrymmet för terrorister och brottslingar. Men splittringen kvarstår.

Arbetet får inte göra halt vid EU:s gränser. Att skydda EU och EU-medborgarna handlar inte bara om att garantera säkerheten inom EU:s gränser, utan också om att verka för säkerhet utanför EU. EU:s strategi för yttre säkerhet inom den gemensamma utrikes- och säkerhetspolitiken (Gusp) och den gemensamma säkerhets- och försvarspolitiken (GSFP) förblir en viktig del av EU:s insatser för att förbättra säkerheten inom EU. Samarbete med tredjeländer och på global nivå för att angripa gemensamma utmaningar är av central betydelse för effektiva och heltäckande insatser, eftersom stabilitet och säkerhet i EU:s grannskap är av avgörande betydelse för EU:s egen säkerhet.

Med utgångspunkt i tidigare arbete i Europaparlamentet[4], rådet[5] och kommissionen[6] visar den här nya strategin att en verklig och fungerande säkerhetsunion måste ha en stark kärna av verktyg och politik för att åstadkomma säkerhet i praktiken, i kombination med insikten om att säkerheten har konsekvenser för alla delar av samhället och all offentlig politik. EU måste säkerställa en trygg miljö för alla oavsett ras, etniskt ursprung, religion, övertygelse, kön, ålder eller sexuell läggning.

Den här strategin täcker åren 2020–2025 och är inriktad på kapacitetsuppbyggnad för framtidssäker säkerhetspolitik. Den tar ett helhetsgrepp på samhället som på ett samordnat sätt kan svara på en föränderlig hotbild. Vidare fastställs strategiska prioriteringar och motsvarande åtgärder för att hantera digitala och fysiska risker på ett integrerat sätt över hela linjen inom säkerhetsunionen, särskilt på de områden där EU kan tillföra ett mervärde. Målet är att erbjuda säkerhetsresultat som skyddar alla i EU.

II. En föränderlig europeisk hotbild

Medborgarnas säkerhet, välstånd och välbefinnande är beroende av att de är trygga. Hoten mot den säkerheten beror på hur sårbara deras liv och försörjning är. Ju större sårbarhet, desto större är risken för att den utnyttjas. Både sårbarheter och hot utvecklas hela tiden, och EU behöver anpassa sig.

Vår vardag är beroende av ett brett utbud av tjänster, t.ex. energitjänster, transporter och finanstjänster samt hälso- och sjukvård. De bygger i sin tur på både fysisk och digital infrastruktur, vilket ökar sårbarheten och risken för störningar. Under covid-19-pandemin har många företag och offentliga tjänster tack vare ny teknik kunnat fortsätta, bl.a. genom att hålla oss i kontakt med varandra genom distansarbete och genom att hålla i gång distributionskedjornas logistik. Men detta har också öppnat dörren för en exempellös ökning

[4] Till exempel arbetet i Europaparlamentets utskott för terrorismfrågor, som rapporterade i november 2018.

[5] Från rådets slutsatser från juni 2015 om en förnyad strategi för inre säkerhet till resultaten av rådets överläggningar i december 2019.

[6] *Att genomföra den europeiska säkerhetsagendan mot terrorism och bana väg för en säkerhetsunion*, COM(2016) 230 final, 20.4.2016. Se den färska utvärderingen av genomförandet av lagstiftningen på området för inre säkerhet: *Implementation of Home Affairs legislation in the field of internal security - 2017–2020*, SWD(2020)135.

av skadliga attacker, där man för brottsliga ändamål[7] försöker utnyttja de störningar som pandemin och övergången till distansarbete orsakar. Varubrist har skapat nya möjligheter för organiserad brottslighet. Konsekvenserna kunde ha varit ödesdigra och stört viktiga vårdtjänster när de stod under hårdast tryck.

De alltfler sätt på vilka den digitala tekniken berikar våra liv har också medfört att teknikens **cybersäkerhet** blir en fråga av strategisk betydelse[8]. Hushåll, banker, finanstjänster och företag (särskilt små och medelstora) drabbas hårt av cyberattacker. Riskerna för skada blir desto större på grund av hur fysiska och digitala system är beroende av varandra: alla fysiska konsekvenser påverkar självfallet digitala system, medan cyberattacker mot informationssystem och digital infrastruktur kan sätta stopp för nödvändiga tjänster[9]. Utvecklingen av sakernas internet och den tilltagande användningen av artificiell intelligens medför både nya fördelar och nya risker.

Vår värld bygger på digital infrastruktur, digital teknik och digitala system som gör det möjligt för oss att grunda företag, konsumera produkter och utnyttja tjänster. Allt detta förutsätter kommunikation och interaktion. Nätberoendet har skapat utrymme för en våg av **cyberbrott**.[10] ”Cyberbrott som tjänst” och den underjordiska brottsliga cyberekonomin ger enkel tillgång till cyberbrottsliga varor och tjänster på nätet. Brottslingarna anpassar snabbt ny teknik till sina egna syften. Exempelvis har förfalskade läkemedel nästlat sig in i den lagliga leveranskedjan för läkemedel[11]. Den exponentiella ökningen av material som rör sexuella övergrepp mot barn på nätet[12] har visat hur förändrade brottsmönster får konsekvenser för samhället. Enligt en aktuell undersökning oroar sig de flesta i EU (55 %) för att brottslingar och bedragare ska få tillgång till deras data[13].

Den **globala miljön** förvärrar också de här hoten. Tredjeländers bestämda industripolitik, i kombination med fortsatta immaterialrättsliga intrång som möjliggörs av informationsteknik, förändrar det strategiska paradigmet för att skydda och främja EU:s intressen. Detta förstärks av framväxten av produkter med dubbla användningsområden, vilket innebär att en stark civil tekniksektor är en viktig resurs för försvars- och säkerhetskapaciteten. Industrispionage har långtgående konsekvenser för ekonomin, sysselsättningen och tillväxten i EU: dataintrång i företagshemligheter kostar EU uppskattningsvis 60 miljarder euro[14]. Detta föranleder grundlig reflektion över hur beroendena och den ökade exponeringen för cyberhot påverkar EU:s förmåga att skydda både enskilda och företag.

---

7 Europol: *Beyond the pandemic. How COVID-19 will shape the serious and organised crime landscape in the EU* (april 2020).

8 *Kommissionens rekommendation om it-säkerhet i 5G-nät*, C(2019) 2335, meddelandet *Säker 5G-utbyggnad i EU – Genomförande av EU:s verktygslåda*, COM(2020) 50.

9 Brnos universitetssjukhus i Tjeckien utsattes i mars 2020 för en cyberattack som tvingade sjukhuset att boka om patienter och senarelägga operationer (Europol: *Pandemic Profiteering. How criminals exploit the COVID-19 crisis*). Artificiell intelligens kan missbrukas för digitala, politiska och fysiska angrepp liksom för övervakning. Data från sakernas internet (smarta armbandsur, virtuella assistenter osv.) kan användas för att övervaka enskilda personer.

10 Enligt vissa prognoser kommer kostnaderna för dataintrång att 2024 uppgå till 5 biljoner dollar per år, en ökning från 3 biljoner dollar 2015 (Juniper Research, *The Future of Cybercrime & Security*).

11 Enligt en studie från 2016 (Legiscript) bedrev uppskattningsvis bara 4 % av internetapoteken i världen laglig verksamhet, och konsumenterna i EU var en högintressant målgrupp för de 30 000–35 000 oseriösa nätapoteken.

12 *EU Strategy for a more effective fight against child sexual abuse*, COM(2020) 607.

13 Europeiska unionens byrå för grundläggande rättigheter (2020), *Your rights matter*: *Security concerns and experiences*, *Fundamental Rights Survey*, Luxemburg, Publikationsbyrån.

14 The scale and impact of industrial espionage and theft of trade secrets through cyber, 2018.

Covid-19-krisen har också visat hur sociala motsättningar och osäkerhet leder till säkerhetsluckor. Potentialen för mer sofistikerade **hybridattacker** av stater och andra aktörer har ökat, och blottorna utnyttjas genom en blandning av cyberattacker, skador på kritisk infrastruktur[15], desinformationskampanjer och radikalisering av den politiska debatten.[16]

Samtidigt fortsätter de välkända hoten att utvecklas. Tendensen för **terroristattacker** i EU var sjunkande under 2019. Hotet mot EU-medborgarna från jihadistattacker utförda eller inspirerade av Daish och al-Qaida och närstående organisationer förblir dock högt[17]. Samtidigt ökar hotet från den våldsamma högerextremismen[18]. Rasistiskt inspirerade attacker måste tas på största allvar: de dödliga antisemitiska terrorattackerna i Halle var en påminnelse om behovet att trappa upp reaktionerna i enlighet med rådets uttalande från 2018[19]. En av fem personer i EU oroar sig mycket för en terrorattack de närmaste tolv månaderna[20]. Merparten av den senaste tidens terrorattacker var lågteknologiska där ensamvargar gav sig på enskilda på allmänna platser, samtidigt som terrorpropagandan tog sig nya former med direktsändningen på nätet från attackerna i Christchurch[21]. Hotet från radikaliserade individer är fortfarande högt, och kan förstärkas av återvändande utländska terroriststridande och extremister som släpps ur fängelse[22].

Krisen har också visat hur befintliga hot kan utvecklas under nya omständigheter. **Organiserade kriminella grupper** har utnyttjat varubrist som skapat möjligheter för nya olagliga marknader. Den olagliga narkotikahandeln förblir den största brottsliga marknaden i EU med ett försäljningsvärde på uppskattningsvis minst 30 miljarder euro per år i EU[23]. Människohandeln fortsätter: uppskattningsvis uppgår den totala vinsten i hela världen för alla former av utnyttjande till 30 miljarder euro[24]. Världshandeln med förfalskade läkemedel uppgick till 38,9 miljarder euro[25]. Samtidigt gör den låga andelen beslag att brottslingarna kan fortsätta att expandera sin kriminella verksamhet och nästla sig in i den lagliga ekonomin[26]. Brottslingar och terrorister har lättare att få tillgång till skjutvapen från marknaden på nätet och genom ny teknik som 3D-utskrifter[27]. Artificiell intelligens, ny

---

15 Med kritisk infrastruktur menas anläggningar som är nödvändiga för att upprätthålla centrala samhällsfunktioner, hälsa, säkerhet, trygghet och människors ekonomiska eller sociala välfärd och där driftsstörning eller förstörelse av dessa skulle få betydande konsekvenser (rådets direktiv 2008/114/EG).

16 97 % av allmänheten i EU har stött på fejknyheter, 38 % gör det dagligen. Se JOIN(2020) 8 final.

17 Sammanlagt 119 genomförda, misslyckade eller avvärjda terrorattacker rapporterades av 13 medlemsstater, med 10 döda och 27 skadade (Europol, *European Union Terrorism Situation and Trend Report*, 2020).

18 Under 2019 inträffade sex högerextrema terroristattacker (en genomförd, en misslyckad, fyra avvärjda: tre medlemsstater), jämfört med endast en under 2018, med ytterligare döda i fall som inte klassificerats som terrorism (Europol, 2020).

19 Se även rådets uttalande om kampen mot antisemitism och om utarbetande av en gemensam säkerhetsstrategi för att bättre skydda judiska gemenskaper och institutioner i Europa.

20 EU:s byrå för grundläggande rättigheter: *Your rights matter: Security concerns and experiences*, 2020.

21 Från juli 2015 till årsslutet 2019 påträffade Europol terroristmaterial på 361 plattformar (Europol, 2020).

22 Europol: *A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism*, 2019.

23 Europeiska centrumet för kontroll av narkotika och narkotikamissbruk (EMCDDA) och Europol: *EU Drugs Market Report 2019*.

24 Europol, *Report on Trafficking in Human Beings, Financial Business Model* (2015).

25 Rapport från Europeiska unionens immaterialrättsmyndighet och OECD, Trade in counterfeit pharmaceutical products

26 Rapporten *Återvinning av tillgångar och förverkande: Åtgärder för att se till att brott inte lönar sig*, COM(2020) 217.

27 Under 2017 användes skjutvapen i 41 % av alla terroristattacker (Europol, 2018).

teknik och robotteknik ökar risken ytterligare för att brottslingar ska utnyttja innovationens fördelar med skadliga intentioner[28].

Dessa hot spänner över många fält och drabbar olika delar av samhället på olika sätt. De utgör alla en allvarlig risk för enskilda och företag och kräver en heltäckande och konsekvent reaktion på EU-nivå. När blottor i säkerheten till och med kan bero på små uppkopplade hushållsapparater som internetanslutna kylskåp eller kaffebryggare kan vi inte längre lita enbart på traditionella statliga aktörer för att garantera vår säkerhet. Näringsidkarna måste ta ett större ansvar för cybersäkerheten i de produkter och tjänster som de släpper ut på marknaden, medan enskilda åtminstone behöver ha grundläggande insikter i cybersäkerhet för att kunna skydda sig.

III. En samordnad EU-reaktion för hela samhället

EU har redan visat hur den kan tillföra ett verkligt mervärde. Sedan 2015 har säkerhetsunionen skapat nya samband för hur säkerhetspolitiken ska hanteras på EU-nivå. Men mer behöver göras för att engagera hela samhället, på alla förvaltningsnivåer, inom alla sektorer av näringslivet och dessutom alla enskilda i alla medlemsstater. Den ökande medvetenheten om riskerna med beroende[29] och behovet av en kraftfull europeisk industristrategi[30] för tanken till ett EU med en kritisk massa av industri, teknikproduktion och resiliens i försörjningskedjan. Med styrka avses också fullständig respekt för de grundläggande rättigheterna och EU:s värden: de är en förutsättning för en legitim, verkningsfull och uthållig säkerhetspolitik. Den här strategin för säkerhetsunionen innehåller konkreta handlingslinjer som man kan gå vidare med. Den är upplagd kring följande gemensamma mål:

- ***Kapacitetsuppbyggnad för tidig upptäckt, förebyggande och snabb krishantering:*** EU behöver vara mer resilient för att kunna förebygga, skydda mot och hantera framtida chocker. Vi behöver bygga upp kapaciteten att tidigt upptäcka och snabbt reagera på säkerhetskriser genom ett heltäckande och samordnat tillvägagångssätt, både övergripande och genom initiativ för enskilda sektorer (t.ex. finans, energi, rättsväsende, polis, vård, sjöfart och transporter) med utgångspunkt i befintliga verktyg och initiativ[31]. Kommissionen tänker också lägga fram förslag om ett brett upplagt krishanteringssystem i EU, som också kan vara relevant för säkerhetsfrågor.
- ***Fokus på resultat:*** En resultatinriktad strategi måste baseras på en noggrann hot- och riskbedömning så att våra insatser styrs dit de behövs bäst. Rätt regler och rätt verktyg måste utformas och sättas in. Det behövs tillförlitliga strategiska underrättelser som grund för EU:s säkerhetspolitik. Där det krävs EU-lagstiftning måste den följas upp så

[28] I juli lade franska och nederländska polis- och åklagarmyndigheter i samarbete med Europol och Eurojust fram resultaten av en gemensam utredning för att spränga EncroChat, ett krypterat telefonnät som användes av kriminella grupperingar med anknytning till våldsamma attacker, korruption, mordförsök och storskalig narkotikatransport.

[29] Risker med beroende av utlandet avser ökad exponering för potentiella hot, t.ex. utnyttjande av sårbarhet i it-komponenter i kritisk infrastruktur (däribland energi, transporter, banktjänster samt hälso- och sjukvård), kapning av industriella kontrollsystem och ökad kapacitet för dataintrång och spionage.

[30] Kommissionens meddelande *En ny industristrategi för EU*, COM(2020) 102.

[31] Exempelvis EU-arrangemanget för integrerad politisk krishantering (IPCR), Centrumet för samordning av katastrofberedskap, kommissionens rekommendation om samordnade insatser vid storskaliga cyberincidenter och cyberkriser (C/2017/6100), *EU operational protocol for countering hybrid threats (EU Playbook)* SWD(2016) 227 (ej översatt till svenska).

att den tillämpas fullständigt, så att fragmentering undviks och inga blottor uppstår. Ett effektivt genomförande av den här strategin förutsätter också att det anslås tillräckliga medel under nästa programperiod 2021–2027, bl.a. till de EU-organ som berörs.

- ***Alla i den offentliga och privata sektorn drar sitt strå till stacken:*** De centrala aktörerna i den offentliga och privata sektorn har varit motvilliga att dela med sig av säkerhetsrelevant information, oavsett om det beror på rädsla att äventyra den nationella säkerheten eller konkurrenskraften[32]. Men vi når bäst resultat när alla drar åt samma håll. Främst innebär detta ett intensivare samarbete mellan medlemsstaterna, med polis, domstolar och andra myndigheter, och med EU:s institutioner och organ, för att bygga upp den samsyn och den växelverkan som behövs för gemensamma lösningar. Samarbete med den privata sektorn har också central betydelse, särskilt med tanke på att näringslivet äger en stor del av den digitala och övriga infrastruktur som krävs för att effektivt bekämpa brottslighet och terrorism. Enskilda kan också bidra, till exempel genom att bygga upp den kompetens och medvetenhet som krävs för att bekämpa cyberbrottslighet och desinformation. Slutligen måste denna gemensamma satsning sträcka sig över våra gränser så att vi knyter närmare band med likasinnade partner.

IV. Skydda alla i EU – strategiska prioriteringar för säkerhetsunionen

EU är unikt lämpat att reagera på dessa nya globala hot och utmaningar. Hotbilden ovan visar fyra sammanhängande strategiska prioriteringar för vidare behandling på EU-nivå, under fullständigt hänsynstagande till de grundläggande rättigheterna: i) en framtidssäkrad säkerhetsmiljö, ii) hantering av föränderliga hot, iii) skydd av människor i EU från terrorism och organiserad brottslighet samt iv) ett starkt europeiskt säkerhetsekosystem.

1. En framtidssäkrad säkerhetsmiljö

Skyddad och resilient kritisk infrastruktur

Enskilda är beroende av central infrastruktur i vardagen, för att resa, arbeta, utnyttja viktiga offentliga tjänster som sjukhus, transporter och energiförsörjning och för att utöva sina demokratiska rättigheter. Om denna infrastruktur inte är tillräckligt skyddad och resilient kan attacker orsaka enorma störningar – fysiska eller digitala – både i enskilda medlemsstater och kanske i hela EU.

EU:s befintliga ram för skyddad och resilient kritisk infrastruktur[33] har inte hållit jämna steg med riskutvecklingen. Att saker och ting i allt högre grad är beroende av varandra innebär att störningar i en sektor omedelbart kan påverka verksamheten i andra: en attack mot elproduktionen kan slå ut telekommunikation, sjukhus, banker eller flygplatser, medan en attack mot den digitala infrastrukturen kan störa elnät eller finanstjänster. I takt med att vår ekonomi och vårt samhälle mer och mer flyttar ut på nätet blir sådana här risker alltmer akuta. Den rättsliga ramen måste hantera denna ökande grad av sammankoppling och ömsesidigt beroende med kraftfulla åtgärder för skyddad och resilient kritisk infrastruktur, både it-infrastruktur och fysisk infrastruktur. Viktiga tjänster, även de som bygger på

[32] Gemensamt meddelande *Resiliens, avskräckning och försvar*: *ett starkt cyberförsvar för EU*, JOIN(2017) 450.

[33] Direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (EUT L 194, 19.7.2016), Rådets direktiv 2008/114/EG om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna.

rymdinfrastruktur, måste skyddas på lämpligt sätt mot nuvarande och förutsebara hot, men de måste också vara resilienta. Det innebär att systemet kan förbereda sig på och planera för, absorbera, återhämta sig från och bättre anpassa sig till skadliga händelser.

Samtidigt har medlemsstaterna utnyttjat sitt utrymme för skönsmässig bedömning genom att införliva den befintliga lagstiftningen på olika sätt. Den därav följande splittringen kan undergräva den inre marknaden och försvåra den gränsöverskridande samordningen, framför allt i gränsregioner. De som tillhandahåller samhällsviktiga tjänster i olika medlemsstater måste följa olika rapporteringssystem. Kommissionen undersöker om **nya ramar för fysisk och digital infrastruktur** kan medföra mer enhetlighet och en mer sammanhängande strategi för ett tillförlitligt tillhandahållande av grundläggande tjänster. Ramen behöver kompletteras med **sektorsspecifika initiativ** för att hantera de särskilda riskerna med kritisk infrastruktur, t.ex. transport, energi, finans och hälso- och sjukvård[34]. Med tanke på hur beroende finanssektorn är av it-tjänster och dess allvarliga sårbarhet för cyberattacker, är ett första steg ett initiativ om digital operativ resiliens i finanssektorn. På grund av energisystemets särskilda känslighet och betydelse tas ett särskilt initiativ för att stödja starkare resiliens i kritisk energiinfrastruktur mot fysiska hot och cyber- och hybridhot, vilket garanterar lika villkor för energiföretag med gränsöverskridande verksamhet.

Utländska direktinvesteringar som sannolikt inverkar på säkerheten hos kritisk infrastruktur eller teknik ska också bedömas av EU:s medlemsstater och kommissionen enligt de nya EU-reglerna om granskning av utländska direktinvesteringar[35].

EU kan också skapa nya verktyg för att stödja den kritiska infrastrukturens resiliens. Internet i världen har hittills visat sig mycket resilient, särskilt när det gäller förmågan att hantera ökade trafikvolymer. Vi måste dock vara beredda på framtida kriser som hotar internets säkerhet, stabilitet och resiliens. Att se till att internet fortsätter att fungera innebär effektiva ingripanden mot cyberincidenter och skadlig nätverksamhet och att begränsa beroendet av infrastruktur och tjänster som är belägna utanför EU. Det förutsätter en kombination av lagstiftning, där befintliga regler ses över för att säkerställa en hög gemensam säkerhetsnivå i nätverks- och informationssystem i EU, ökade satsningar på forskning och innovation, och eventuellt en utbyggnad eller befästning av central internetinfrastruktur, särskilt domännamnssystemet[36].

En viktig faktor för att skydda viktiga europeiska och nationella digitala resurser är att erbjuda den kritiska infrastrukturen en kanal för säker kommunikation. Kommissionen arbetar tillsammans med medlemsstaterna för att bygga upp en certifierad säker heltäckande

[34] Eftersom vården stått under särskild press under covid-19-krisen tänker kommissionen också överväga initiativ för att stärka EU:s hälsosäkerhetsram och göra det enklare för ansvariga EU-organ att reagera på allvarliga gränsöverskridande hälsohot.

[35] Europaparlamentets och rådets förordning (EU) 2019/452 av den 19 mars 2019 om upprättande av en ram för granskning av utländska direktinvesteringar i unionen börjar tillämpas fullständigt den 11 oktober 2020 och ger EU ett nytt samarbetsverktyg för att granska direktinvesteringar från länder utanför EU som kan påverka säkerheten eller den allmänna ordningen. Enligt förordningen ska medlemsstaterna och kommissionen bedöma risker i samband med sådana utländska direktinvesteringar och, när det är lämpligt och relevant för fler än en medlemsstat, föreslå lämpliga medel för att minska riskerna.

[36] Domännamnssystemet (DNS) är ett hierarkiskt och decentraliserat namngivningssystem för datorer, tjänster och andra resurser som är anslutna till internet eller ett privat nät. DNS översätter domännamn till de IP-adresser som behövs för att hitta och identifiera datatjänster och datorer.

kvantinfrastruktur, mark- och rymdbaserad, i kombination med det säkra offentliga satellitkommunikationssystemet i rymdprogramförordningen[37].

Cybersäkerhet

Antalet cyberattacker fortsätter att öka[38]. Attackerna är mer sofistikerade än någonsin, kommer från många olika håll i och utanför EU och är inriktade på områden med maximal sårbarhet. Stater eller statsstödda aktörer är ofta involverade, och de siktar in sig på viktig digital infrastruktur som stora leverantörer av molntjänster[39]. Cyberrisker har också visat sig utgöra ett allvarligt hot mot finanssystemet. Internationella valutafonden uppskattar att bankerna varje år förlorar 9 % av sina nettoinkomster på grund av cyberattacker, vilket motsvarar ca 100 miljarder dollar[40]. Övergången till uppkopplade enheter medför stora fördelar för användarna, men i takt med att färre data lagras och behandlas i datacentraler och fler behandlas närmare användaren i utkanten av systemet[41], kommer cybersäkerheten inte längre att kunna fokusera på skydd av centrala punkter[42].

EU lade 2017 fram en strategi för cybersäkerhet med resiliensuppbyggnad, snabba insatser och effektiv avskräckning i centrum[43]. EU måste nu se till att dess cybersäkerhet håller jämna steg med verkligheten, för att ge både resiliens och reaktionsförmåga. Detta kräver ett helhetsgrepp över hela samhället, där EU:s institutioner och organ, medlemsstaterna, näringslivet, forskarna och allmänheten ger cybersäkerheten den prioritet den behöver[44]. Helhetsgreppet måste kompletteras med sektorsspecifika cybersäkerhetsstrategier för områden som energi, finanstjänster, transporter och hälso- och sjukvård. Nästa fas av EU:s arbete bör sammanställas i en reviderad europeisk strategi för cybersäkerhet.

Nya och förbättrade former av samarbete mellan underrättelsetjänster, EU Intcen och andra organisationer som sysslar med säkerhetsfrågor bör vara en del av insatserna för att öka cybersäkerheten och bekämpa terrorism, extremism, radikalism och hybridhot.

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. Den process som infördes 2019 genom kommissionens rekommendation om it-säkerhet i 5G-nät[45] har nu lett till att medlemsstaterna agerat när det gäller de centrala åtgärderna i 5G-verktygslådan[46].

Ett av de viktigaste behoven på lång sikt är att utveckla en kultur av **inbyggd cybersäkerhet**, där säkerheten konstrueras in i varor och tjänster redan från början. Ett

---

[37] *Förslag till förordning om inrättande av unionens rymdprogram och Europeiska unionens rymdprogrambyrå*, COM(2018) 447.

[38] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[39] Distribuerade överbelastningsattacker är ett ständigt hot: de stora leverantörerna var tvungna att avvärja massiva sådana attacker. t.ex. mot Amazons webbtjänster i februari 2020.

[40] https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/

[41] Edge computing är en distribuerad, öppen it-arkitektur med decentraliserad processorkraft som möjliggör mobildata och sakernas internet. I edge computing behandlas data av själva enheten eller av en lokal dator eller server, dvs. i utkanten av systemet, därav namnet, i stället för att data överförs till en datacentral.

[42] Meddelandet *En EU-strategi för data*, COM(2020) 66 final.

[43] Gemensamt meddelande *Resiliens, avskräckning och försvar*: *ett starkt cyberförsvar för EU*, JOIN(2017) 450.

[44] Rapporten *Cybersecurity – our digital Anchor* från Gemensamma forskningscentrumet ger tvärvetenskapliga insikter i cybersäkerhetens utveckling de senaste 40 åren.

[45] Kommissionens rekommendation om it-säkerhet i 5G-nät, C(2019) 2335. Enligt rekommendationen ska den ses över under det sista kvartalet 2020.

[46] Se rapporten från samarbetsgruppen för nät- och informationssäkerhet om tillämpningen av verktygslådan, 24 juli 2020.

viktigt bidrag till detta är den nya ramen för cybersäkerhetscertifiering enligt cybersäkerhetsakten[47]. Ramen är redan på väg: två certifieringssystem håller redan på att utarbetas, medan prioriteringar för ytterligare system ska fastställas senare i år. Samarbetet mellan EU:s cybersäkerhetsbyrå (Enisa), dataskyddsmyndigheterna och Europeiska dataskyddsstyrelsen[48] har central betydelse på detta område.

Kommissionen har redan konstaterat att det behövs en **gemensam cyberenhet** för ett strukturerat och samordnat operativt samarbete. Det kan även omfatta en mekanism för ömsesidigt bistånd vid kriser på EU-nivå. Med utgångspunkt i cybersäkerhetsrekommendationen[49] kan den gemensamma cyberenheten skapa förtroende mellan de olika aktörerna i det europeiska cybersäkerhetsekosystemet och erbjuda medlemsstaterna viktiga tjänster. Kommissionen tänker inleda diskussioner med de berörda parterna (med början i medlemsstaterna) och fastställa en tydlig process med etappmål och tidsplan före slutet av 2020.

Det är också viktigt med gemensamma regler om informationssäkerhet och cybersäkerhet för alla EU:s institutioner, organ och byråer. Målet bör vara att fastställa bindande och höga gemensamma normer för säkert informationsutbyte, säker digital infrastruktur och säkra system vid alla EU:s institutioner, organ och byråer. Den nya ramen bör stödja ett starkt och effektivt operativt samarbete om cybersäkerhet vid alla EU:s institutioner, organ och byråer, med fokus på uppgifterna för incidenthanteringsorganisationen för EU:s institutioner och byråer (Cert-EU).

Med tanke på den globala karaktären är det avgörande att bygga upp och upprätthålla stabila **internationella partnerskap** för att förebygga, avskräcka från och reagera på cyberattacker. I ramen för EU:s gemensamma reaktion på skadliga cyberaktiviteter (den s.k. cyberdiplomatiska verktygslådan)[50] anges åtgärder inom den gemensamma utrikes- och säkerhetspolitiken, däribland restriktiva åtgärder (sanktioner), som kan sättas in mot aktiviteter som skadar EU:s politiska och ekonomiska intressen och säkerhetsintressen. EU bör också fördjupa sitt arbete genom utvecklings- och samarbetsfonderna för att tillhandahålla kapacitetsuppbyggnad till stöd för partnerländer som vill stärka sina digitala ekosystem, reformera nationell lagstiftning och följa internationella normer. Det ökar samhällets övergripande resiliens och dess förmåga att motverka och reagera effektivt på cyberhot. Här ingår särskilt arbete för att främja EU:s normer och lagstiftning för att öka cybersäkerheten i partnerländerna i grannskapet[51].

Skydd av offentliga platser

Den senaste tidens terrorattacker har inriktats på **offentliga platser**, däribland gudstjänstlokaler och transportnav, och har utnyttjat dessas öppna och tillgängliga karaktär. Den tilltagande terrorism som utlöses av politisk eller ideologiskt motiverad extremism har gjort detta hot ännu mer överhängande. Här krävs både ett starkare fysiskt skydd av sådana

[47] Förordning (EU) 2019/881 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (cybersäkerhetsakten).

[48] Meddelandet *Dataskydd som en pelare för medborgarnas egenmakt och EU:s strategi för den digitala övergången – tillämpning av den allmänna dataskyddsförordningen under två års tid*, COM(2020) 264.

[49] Kommissionens rekommendation 2017/1584 av den 13 september 2017 om samordnade insatser vid storskaliga cyberincidenter och cyberkriser

[50] http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

[51] Se de riktlinjer för EU:s externa cyberkapacitetsuppbyggnad som rådet antog i sina slutsatser den 26 juni 2018.

platser och välfungerande detektionssystem, utan att medborgarnas friheter undergrävs[52]. Kommissionen tänker stärka det offentlig-privata samarbetet för att skydda offentliga platser, med finansiering, utbyte av erfarenhet och god praxis samt särskilda riktlinjer[53] och rekommendationer[54]. Informationskampanjer, krav på och testning av detektionsutrustning och förbättrade bakgrundskontroller för att åtgärda interna hot ingår också i strategin. Det är också viktigt att ha i åtanke att minoriteter och utsatta personer kan drabbas oproportionerligt hårt, bl.a. personer som blir måltavlor på grund av religion eller kön, och det kräver särskild uppmärksamhet. Regionala och lokala myndigheter har en viktig roll för att förbättra säkerheten på offentliga platser. Kommissionen bidrar också till att främja städernas innovation när det gäller säkerheten på offentliga platser[55]. Det nya partnerskapet inom EU:s agenda för städer[56] kring säkerhet på offentliga platser som lades fram i november 2018 visar medlemsstaternas, kommissionens och städernas starka engagemang för att bättre åtgärda hot mot säkerheten i städer.

Marknaden för **drönare** fortsätter att expandera, och de har många värdefulla och legitima användningsområden. De kan dock också missbrukas av brottslingar och terrorister, och utgör ett särskilt hot mot offentliga platser. Måltavlorna kan vara enskilda, folksamlingar, kritisk infrastruktur, polis, gränser eller offentliga platser. Kunskap om användning av drönare i konflikter kan nå Europa direkt (via återvändande utländska terroriststridande) eller via nätet. Bestämmelser som redan utvecklats av Europeiska byrån för luftfartssäkerhet är ett viktigt första steg på områden som registrering av drönarpiloter och obligatorisk fjärridentifiering av drönare. Eftersom drönare blir allt mer allmänt tillgängliga, billigare och får allt fler funktioner, behövs ytterligare åtgärder. Det kan vara fråga om informationsutbyte, riktlinjer och god praxis som alla, inklusive polisen, kan använda, samt mer testning av motåtgärder mot drönare[57]. Dessutom bör konsekvenserna för integritet och dataskydd av drönaranvändning på offentliga platser analyseras ytterligare och åtgärdas.

Centrala åtgärder

- Lagstiftning om skyddad och resilient kritisk infrastruktur
- Översyn av nätverks- och informationssäkerhetsdirektivet
- Initiativ om förstärkt resiliens hos finanssektorns it-system
- Skydd och cybersäkerhet för kritisk energiinfrastruktur och cybersäkerhetsregler för gränsöverskridande elflöden
- Europeisk strategi för cybersäkerhet
- Nästa steg mot inrättandet av en gemensam cyberenhet
- Gemensamma regler om informationssäkerhet och cybersäkerhet för alla EU:s institutioner, organ och byråer

[52] System för biometrisk identifiering på distans bör granskas särskilt. Kommissionens inledande synpunkter beskrivs i kommissionens vitbok av den 19 februari 2020 om artificiell intelligens, COM(2020) 65.

[53] Exempelvis riktlinjerna om säkerhetsbarriärer för skydd av offentliga platser (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120307/hvm_v3.pdf).

[54] Riktlinjer för god praxis finns i SWD(2019) 140, som innehåller ett avsnitt om offentlig-privat samarbete. Anslagen från Fonden för inre säkerhet (polis) inriktas särskilt på att förbättra det offentlig-privata samarbetet.

[55] Tre städer (Pireus i Grekland, Tammerfors i Finland och Turin i Italien) ska testa nya lösningar inom Innovativa åtgärder i städerna, som medfinansieras av Europeiska regionala utvecklingsfonden (Eruf).

[56] EU-agendan för städer är en ny arbetsmetod på flera nivåer som främjar samarbete mellan medlemsstater, städer, kommissionen och andra berörda parter för att stimulera tillväxt, goda boendemiljöer och innovation i Europas städer och kartlägga och hantera sociala utmaningar.

[57] Nyligen inrättades ett flerårigt testprogram för att hjälpa medlemsstaterna att utveckla gemensamma metoder och en testplattform på området.

- Ökat samarbete för skydd av offentliga platser, inklusive gudstjänstlokaler
- Utbyte av bästa praxis för att motverka missbruk av drönare

2. Hantera framväxande hot

Cyberbrottslighet

Tekniken skapar nya möjligheter för samhället. Den erbjuder också domstolarna och polisen nya verktyg. Men samtidigt skapar den också utrymme för brottslingar. Sabotageprogram, intrång i personuppgifter eller företagsdata genom hackning och utstörning av digital verksamhet som orsakar ekonomisk skada eller skadat anseende, ökar. En resilient miljö tack vare stark cybersäkerhet är den första försvarslinjen. Polisen måste kunna arbeta med digitala utredningar med tydliga regler för att utreda och lagföra brott och ge brottsoffren det skydd som krävs. Arbetet bör utgå från arbetsgruppen mot cyberbrottslighet (Joint Cybercrime Action Task Force) vid Europol och beredskapsprotokollet för EU:s brottsbekämpningsinsatser (Law Enforcement Emergency Response Protocol) som upprättats för att samordna insatser vid storskaliga cyberattacker. Det är också viktigt med verkningsfulla mekanismer som möjliggör partnerskap och samarbete mellan den offentliga och privata sektorn.

Samtidigt bör kampen mot cyberbrottslighet prioriteras i den strategiska kommunikationen överallt i EU, för att varna allmänheten för riskerna och informera om de förebyggande åtgärder de kan vidta. Detta bör ingå i en proaktiv strategi. Ett annat viktigt steg är att fullständigt genomföra den nuvarande rättsliga ramen[58]. Kommissionen är beredd att inleda överträdelseförfaranden när det behövs, och tänker se över ramen för att se till att den förblir ändamålsenlig. Tillsammans med Europol och EU:s cybersäkerhetsbyrå Enisa kommer kommissionen också att undersöka om det är genomförbart med ett system för snabb varning i EU för cyberbrott som kan garantera informationsflödet och snabba reaktioner om cyberbrott plötsligt ökar.

Cyberbrottslighet är en global utmaning som kräver effektivt internationellt samarbete. EU stöder Europarådets Budapestkonvention om it-brottslighet, en effektiv och väletablerad ram som låter alla länder fastställa vilka system och kommunikationskanaler de behöver för att kunna samarbeta effektivt med varandra.

Nästan hälften av människorna i EU oroar sig för missbruk av data[59] och **identitetsstöld**[60]. Bedräglig användning av identiteter för ekonomisk vinning är en sak, men det kan också få allvarliga personliga och psykologiska konsekvenser, t.ex. att identitetstjuven gör olovliga inlägg som kan stanna kvar på nätet i åratal. Kommissionen ska undersöka tänkbara praktiska åtgärder för att skydda människor mot alla former av identitetsstöld, med beaktande av det kommande initiativet för en europeisk digital identitet[61].

---

[58] Direktiv 2013/40/EU om angrepp mot informationssystem:

[59] 46 % (Eurobarometer om allmänhetens inställning till cybersäkerhet, januari 2020).

[60] Det överväldigande flertalet av dem som svarade på Eurobarometern 2018 om inställningar (95 %) betraktade identitetsstöld som ett allvarligt brott, och sju av tio som ett mycket allvarligt brott. Eurobarometern i januari 2020 bekräftade att människor oroar sig för cyberbrottslighet, nätbedrägerier och identitetsstöld: två tredjedelar av de tillfrågade oroade sig för bankbedrägerier (67 %) eller identitetsstöld (66 %).

[61] Meddelande framlagt den 19 februari 2020: *Att forma EU:s digitala framtid*, COM(2020) 67.

Att ta itu med cyberbrottsligheten förutsätter framsynthet. I takt med att vi använder ny teknik för att stärka ekonomin och samhället kan brottslingar också försöka utnyttja tekniken för skadliga ändamål. Exempelvis kan brottslingar använda artificiell intelligens för att spåra och identifiera lösenord eller för att göra det enklare att framställa skadlig kod, och utnyttja bilder och ljud för identitetsstöld eller bedrägeri.

Modern polisverksamhet

Polis och rättsväsende måste anpassa sig till den nya tekniken. Den tekniska utvecklingen och nya hot innebär att polisen behöver ha tillgång till nya verktyg, förvärva ny kompetens och utveckla nya utredningsmetoder. För att komplettera den lagstiftning som ska förbättra den gränsöverskridande tillgången till elektroniska bevis i brottsutredningar kan EU hjälpa polis och åklagare att utveckla den kapacitet som krävs för att identifiera, säkra och läsa de data som behövs för att utreda brott och använda data som bevis i domstol. Kommissionen kommer att undersöka sätt att **förbättra polisens kapacitet i digitala utredningar** och fastställa hur man på bästa sätt kan utnyttja forskning och utveckling för att skapa nya polisiära verktyg, och hur utbildning kan erbjuda polis och rättsväsende rätt kompetens. Det omfattar också noggranna vetenskapliga utvärderingar och testmetoder som kommissionens gemensamma forskningscentrum tar fram.

Gemensamma strategier kan också göra att **artificiell intelligens, rymdkapacitet, stordata** och **högpresterande datorsystem integreras** i säkerhetspolitiken på ett sätt som är effektivt både för att bekämpa brott och för att värna de grundläggande rättigheterna. Artificiell intelligens kan vara ett kraftfullt verktyg mot brottslighet, med en enorm utredningskapacitet där stora mängder information analyseras och mönster och avvikelser identifieras[62]. Artificiell intelligens kan också tillhandahålla konkreta verktyg som kan hjälpa till att identifiera terroristmaterial på nätet, upptäcka misstänkta transaktioner vid försäljning av farliga produkter och erbjuda allmänheten hjälp i nödsituationer. För att förverkliga denna potential behöver man sammanföra forskning, innovation och användare av artificiell intelligens med rätt styrning och teknisk infrastruktur, och aktivt involvera näringslivet och högskolorna. Det förutsätter också att man följer högsta tänkbara normer för skydd av de grundläggande rättigheterna i förening med ett verkningsfullt skydd av allmänheten. Framför allt måste beslut som påverkar enskilda personer kunna granskas av människor och överensstämma med den relevanta EU-lagstiftningen[63].

Elektronisk information och elektroniska bevis behövs i omkring 85 % av alla utredningar av allvarliga brott, och 65 % av alla ansökningar går till operatörer etablerade i en annan jurisdiktion[64]. Det faktum att traditionella fysiska spår har flyttat ut på nätet ökar klyftan mellan polisens och brottslingarnas förmåga ytterligare. Därför är det särskilt viktigt med tydliga regler för gränsöverskridande tillgång till elektroniska bevis för brottsutredningar. Detta är anledningen till att Europaparlamentet och rådet snabbt bör anta förslagen om elektroniska bevis för att förse polisen med effektiva verktyg . Gränsöverskridande åtkomst till e-bevis genom multilaterala och bilaterala internationella förhandlingar är också av central betydelse för att fastställa kompatibla internationella regler[65].

---

[62] Exempelvis ekobrott.

[63] Det innebär efterlevnad av den befintliga lagstiftningen, däribland den allmänna dataskyddsförordningen (EU) 2016/679 samt dataskyddsdirektivet (EU) 2016/680 om behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder.

[64] Arbetsdokument från kommissionens avdelningar, SWD(2018) 118 final.

[65] Särskilt det andra tilläggsprotokollet till Europarådets Budapestkonvention om it-brottslighet och avtalet mellan EU och USA om gränsöverskridande åtkomst till e-bevis.

Åtkomsten till digitala bevis beror också på tillgången till information. Om data raderas för snabbt kan viktiga bevis försvinna och då går det inte längre att identifiera och lokalisera misstänkta personer och kriminella nätverk (eller offer). Å andra sidan ger datalagringssystem upphov till frågor om skydd av den personliga integriteten. Beroende på utfallet i de mål som för närvarande behandlas av EU-domstolen, kommer kommissionen att bedöma hur man ska gå vidare med datalagringen.

Åtkomst till registreringsinformation för domännamn på internet (Whois-data)[66] är viktig för brottsutredningar, cybersäkerhet och konsumentskydd. I väntan på en ny Whois-policy från Internet Corporation for Assigned Names and Numbers (ICANN), har det dock blivit allt svårare att komma åt den här informationen. Kommissionen fortsätter att samarbeta med ICANN i flerpartsgemenskapen för att se till att legitima aktörer som ansöker om tillgång, däribland polisen, ska kunna få effektiv tillgång till Whois-data i enlighet med dataskyddsbestämmelser i EU och internationellt. I detta ingår att bedöma möjliga lösningar, bland annat om det kan bli nödvändigt med lagstiftning för att förtydliga reglerna för tillgång till sådan information.

Polis och rättsliga myndigheter behöver också vara utrustade så att de, så snart **5G-nätet för mobil telekommunikation** är fullt utbyggt i EU, kan få tillgång till nödvändiga uppgifter och bevis på ett sätt som respekterar sekretessen vid kommunikation. Kommissionen stöder en utökad och samordnad strategi för att bygga upp internationella normer, fastställa bästa praxis, process och teknisk interoperabilitet på viktiga tekniska områden som AI, sakernas internet och blockkedjeteknik.

En avsevärd del av utredningarna av alla slags brott och terrorism omfattar i dag **krypterad information**. Kryptering är mycket viktig i den digitala världen för att säkra digitala system och transaktioner och för att skydda en rad grundläggande rättigheter, som yttrandefrihet, personlig integritet och dataskydd. Men om det används för kriminella ändamål kan det också maskera brottslingars identitet och dölja innehållet i deras kommunikation. Kommissionen ska undersöka och stödja balanserade tekniska, driftsmässiga och juridiska lösningar på problemen och främja en strategi som både upprätthåller krypteringens effektivitet när det gäller att skydda den personliga integriteten och kommunikationssäkerheten, samtidigt som den ger en effektiv reaktion på brottslighet och terrorism.

Bekämpning av terroristrelaterat innehåll på nätet

Att anpassa säkerheten på internet och i den fysiska miljön innebär fortsatta åtgärder för att **motverka olagligt innehåll på nätet**. De största hoten mot medborgarna – terrorism, extremism och sexuella övergrepp mot barn – baseras allt mer på den digitala miljön. Det kräver konkreta åtgärder och en ram för att säkerställa att de grundläggande rättigheterna respekteras. Ett viktigt första steg är att snabbt slutföra förhandlingarna om den föreslagna lagstiftningen om terroristrelaterat innehåll på nätet[67] och se till att den genomförs. Att stärka det frivilliga samarbetet mellan polis och den privata sektorn i **EU:s internetforum** är också viktigt för att bekämpa att terrorister, våldsamma extremister och brottslingar missbrukar internet. EU-enheten för anmälan av innehåll på internet inom Europol kommer även fortsättningsvis att spela en viktig roll när det gäller att övervaka terroristgruppers verksamhet på nätet och de åtgärder som vidtas av plattformar[68], liksom i den fortsatta

[66] Lagrade i databaser som underhålls av 2 500 registerenheter och registerförare stationerade världen över.
[67] *Förslag om förhindrande av spridning av terrorisminnehåll på nätet*, COM(2018) 640, 12 september 2018.
[68] Europol, november 2019.

utvecklingen av **EU:s krisprotokoll**[69]. Dessutom kommer kommissionen att fortsätta samarbetet med internationella partner, inbegripet i **det globala internetforumet för terrorismbekämpning**, för att hantera dessa utmaningar på global nivå. Arbetet med att stödja utvecklingen av alternativa budskap och motbudskap genom programmet för att stärka det civila samhällets ställning[70] fortsätter.

För att förhindra och motverka spridningen av olaglig hatpropaganda på nätet lanserade kommissionen 2016 en uppförandekod, med ett frivilligt åtagande från digitala plattformar att ta bort innehåll med hatpropaganda. Den senaste utvärderingen visade att företagen inom 24 timmar bedömer 90 % av flaggat innehåll och tar bort 71 % av innehåll som bedöms vara olaglig hatpropaganda. Plattformarna måste dock förbättra insynen och återkopplingen till användare ännu mer och säkerställa att det flaggade innehållet bedöms konsekvent[71].

EU:s internetforum kommer också att underlätta utbyten av befintlig och nyutvecklad teknik för att ta itu med utmaningar som rör sexuella övergrepp mot barn på internet. Att intensifiera **kampen mot sexuella övergrepp mot barn**[72] har högsta prioritet i den nya strategin och ska intensifieras, och man ska försöka maximera användningen av de verktyg som finns tillgängliga på EU-nivå för att bekämpa den här typen av brott. Företag måste kunna fortsätta sitt arbete med att upptäcka och ta bort material om sexuella övergrepp mot barn på nätet, och de skador som detta material orsakar kräver en ram med tydliga och permanenta skyldigheter att ta itu med problemet. I strategin kommer också att tillkännages att kommissionen ska börja förbereda sektorsspecifik lagstiftning för att mer ändamålsenligt ta itu med sexuella övergrepp mot barn på nätet, med full respekt för de grundläggande rättigheterna.

Den kommande lagen om digitala tjänster också kommer också att förtydliga och uppgradera ansvars- och säkerhetsbestämmelserna för digitala tjänster och undanröja hinder för att ta itu med olagligt innehåll och olagliga varor och tjänster.

Dessutom kommer kommissionen att fortsätta att samarbeta med internationella partner och **det globala internetforumet för terrorismbekämpning**, inbegripet genom den oberoende rådgivande kommittén, för att diskutera hur man ska hantera dessa utmaningar på global nivå samtidigt som EU:s värden och grundläggande rättigheter bevaras. Nya ämnen bör också tas upp, såsom algoritmer och onlinespel[73].

Hybridhot

Omfattningen och mångfalden av hybridhot är i dag större än någonsin. Under covid-19-krisen syntes ännu fler bevis på detta, med många statliga och icke-statliga aktörer som försökte utnyttja pandemin – framför allt genom att manipulera informationsmiljön och utmana central infrastruktur. Sådana risker innebär att den sociala sammanhållningen försvagas och förtroendet för EU-institutionerna och medlemsstaternas regeringar undergrävs.

EU:s strategi mot hybridhot anges i 2016 års gemensamma ram[74] och 2018 års gemensamma meddelande om att öka motståndskraften mot hybridhot[75]. Åtgärderna på EU-nivå stöds av

---

69 A Europe that protects - EU Crisis Protocol: responding to terrorist content online (oktober 2019)

70 Kopplat till arbetet med programmet kunskapsspridning om radikalisering, se avsnitt IV.3 nedan.

71 https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf

72 *EU Strategy for a more effective fight against child sexual abuse*, COM(2020) 607.

73 Terrorister använder alltmer meddelandesystemen på spelplattformar för att kommunicera, och unga terrorister spelar också upp våldsamma attacker i videospel.

74 Gemensam ram för att motverka hybridhot – Europeiska unionens insatser, JOIN(2016) 18.

75 Att öka motståndskraften och stärka kapaciteten att hantera hybridhot, JOIN(2018) 16.

en stor mängd verktyg som täcker hela spektrumet av inre och yttre aspekter, och grundas på en helhetsstrategi som inbegriper hela samhället och på nära samarbete med strategiska partner, bland andra Nato och G7. En rapport om genomförandet av EU:s strategi för hybridhot offentliggörs tillsammans med den här strategin[76]. Utifrån kartläggningen[77] som läggs fram parallellt med denna strategi kommer kommissionen och Europeiska utrikestjänsten att skapa en **begränsad onlineplattform** där medlemsstaterna kan ta del av verktyg och åtgärder mot hybridhot på EU-nivå.

Även om ansvaret för att motverka hybridhot i första hand ligger hos medlemsstaterna – på grund av de inneboende kopplingarna till nationell säkerhets- och försvarspolitik – finns det några sårbara punkter som är gemensamma för alla medlemsstater och vissa hot som sträcker sig över gränserna, till exempel sådana som riktar in sig på gränsöverskridande nätverk eller infrastrukturer. Kommissionen och den höga representanten kommer att ta fram en EU-strategi för hybridhot som integrerar den yttre och den inre dimensionen i ett kontinuerligt flöde och sammanför de nationella och EU-övergripande frågorna. Detta måste täcka hela spektrumet av åtgärder – från tidig upptäckt, analys, medvetenhet, resiliensuppbyggnad och förebyggande till krishantering och konsekvenshantering.

Förutom förstärkt genomförande, och med tanke på att hybridhoten hela tiden utvecklas, ska särskild uppmärksamhet ägnas åt att **integrera hybridfrågor i det politiska beslutsfattandet**, för att hålla jämna steg med den dynamiska utvecklingen och se till att inga potentiellt relevanta initiativ förbises. Effekterna av nya initiativ kommer också att bedömas i förhållande till hybridhot, inbegripet inom områden som hittills legat utanför ramen för hybridhot, såsom utbildning, teknik och forskning. Med denna strategi skulle man kunna utnyttja arbetet som gjorts inom konceptualiseringen av hybridhot, vilket ger en heltäckande bild av de olika verktyg som motståndarna kan tänkas använda[78]. Syftet bör vara att säkerställa att beslutsprocessen stöds av en regelbunden och omfattande underrättelsebaserad rapportering om utvecklingen av hybridhot. Detta kommer i hög grad att bygga på medlemsstaternas underrättelser och på ett utökat underrättelsesamarbete med medlemsstaternas behöriga myndigheter genom EU Intcen.

För att utveckla en **lägesbild** kommer kommissionen och Europeiska utrikestjänsten att undersöka möjligheterna att effektivisera informationsflödena från olika källor, däribland medlemsstaterna och EU:s byråer som Enisa, Europol och Frontex. EU:s gemensamma enhet för hybridhot kommer att fortsätta vara unionens kontaktpunkt för bedömningar av hybridhot. Det är centralt att **bygga upp resiliens** för att förebygga och skydda mot hybridhot. Det är därför mycket viktigt att systematiskt registrera och objektivt mäta framstegen på detta område. Ett första steg kommer att bli att identifiera utgångsvärdena för sektorspecifik resiliens mot hybridhot, för såväl medlemsstater som EU-institutioner och EU-organ. För att öka **beredskapen för insatser vid hybridkriser** bör det befintliga protokollet ses över, enligt vad som angavs i 2016 års EU Playbook[79], för att återspegla en

[76] SWD(2020) 153 *Rapport om genomförandet av 2016 års gemensamma ram för att motverka hybridhot och det gemensamma meddelandet från 2018 om att öka motståndskraften och stärka kapaciteten att hantera hybridhot*.

[77] SWD(2020) 152 *Kartläggning av åtgärder för att öka motståndskraften och motverka hybridhot*.

[78] *The Landscape of Hybrid Threats*: *A conceptual Model*, JRC117280, gemensamt utarbetad av gemensamma forskningscentrumet och Europeiska kompetenscentrumet för motverkande av hybridhot.

[79] EU operational protocol for countering hybrid threats (EU Playbook), SWD (2016) 227.

bredare granskning och stärka EU:s krishanteringssystem som för närvarande behandlas[80]. Målet är att maximera effekten av EU:s åtgärder genom att snabbt föra samman sektoriella insatser och säkerställa ett smidigt samarbete med våra partner, i första hand Nato.

Centrala åtgärder
• Säkerställa att lagstiftningen om it-brottslighet genomförs och är ändamålsenlig • En strategi för effektivare bekämpning av sexuella övergrepp mot barn • Förslag om upptäckt och borttagning av material om sexuella övergrepp mot barn • En EU-strategi för att motverka hybridhot • En översyn av EU:s operativa protokoll för att motverka hybridhot (EU Playbook) • En bedömning av hur brottsbekämpningskapaciteten kan utökas i digitala utredningar

3. Skydda EU från terrorism och organiserad brottslighet

Terrorism och radikalisering

Terroristhotet i EU är fortfarande stort. Trots att antalet attacker har minskat överlag, kan de fortfarande få förödande effekt. Radikaliseringen kan också mer allmänt polarisera och på så sätt destabilisera den sociala sammanhållningen. Medlemsstaterna har det primära ansvaret i kampen mot terrorism och radikalisering. Den ständigt ökande gränsöverskridande/sektorsövergripande dimensionen i hotet kräver dock ytterligare åtgärder inom EU:s samarbete och samordning. Ändamålsenligt genomförande av EU:s lagstiftning mot terrorism, inbegripet restriktiva åtgärder[81], är en prioritet. Det är fortfarande ett mål att utöka Europeiska åklagarmyndighetens mandat till att omfatta gränsöverskridande terroristbrott.

Kampen mot terrorismen börjar med att man tar itu med de bakomliggande orsakerna. Polariseringen i samhället, verklig eller uppfattad diskriminering och andra psykologiska och sociologiska faktorer kan stärka människors mottaglighet för radikala uttalanden. I detta sammanhang hänger kampen mot **radikalisering** ihop med att främja social sammanhållning på lokal, nationell och europeisk nivå. Många verkningsfulla initiativ och strategier har tagits fram under det senaste årtiondet, särskilt genom nätverket för kunskapsspridning om radikalisering och EU-städer mot radikalisering[82]. Nu är det dags att överväga åtgärder för att effektivisera EU:s politik, initiativ och medel för att hantera radikaliseringen. Sådana åtgärder kan stödja utvecklingen av kapacitet och kompetens, öka samarbetet, stärka faktabasen och bidra till att utvärdera framstegen, engagera alla relevanta aktörer, inbegripet yrkesverksamma i första ledet, beslutsfattare och den akademiska världen[83]. Mjuka politikområden som utbildning, kultur, ungdom och idrott kan bidra till att förebygga radikalisering och genom att erbjuda nya möjligheter för unga människor i riskzonen och skapa sammanhållning inom EU[84]. Prioriterade områden är bland annat arbete

[80] Efter videokonferensen den 26 mars 2020 antog ledamöterna i Europeiska rådet ett uttalande om EU:s åtgärder till följd av covid-19-utbrottet och uppmanade kommissionen att lägga fram förslag om ett mer ambitiöst och mer omfattande krishanteringssystem inom EU.

[81] Rådet har antagit restriktiva åtgärder i förhållande till IS (Daish) och al-Qaida, och även specifika restriktiva åtgärder riktade mot vissa personer och enheter i syfte att bekämpa terrorismen. Se EU:s sanktionskarta (https://www.sanctionsmap.eu/#/main). Där finns en översikt över alla restriktiva åtgärder.

[82] Pilotinitiativet EU-städer mot radikalisering har det dubbla målet att främja utbyte av sakkunskap mellan EU:s städer och samla in synpunkter på hur lokala samhällen bäst kan stödjas på EU-nivå.

[83] Exempelvis finansiering inom ramen för Europeiska säkerhetsfonden och programmet Medborgarskap.

[84] EU-åtgärder som virtuella utbyten inom Erasmus+ och e-twinning.

med tidig upptäckt och riskhantering, uppbyggnad av resiliens och avståndstagande samt rehabilitering och återanpassning i samhället.

Terrorister har försökt skaffa sig och tillverka vapen av **kemiska, biologiska, radiologiska och nukleära**(CBRN)[85] material, och utveckla kunskap och kapacitet att använda dem[86]. I terrorpropagandan ges CBRN-attackernas potential en framträdande plats. Med en så stor potentiell skaderisk krävs särskild uppmärksamhet. Utifrån den strategi som används för att reglera tillgången till sprängämnesprekursorer, kommer kommissionen att undersöka möjligheten begränsa tillgången till vissa farliga kemikalier som skulle kunna användas för att utföra attacker. Utvecklingen av kapacitet för EU:s för civilskyddsinsatser (rescEU) på området CBRN kommer också att vara viktig. Samarbete med tredjeländer är också viktigt för att förstärka en gemensam kultur av CBRN-säkerhet, där man fullt ut tar vara på EU:s kompetenscentrum för CBRN. Detta samarbete ska omfatta nationella brist- och riskbedömningar, stöd till nationella och regionala CBRN-åtgärdsplaner, utbyte av god praxis och verksamhet för kapacitetsuppbyggnad på CBRN-området.

EU har tagit fram den mest avancerade lagstiftningen i världen för att begränsa tillgången till **sprängämnesprekursorer**[87] och upptäcka misstänkta transaktioner som syftar till att bygga improviserade sprängladdningar. Men hotet från hemmagjorda sprängämnen är fortfarande högt, och de har använts i många attacker i hela EU[88]. Första steget måste bli att genomföra bestämmelserna och se till att internetmiljön inte gör det möjligt att kringgå kontrollerna.

En annan viktig del i kampen mot terrorismen är en effektiv lagföring av dem som har begått terroristbrott, bland annat **utländska terroriststridande** för närvarande i Syrien och Irak. Dessa frågor hanteras främst av medlemsstaterna men EU:s samordning och stöd kan hjälpa dem att hantera gemensamma utmaningar. De åtgärder som redan har påbörjats för att fullt ut genomföra lagstiftningen om gränssäkerhet[89] och till fullo använda alla relevanta EU-databaser för att utbyta information om kända misstänkta, kommer också att vara ett viktigt steg. Förutom att identifiera högriskpersoner krävs även en återanpassnings- och rehabiliteringspolicy. Yrkesöverskridande samarbete, inbegripet med fängelsepersonal och övervakare, ska öka den rättsliga förståelsen av hur det går till att radikaliseras till våldsbejakande extremism och den rättsliga sektorns strategi för straff och alternativ till frihetsberövande.

Kampen mot utländska terroriststridande är ett tydligt exempel på kopplingen mellan inre och **yttre säkerhet.** Samarbete i terrorismbekämpning och förebyggande och motverkande av radikalisering och våldsam extremism är avgörande för säkerheten inom EU[90]. Det behövs ytterligare åtgärder för att utveckla partnerskap för terrorismbekämpning och samarbete med länder i grannskapet och övriga världen, där man utnyttjar expertkunskapen

[85] Under de senaste två åren har det förekommit flera fall både i Europa (Frankrike, Tyskland och Italien) och på andra ställen (Tunisien och Indonesien) där biologiska agens använts (vanligen växtbaserade toxiner).

[86] Rådet har antagit restriktiva åtgärder mot spridning och användning av kemiska vapen.

[87] Kemikalier som kan missbrukas för att tillverka hemmagjorda sprängämnen. Dessa regleras i förordning (EU) 2019/1148 om marknadsföring och användning av sprängämnesprekursorer.

[88] Några exempel på sådana förödande angrepp är attackerna i Oslo (2011), Paris (2015), Bryssel (2016) och Manchester (2017). I en attack med hemmagjorda sprängämnen i Lyon 2019 skadades tretton personer.

[89] Däribland det nya mandatet för Europeiska gräns- och kustbevakningsbyrån (Frontex).

[90] I rådets slutsatser av den 16 juni 2020 underströks behovet av att EU:s medborgare skyddas mot terrorism och våldsam extremism i alla former och oberoende av deras ursprung, och att ytterligare förstärka EU:s engagemang och åtgärder för terrorismbekämpning inom vissa prioriterade geografiska och tematiska områden.

inom nätverket för kampen mot terrorism i EU/säkerhetsexperter. Den gemensamma handlingsplanen för terrorismbekämpning på västra Balkan är ett bra exempel på sådant riktat samarbete. Framför allt bör insatser göras för att stödja partnerländernas kapacitet att identifiera och lokalisera utländska terroriststridande. EU ska också fortsätta att stödja multilateralt samarbete och arbeta med de ledande aktörerna på detta område, så som FN, Nato, Europarådet, Interpol och OSSE. Man ska också samarbeta med det globala forumet för terroristbekämpning och den globala koalitionen mot Daish, liksom relevanta aktörer i civilsamhället. Unionens utrikespolitiska instrument, inbegripet utveckling och samarbete, spelar också en viktig roll vid samarbetet med tredjeländer för att förebygga terrorism och piratdåd. Internationellt samarbete är också viktigt för att strypa alla källor till **finansiering av terrorism**, exempelvis genom arbetsgruppen för finansiella åtgärder.

Organiserad brottslighet

Den organiserade brottsligheten innebär en enorm ekonomisk och personlig kostnad. Den ekonomiska förlusten på grund av organiserad brottslighet och korruption har uppskattats till mellan 218 och 282 miljarder euro per år[91]. Över 5 000 organiserade kriminella grupper var under utredning i Europa under 2017 – en ökning med 50 % jämfört med 2013[92]. Organiserad brottslighet bedrivs allt mer över gränserna, inbegripet i EU:s omedelbara grannskap, vilket kräver ett intensifierat operativt samarbete och informationsutbyte med partner i grannskapet.

Nya utmaningar uppstår och brotten går ut på nätet. Under covid-19-pandemin märktes en enorm ökning av nätbedrägerier mot utsatta grupper, och hälso- och sanitetsprodukter blev föremål för stölder och inbrott[93]. EU måste öka sitt arbete mot organiserad brottslighet, även på internationell nivå, med fler redskap för att nedmontera den organiserade brottslighetens affärsmodell. Att bekämpa den organiserade brottsligheten kräver också ett nära samarbete med lokala och regionala myndigheter och med civilsamhället, som är främsta partner både när det gäller brottsförebyggande arbete och hjälp och assistans till brottsoffer. Ett särskilt stort behov finns i förvaltningarna i gränsregioner. Detta arbete kommer att samlas i en **agenda för att bekämpa organiserad brottslighet**.

Mer än en tredjedel av de organiserade kriminella grupper som är verksamma i EU är inblandade i produktion, handel eller distribution av narkotika. Narkotikamissbruk ledde till över åttatusen dödsfall på grund av överdoser i EU under 2019. Större delen av **narkotikahandeln** sker över gränserna och mycket av vinsterna infiltrerar den lagliga ekonomin[94]. En ny EU-agenda om narkotika[95] kommer att stärka EU:s och medlemsstaternas insatser för att minska efterfrågan och tillgången på narkotika, fastställa gemensamma åtgärder mot ett gemensamt problem och öka dialogen och samarbetet mellan EU och externa partner i narkotikafrågor. Efter en utvärdering av Europeiska centrumet för kontroll av narkotika och narkotikamissbruk ska kommissionen bedöma om dess mandat behöver uppdateras för att klara nya utmaningar.

Organiserade kriminella grupper och terrorister är också nyckelspelare i handeln med **illegala skjutvapen**. Mellan 2009 och 2018 skedde 23 masskjutningar i Europa, med mer än

[91] I bruttonationalprodukt (BNP); Europols rapport: ”Does crime still pay?” – Criminal asset recovery in the EU, 2016.
[92] Europol, hotbildsbedömningar avseende den grova organiserade brottsligheten (Socta) 2013 och 2017.
[93] Europol, 2020.
[94] EMCDDA och Europol, Rapport om narkotikamarknaden i EU 2019. (November 2019).
[95] *EU Drugs Agenda and Action Plan 2021-2025*, COM(2020) 606.

340 döda[96]. Skjutvapen smugglas ofta till EU genom dess omedelbara grannskap[97]. Det tyder på ett behov av att öka samordningen och samarbetet såväl inom EU som med internationella partner, särskilt Interpol, för att harmonisera informationsinsamlingen och rapporteringen om beslag av skjutvapen. Det är också mycket viktigt att förbättra spårbarheten för vapen, inbegripet på nätet, och säkerställa informationsutbyte mellan tillståndsmyndigheter och polis och åklagare. Kommissionen lägger fram en ny **EU-handlingsplan mot olaglig handel med skjutvapen**[98] och ska också bedöma om bestämmelserna om exporttillstånd och import- och transiteringsåtgärder för skjutvapen fortfarande är ändamålsenliga[99].

Kriminella organisationer behandlar migranter och personer i behov av internationellt skydd som handelsvaror. 90 % av de irreguljära migranter som anländer till EU har fått hjälp av ett kriminellt nätverk[100]. Smuggling av migranter hör också ofta ihop med andra former av organiserad brottslighet, särskilt människohandel[101]. Förutom det enorma mänskliga lidandet inom människohandel, uppskattar Europol att den årliga vinsten för alla former av utnyttjande i människohandel uppgår till 29,4 miljarder euro per år globalt. Detta är en gränsöverskridande brottslighet som livnär sig på olaglig efterfrågan inom och utanför EU och som påverkar alla medlemsstater. Det dåliga resultatet när det gäller att identifiera, lagföra och bestraffa dessa brott innebär att det krävs en ny strategi för att intensifiera åtgärderna. En ny **omfattande strategi mot människohandel** ska knyta ihop de olika åtgärderna. Dessutom ska kommissionen lägga fram en **ny EU-handlingsplan mot smuggling av migranter** för 2021–2025. Båda områdena ska inriktas på att bekämpa kriminella nätverk, öka samarbetet och stödja de brottsbekämpande myndigheternas arbete.

Organiserade kriminella grupper söker också, precis som terrorister, möjligheter på andra områden, särskilt områden som genererar stora förtjänster med låg risk att upptäckas, såsom **miljöbrott**. Olaglig jakt och handel med vilda djur, olaglig gruvdrift, avverkning och olaglig hantering och transport av avfall har blivit den fjärde största kriminella verksamheten världen över[102]. Det har också förekommit ett kriminellt utnyttjande av utsläppsrätter och system för energicertifikat, och missbruk av medel som avsatts för miljömässig resiliens och hållbar utveckling. Förutom att kommissionen stöder åtgärder från EU, medlemsstaterna och det internationella samfundet för att intensifiera satsningarna mot miljöbrott[103], ska den även bedöma om direktivet om miljöbrott[104] fortfarande är ändamålsenligt. **Handel med kulturföremål** har också blivit en av de mest lukrativa kriminella verksamheterna, en källa till finansiering för såväl terrorister som organiserad brottslighet, och den ökar hela tiden. Åtgärder bör vidtas för att förbättra spårbarheten för kulturföremål på och utanför nätet, på

[96] Flemish Peace Institute, Armed to kill. (oktober 2019)

[97] EU har finansierat kampen mot spridning av och handel med handeldvapen och lätta vapen i regionen sedan 2002, och har bland annat finansierat nätverket för skjutvapenexperter i Sydösteuropa (Seefen). Sedan 2019 är partnerländerna på västra Balkan fullt engagerade i prioriteringen av skjutvapen inom Europeiska sektorsövergripande plattformen mot brottshot (Empact).

[98] COM(2020) 608.

[99] Europaparlamentets och rådets förordning (EU) nr 258/2012 av den 14 mars 2012 om genomförande av artikel 10 i FN:s protokoll om olaglig tillverkning av och handel med eldvapen.

[100] Källa: Europol.

[101] Europol, Europeiska centrumet för bekämpning av människosmuggling (EMSC), 4:e årsrapporten.

[102] FN:s miljöprograms (Unep) och Interpols bedömning av snabbinsatser: The Rise of Environmental Crime, juni 2016.

[103] Se *Den europeiska gröna given*, COM(2019) 640 final.

[104] Europaparlamentets och rådets direktiv 2008/99/EG om skydd för miljön genom straffrättsliga bestämmelser.

den inre marknaden och i samarbete med tredjeländer där kulturföremål plundrats och tillhandahålla aktivt stöd till polis och forskare.

Ekobrott är mycket komplexa, men de påverkar varje år miljontals medborgare och tusentals företag i EU. Det är mycket viktigt att bekämpa bedrägeri och det kräver åtgärder på EU-nivå. Europol, tillsammans med Eurojust, Europeiska åklagarmyndigheten och Europeiska byrån för bedrägeribekämpning, stöder medlemsstaterna och EU med att skydda de ekonomiska och finansiella marknaderna och skattebetalarnas pengar. Europeiska åklagarmyndigheten ska vara helt operativ i slutet av 2020 och utreda, lagföra och väcka talan mot brott mot unionens budget, såsom bedrägeri, korruption och penningtvätt. Den ska också ta itu med gränsöverskridande momsbedrägerier som varje år kostar skattebetalarna minst 50 miljarder euro.

Kommissionen ska också stödja utvecklingen av expertis och en rättslig ram mot nya, framväxande risker, som kryptotillgångar och nya betalningssystem. Framför allt planerar kommissionen att titta på hur man ska hantera framväxten av kryptotillgångar som bitcoin och den nya teknikens effekter på hur man utfärdar, handlar med och får tillgång till finansiella tillgångar.

Det bör råda nolltolerans inom Europeiska unionen när det gäller olagliga pengar. Under mer än trettio år har EU utvecklat ett stabilt regelverk för att förhindra och bekämpa **penningtvätt** och finansiering av terrorism, med full respekt för behovet av att skydda personuppgifter. Det råder dock allt större enighet om att genomförandet av det nuvarande ramverket behöver avsevärda förbättringar. Det är stora skillnader i hur ramverket tillämpas och finns allvarliga brister i efterlevnaden av bestämmelserna, vilket måste åtgärdas. Som angavs i handlingsplanen från maj 2020[105] har arbetet påbörjats med att bedöma alternativ för att stärka EU:s ram för att bekämpa penningtvätt och motverka finansiering av terrorism. Områden som ska undersökas omfattar sammankoppling av nationella centraliserade bankkontoregister, vilket avsevärt skulle kunna påskynda tillgången till finansiell information för finansunderrättelseenheter och behöriga myndigheter.

De organiserade kriminella gruppernas förtjänst uppskattas till 110 miljarder per år i EU. De nuvarande åtgärderna omfattar harmoniserad lagstiftning om förverkande och återvinning av tillgångar[106], för att förbättra frysningen och förverkandet av kriminella tillgångar i EU och underlätta ömsesidigt förtroende och effektivt gränsöverskridande samarbete mellan medlemsstaterna. Det är dock bara ungefär 1 % av dessa förtjänster som förverkas[107], vilket innebär att de kriminella grupperna kan investera i att utöka sin brottsliga verksamhet och nästla sig in i den lagliga ekonomin. Små och medelstora företag som har svårt att få tillgång till krediter är en viktig målgrupp för penningtvätt. Kommissionen ska analysera genomförandet av lagstiftningen[108] och det eventuella behovet av ytterligare gemensamma regelverk, inbegripet förverkande utan föregående fällande dom. Kontoren för återvinning av tillgångar[109], som är de främsta aktörerna när det gäller återvinning av tillgångar, skulle också kunna utrustas med bättre verktyg för att identifiera och spåra

[105] *Action Plan on preventing money laundering and terrorist financing*, COM(2020) 2800.

[106] Enligt unionsrätten måste kontor för återvinning av tillgångar inrättas i alla medlemsstater.

[107] *Rapport om återvinning och förverkande av tillgångar: Åtgärder för att se till att brott inte lönar sig*, COM(2020) 217 final.

[108] Europaparlamentets och rådets direktiv 2014/42/EU av den 3 april 2014 om frysning och förverkande av hjälpmedel vid och vinning av brott i Europeiska unionen.

[109] Rådets beslut 2007/845/RIF av den 6 december 2007 om samarbete mellan medlemsstaternas kontor för återvinning av tillgångar när det gäller att spåra och identifiera vinning eller annan egendom som härrör från brott.

tillgångar på ett snabbare sätt över hela unionen och på så sätt öka andelen förverkade tillgångar.

Det finns en stark koppling mellan organiserad brottslighet och **korruption**. En grov uppskattning tyder på att enbart korruptionen kostar EU:s ekonomi 120 miljarder euro per år[110]. Förhindrandet av och kampen mot korruption kommer även i fortsättningen att övervakas regelbundet enligt rättsstatsmekanismen och den europeiska planeringsterminen. Europeiska planeringsterminen har bedömt utmaningarna i kampen mot korruption, såsom offentlig upphandling, offentlig förvaltning, affärsmiljön och sjukvården. Kommissionens nya årsrapport om rättsstatsprincipen kommer att omfatta kampen mot korruption och möjliggöra en förebyggande dialog med nationella myndigheter och berörda aktörer på EU-nivå och nationell nivå. Civilsamhällets organisationer kan också spela en viktig roll i att stimulera myndigheternas åtgärder när det gäller att förebygga och bekämpa organiserad brottslighet och korruption, och de grupperna skulle också med fördel kunna sammanföras i ett gemensamt forum. På grund av sin gränsöverskridande karaktär är samarbete med och bistånd till regioner som gränsar till EU en annan viktig dimension när det gäller organiserad brottslighet och korruption.

Centrala åtgärder
• Agenda för terrorismbekämpning för EU, inbegripet förnyade insatser mot radikalisering i EU • Nytt samarbete med viktiga tredjeländer och internationella organisationer mot terrorism • Handlingsplan för att bekämpa organiserad brottslighet, inklusive människohandel • EU:s agenda för narkotikapolitiken och handlingsplan 2021–2025 • Bedömning av Europeiska centrumet för kontroll av narkotika och narkotikamissbruk • EU:s handlingsplan mot olaglig handel med skjutvapen 2020–2025 • Översyn av lagstiftningen om beslut om frysning och förverkande och om kontor för återvinning av tillgångar • Bedömning av direktivet om miljöbrott • EU:s åtgärdsplan mot smuggling av migranter, 2021–2025

4. Ett starkt säkerhetsekosystem

En genuin och effektiv säkerhetsunion måste vara något som alla delar av 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, brottsoffer samt vittnen.

All politik behöver en ny säkerhetsdimension och EU kan bidra på alla nivåer. Våld i hemmet är en av de allvarligaste säkerhetsriskerna. I EU har 22 % av kvinnorna utsatts för våld i en nära relation[111]. EU:s anslutning till Istanbulkonventionen om att förebygga och bekämpa våld mot kvinnor och våld i hemmet är fortsatt en viktig prioritering. Om förhandlingarna förblir strandade kommer kommissionen att vidta andra åtgärder för att uppnå samma mål som konventionen, inbegripet förslaget att lägga till våld mot kvinnor i den förteckning över brott som anges i fördraget.

[110] Det är svårt att uppskatta korruptionens totala ekonomiska kostnader, även om försök har gjorts av organ som Internationella handelskammaren, Transparency International, FN:s Global Compact och Världsekonomiskt forum som antyder att kostnaderna för korruptionen uppgår till 5 % av världens BNP.

[111] *En jämlikhetsunion: jämställdhetsstrategi för 2020–2025*, COM(2020) 152.

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 de kraftfullaste verktygen när man ska bekämpa brott och terrorism och utöva rättvisa. Om det ska vara effektivt måste det vara målinriktat och ske vid rätt tidpunkt. Om det ska vara tillförlitligt måste det användas tillsammans med gemensamma skyddsåtgärder och kontroller.

Ett antal EU-instrument och sektorsspecifika strategier[112] har tagits fram för att ytterligare utveckla **det operativa brottsbekämpande samarbetet** mellan medlemsstaterna. Ett av de viktigaste EU-instrumenten till stöd för polissamarbete mellan medlemsstaterna är Schengens informationssystem som används för att utbyta uppgifter om efterlysta och saknade personer och föremål i realtid. Resultatet har märkts i gripande av brottslingar, narkotikabeslag och räddning av potentiella offer[113]. Samarbetet skulle dock kunna öka genom rationalisering och uppgradering av de tillgängliga instrumenten. Större delen av EU:s rättsliga ram som ligger till grund för det operativa polissamarbetet utformades för 30 år sedan. Ett komplext nät av bilaterala avtal mellan medlemsstaterna, varav många är föråldrade eller underutnyttjade, ger risk för fragmentering. I mindre eller kustlösa länder måste poliser som arbetar över gränserna i vissa fall genomföra operativa insatser enligt upp till sju olika regelverk. Resultatet blir att vissa insatser, som förföljande av misstänkta personer över de inre gränserna, helt enkelt inte blir av. Operativt samarbete kring ny teknik såsom drönare omfattas inte heller av den nuvarande EU-ramen .

Operativ ändamålsenlighet kan stödjas med specifikt polissamarbete, som också kan bidra till att ge ett viktigt stöd till andra politiska mål – som synpunkter på säkerheten i den nya bedömningen av utländska direktinvesteringar. Kommissionen kommer att undersöka hur en kod för polissamarbete kan stödja detta. Medlemsstaternas polis och åklagare har allt oftare utnyttjat stöd och expertkunskap på EU-nivå, medan EU Intcen har spelat en central roll när det gäller att främja utbyte av strategiska underrättelser mellan medlemsstaternas underrättelsetjänster och säkerhetstjänster som tillhandahåller information och lägesanalyser till förmån för EU-institutionerna[114]. **Europol** kan också spela en viktig roll genom att utöka sitt samarbete med tredjeländer för att bekämpa brott och terrorism i enlighet med andra externa politikområden och verktyg. Europol står dock inför ett antal allvarliga begränsningar idag – särskilt vad gäller det direkta utbytet av personuppgifter med privata parter – som hindrar dem från att effektivt stödja medlemsstaterna i kampen mot terrorism och brottslighet. Europols mandat utvärderas just nu för att man ska se hur det bör förbättras för att säkerställa att byrån kan utföra sina uppgifter fullt ut. I detta sammanhang bör relevanta myndigheter på EU-nivå (som Olaf, Europol, Eurojust och Europeiska åklagarmyndigheten) också ha ett närmare samarbete och förbättra informationsutbytet.

En annan viktig koppling är vidareutvecklingen av **Eurojust** för att maximera synergierna mellan det brottsbekämpande samarbetet och det straffrättsliga samarbetet. EU skulle också ha fördel av en mer strategisk samstämmighet: **Empact**[115], EU:s policycykel avseende organiserad och grov internationell brottslighet, erbjuder myndigheterna en

[112] Exempelvis EU:s strategi för sjöfartsskydd som ledde till stora framsteg med samarbetet med kustbevakningsuppgifter mellan relevanta EU-byråer.
[113] EU:s kamp mot organiserad brottslighet 2019 (rådet, 2020).
[114] EU Intcen fungerar som den samlade ingången för medlemsstaternas underrättelse- och säkerhetstjänster för att tillhandahålla underrättelsestyrda lägesanalyser till EU.
[115] Empact står för Europeiska sektorsövergripande plattformen mot brottshot

underrättelsestyrd metod för att gemensamt ta itu med de viktigaste brottshoten som påverkar EU. Det har gett goda operativa resultat[116] under de senaste tio åren. Utifrån de yrkesverksammas erfarenhet bör den befintliga mekanismen rationaliseras och förenklas för att man bättre ska kunna hantera de mest brådskande och föränderliga brottshoten inför en ny policycykel 2022–2025.

Aktuell och relevant **information** är nyckeln till det dagliga arbetet med att motverka brott. Trots utvecklingen av nya EU-databaser för säkerhet och gränsförvaltning finns mycket information fortfarande i nationella databaser eller utbyts utanför dessa verktyg. Det resulterar i ett avsevärt merarbete, förseningar och ökad risk för att viktig information förbises Bättre, snabbare och enklare processer, som omfattar hela säkerhetssektorn, skulle ge bättre resultat. Rätt verktyg är avgörande om informationsutbytet ska uppnå sin potential inom ändamålsenligt brottsbekämpande, med nödvändiga skyddsåtgärder så att datadelningen respekterar dataskyddslagar och grundläggande rättigheter. Mot bakgrund av den tekniska och forensiska utvecklingen, utvecklingen inom dataskydd och förändrade operativa behov bör EU överväga om det finns ett behov av att modernisera instrument som **2008 års Prümbeslut** som inrättade automatisk överföring av DNA, fingeravtryck och registreringsuppgifter för fordon, för att göra det möjligt att automatiskt överföra ytterligare uppgiftskategorier som redan finns tillgängliga i medlemsstaternas straffrättsliga och andra databaser för brottsutredningar. Dessutom kommer kommissionen att undersöka möjligheten att utbyta polisregister för att kontrollera om det finns några uppgifter om en person i andra medlemsstater, och underlätta tillgången till dessa uppgifter om de hittas, med alla nödvändiga skyddsåtgärder.

Information om resenärer har bidragit till att förbättra gränskontrollerna, minska den irreguljära migrationen och identifiera personer som utgör säkerhetsrisker. Förhandsinformation om passagerare är personuppgifter för varje passagerare som samlas in av lufttrafikföretag vid incheckning och i förväg sänds till gränskontrollmyndigheterna på bestämmelseorten. En översyn av den rättsliga ramen[117] kunde göra det möjligt att använda informationen på ett mer ändamålsenligt sätt, samtidigt som man säkerställer efterlevnaden av dataskyddslagstiftningen och underlätta passagerarflödet. Passageraruppgiftssamlingar (PNR-uppgifter) är de uppgifter som passagerare lämnar när de bokar flyg. Genomförandet av PNR-direktivet[118] är mycket viktigt och kommission kommer att fortsätta att stödja det och se till att det efterlevs. Som en åtgärd på medellång sikt kommer kommissionen dessutom att inleda en översyn av den nuvarande strategin för**överföring av PNR-uppgifter till tredjeländer**.

Straffrättsligt samarbete är ett nödvändigt komplement till polisens insatser för att bekämpa gränsöverskridande brottslighet. Straffrättsligt samarbete har genomgått en djupgående förändring under de senaste 20 åren. Organ som **europeiska åklagarmyndigheten** och **Eurojust** måste ha resurser för att kunna fungera i full utsträckning eller förstärkas. Samarbetet mellan rättstillämpare skulle också kunna förbättras genom ytterligare steg mot ömsesidigt erkännande av rättsliga avgöranden, juridisk utbildning och informationsutbyte. Målet bör vara att öka det ömsesidiga förtroendet mellan domare och åklagare, vilket är centralt om de gränsöverskridande förfaranden ska bli smidigare. Användningen av **digital teknik** kan också göra våra rättssystem effektivare. Ett

[116] https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf

[117] Rådets direktiv 2004/82/EG av den 29 april 2004 om skyldighet för transportörer att lämna uppgifter om passagerare.

[118] Direktiv (EU) 2016/681 av den 27 april 2016 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet.

nytt system för digitalt utbyte håller på att inrättas för att överföra europeiska utredningsorder, begäranden om ömsesidig rättslig hjälp och kommunikation mellan medlemsstaterna, som stöds av Eurojust. Kommissionen kommer att samarbeta med medlemsstaterna för att skynda på införandet av de nödvändiga it-systemen på nationell nivå.

Internationellt samarbete är också viktigt för ändamålsenlig brottsbekämpning och straffrättsligt samarbete. Bilaterala avtal med viktiga partner spelar en central roll när det gäller att säkra information och bevismaterial från länder utanför EU. **Interpol,** en av de största mellanstatliga kriminalpolisorganisationerna, spelar en viktig roll. Kommissionen kommer att undersöka möjliga sätt att förstärka samarbetet med Interpol, inbegripet eventuell tillgång till Interpols databaser och förstärkning av det operativa och strategiska samarbetet. Polis och åklagare i EU förlitar sig också på viktiga partnerländer för att upptäcka och utreda brottslingar och terrorister. **Partnerskap på säkerhetsområdet mellan EU och tredjeländer** skulle kunna intensifieras för att öka samarbetet för att motverka gemensamma hot som terrorism, organiserad brottslighet, cyberbrott, sexuella övergrepp mot barn och människohandel. En sådan strategi skulle bygga på gemensamma säkerhetsintressen och på etablerade dialoger om samarbete och säkerhet.

Precis som informationsutbyte kan utbyte av expertkunskap vara särskilt värdefullt när det gäller att öka polisens beredskap mot **icke-traditionella hot**. Förutom att uppmuntra utbyte av bästa praxis kommer kommissionen att undersöka en eventuell **samordningsmekanism på EU-nivå för polisstyrkor** i händelse av force majeure som pandemier. Pandemin har också visat att digital närpolisverksamhet, tillsammans med rättsliga ramar för att underlätta polisarbetet på nätet, kommer att bli grundläggande för att bekämpa brottslighet och terrorism. Partnerskap mellan polis och allmänhet, på nätet och utanför, kan förebygga brott och mildra effekterna av organiserad brottslighet, radikalisering och terroristverksamhet. Kopplingen mellan polislösningar på lokal, regional, nationell och unionsnivå är en viktig framgångsfaktor EU:s säkerhetsunion som helhet.

Betydelsen av starka yttre gränser

Med modern och effektiv förvaltning av de yttre gränserna kan dubbla fördelar uppnås: Schengenområdets integritet bevaras och våra medborgares säkerhet tryggas. Om alla relevanta aktörer engageras för att göra mesta möjliga av säkerheten vid gränsen kan det få en verklig effekt på förebyggandet av gränsöverskridande brottslighet och terrorism. Gemensam operativ verksamhet inom den nyligen förstärkta europeiska gräns- och kustbevakningen[119] bidrar till att förebygga och upptäcka gränsöverskridande brottslighet vid de **yttre gränserna** och utanför EU. Tullens verksamhet för att upptäcka säkerhetsrisker hos alla varor innan de anländer till EU och kontrollera varor när de anländer är avgörande i kampen mot gränsöverskridande brottslighet och terrorism. Den kommande handlingsplanen för tullunionen kommer att innehålla åtgärder för att stärka riskhanteringen och öka den inre säkerheten, bland annat genom en bedömning av genomförbarheten av en koppling mellan relevanta informationssystem för analys av säkerhetsrisken.

Ramverket för **interoperabilitet mellan EU:s informationssystem** på området rättsliga och inrikes frågor antogs i maj 2019. Denna nya struktur syftar till att förbättra effektiviteten och

[119] Består av Europeiska gräns- och kustbevakningsbyrån (Frontex) och medlemsstaternas gränsbevakningsmyndigheter och kustbevakningsmyndigheter.

ändamålsenligheten hos de nya eller uppgraderade informationssystemen[120]. Det ska leda till snabbare och mer systematisk information för poliser, gränsvakter och migrationstjänstemän. Det ska underlätta korrekt identifiering och bidra till att bekämpa identitetsbedrägeri. För att detta ska bli verklighet måste genomförandet av interoperabilitet vara en prioritering, både på politisk och teknisk nivå. Nära samarbete mellan EU:s organ och alla medlemsstater kommer att vara av största vikt för att uppnå målet om full interoperabilitet till 2023.

Bedrägerier med resedokument anses vara ett av de vanligaste brotten. Det underlättar för brottslingar och terrorister att förflytta sig i hemlighet, och det spelar en viktig roll i människohandeln och i narkotikahandeln[121]. Kommissionen ska undersöka hur man kan utvidga det nuvarande arbetet med säkerhetsnormer i EU:s uppehålls- och resehandlingar, inklusive genom digitalisering. Från och med augusti 2021 kommer medlemsstaterna att börja utfärda identitetshandlingar och uppehållstillstånd i enlighet med harmoniserade säkerhetsnormer, inklusive ett chip med biometriska kännetecken som kan kontrolleras av alla gränsmyndigheter i EU. Kommissionen kommer att övervaka genomförandet av de nya bestämmelserna, inklusive det successiva utbytet av dokument som för närvarande är i omlopp.

Förstärkt forskning och innovation på säkerhetsområdet

Arbetet med att säkerställa cybersäkerhet och bekämpa organiserad brottslighet, cyberbrott och terrorism bygger i högsta grad på att det utvecklas verktyg för denna framtid: att bidra till att skapa säkrare teknik, hantera utmaningar som tekniken medför och stödja arbetet med brottsbekämpning. Detta bygger i sin tur på privata partner och näringslivet.

Innovation bör ses som ett strategiskt verktyg för att motverka aktuella hot och föregripa såväl framtida risker som möjligheter. Innovativ teknik kan skapa nya verktyg för att hjälpa polis och andra aktörer inom säkerhet. Artificiell intelligens och stordataanalys skulle kunna utnyttja högpresterande datorsystem och ge lättare upptäckt och snabb, omfattande analys[122]. En viktig förutsättning för att utveckla tillförlitlig teknik är data av hög kvalitet, som finns tillgängliga för de behöriga myndigheterna så att de kan träna, testa och validera algoritmer[123]. Mer allmänt är risken för teknikberoende stor idag – EU är exempelvis nettoimportör av produkter och tjänster för cybersäkerhet, med allt vad det innebär för ekonomi och för samhällsviktig infrastruktur. Om EU ska bemästra tekniken och kunna garantera kontinuerlig leverans även vid ogynnsamma händelser och kriser, behövs närvaro och kapacitet i de samhällsviktiga delarna av relevanta värdekedjor.

EU:s **forskning, innovation och tekniska utveckling** ger tillfälle att beakta säkerhetsaspekten allt eftersom denna teknik och dess användningsområden utvecklas. Förslagen inom nästa omgång EU-finansiering kan fungera som viktig stimulans[124]. I

[120] In- och utresesystem (EES), EU-systemet för reseuppgifter och resetillstånd (Etias), det utökade europeiska informationssystemet för utbyte av uppgifter ur kriminalregister (Ecris-TCN), Schengens informationssystem, Informationssystemet för viseringar och det framtida uppdaterade Eurodac.

[121] Kopplingen mellan dokumentförfalskning och människohandel beskrivs i den andra rapporten om de framsteg som gjorts i kampen mot människohandel, COM(2018) 777 och det tillhörande SWD(2018) 473 och Europol, situationsrapporten om människohandel i EU, 2016.

[122] I detta ska kommissionens strategi om artificiell intelligens användas.

[123] *En EU-strategi för data*, COM(2020) 66 final.

[124] Kommissionens förslag till Horisont Europa, Fonden för inre säkerhet, Fonden för integrerad gränsförvaltning, programmet InvestEU, Europeiska regionala utvecklingsfonden och programmet för ett digitalt Europa kommer alla att stödja utvecklingen och spridningen av säkerhetsteknik och säkerhetslösningar i säkerhetssektorns värdekedja.

initiativ om europeiska dataområden och molninfrastruktur har säkerheten beaktats redan från början. Europeiska centrumet för cybersäkerhet inom näringsliv, teknik och forskning och nätverket av nationella samordningscentrum[125] syftar till att inrätta en ändamålsenlig och effektiv struktur för att samla och dela forskningskapaciteten och resultaten inom cybersäkerhet. Unionens rymdprogram tillhandahåller tjänster som stöder säkerheten för EU, medlemsstaterna och enskilda personer[126].

Sedan 2007 har över 600 projekt till ett sammanlagt värde av närmare 3 miljarder euro inletts inom den EU-finansierade säkerhetsforskningen och det gör den till ett viktigt instrument för att driva på teknik och kunskap till stöd för säkerhetslösningar. Som en del i översynen av Europols mandat kommer kommissionen att undersöka inrättandet av en **europeisk innovationsknutpunkt för inre säkerhet**[127]. Syftet skulle vara att tillhandahålla gemensamma lösningar på gemensamma säkerhetsutmaningar och säkerhetsmöjligheter, som medlemsstaterna kanske inte skulle kunna utnyttja ensamma. Samarbete är grundläggande för att rikta investeringarna för att få bästa effekt och utveckla innovativ teknik med såväl säkerhetsmässiga som ekonomiska fördelar.

Kompetens och ökad medvetenhet

Om vi ska kunna bygga ett mer motståndskraftigt samhälle med bättre förberedda företag, förvaltningar och enskilda personer är det mycket viktigt med medvetenhet om säkerhetsfrågor och kompetens att hantera eventuella hot. Utmaningar för it-infrastrukturen och e-systemen har visat på behovet att förbättra vår kapacitet för beredskap och insatser på cybersäkerhetsområdet. Pandemin har också belyst digitaliseringens betydelse på alla områden i EU:s ekonomi och samhälle.

Även **grundläggande kunskaper om säkerhetshot** och hur de kan bekämpas kan ha en verklig inverkan på samhällets resiliens. Medvetenhet om riskerna för cyberbrott och om behovet att skydda sig själv från dem kan tillsammans med skydd från tjänsteleverantörer fungera för att bekämpa cyberattacker. Information om faror och risker med narkotikasmuggling kan göra det svårare för brottslingar att lyckas. EU kan uppmuntra spridning av bästa praxis som genom nätverket av centrum för säkrare internet[128] och kan se till att sådana mål tas med i dess egna program.

Den framtida handlingsplanen för digital utbildning bör innehålla riktade åtgärder för att bygga upp kunskapen om it-säkerhet för hela befolkningen. Den nyligen antagna kompetensagendan[129] stöder kompetensutveckling livet igenom. Det omfattar också insatser för att öka antalet utexaminerade inom naturvetenskap, teknik, ingenjörsvetenskap, humaniora och matematik som behövs inom sådana spetsområden som cybersäkerhet. Ytterligare insatser som finansieras genom programmet för ett digitalt Europa kommer att

[125] *Förslag av den 12 september 2018 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum*, COM(2018) 630 final.

[126] Copernicus, till exempel, erbjuder tjänster som möjliggör övervakning av EU:s yttre gränser och sjöövervakning som underlättar insatser mot piratdåd och smuggling, och stöder också samhällsviktig infrastruktur. När Copernicus är helt i drift kommer det att vara en viktig möjliggörande faktor för civila och militära uppdrag och insatser.

[127] Detta skulle också fungera med Frontex, Cepol, eu-LISA och Gemensamma forskningscentrumet.

[128] Se www.betterinternetforkids.eu: Den centrala portalen och de nationella centrumen för ett säkrare Internet finansieras för närvarande inom ramen för Fonden för ett sammanlänkat Europa, och den framtida finansieringen har förslagits inom ramen för programmet för ett digitalt Europa.

[129] *Den europeiska kompetensagendan för hållbar konkurrenskraft, social rättvisa och motståndskraft*, COM(2020) 274 final

göra det möjligt för yrkesverksamma att hänga med i utvecklingen inom säkerhetshot och samtidigt fylla bristen på detta område på EU:s arbetsmarknad. Den övergripande effekten kommer att bli att enskilda personer kan skaffa sig kompetens för att hantera säkerhetshot och företag kan hitta den arbetskraft de behöver på detta område. Det kommande europeiska forskningsområdet och det europeiska området för utbildning kommer också att främja karriärer inom naturvetenskap, teknik, ingenjörsvetenskap, humaniora och matematik.

Det är också viktigt att **brottsoffer** kan utöva sina rättigheter. De måste få den hjälp och det stöd de behöver med tanke på de specifika omständigheterna. Särskilda ansträngningar krävs när det gäller minoriteter och de mest utsatta brottsoffren, som barn och kvinnor som smugglas för sexuell exploatering eller utsätts för våld i hemmet[130].

Det finns ett särskilt behov av ökad **kompetens inom brottsbekämpning**. De nuvarande och de nya tekniska hoten kräver mer investeringar i kompetensutveckling för brottsbekämpande personal i ett så tidigt skede som möjligt och under hela deras yrkesverksamma liv. Cepol är en viktig partner för att bistå medlemsstaterna med denna uppgift. Utbildning i brottsbekämpande syfte med anknytning till rasism och främlingsfientlighet och mer allmänt medborgerliga rättigheter, måste bli en viktig del i ett säkerhetstänkande i EU. Nationella rättssystem och rättstillämpare måste också vara rustade för att kunna anpassa sig och möta nya utmaningar. Utbildning är avgörande för att myndigheterna på fältet ska kunna använda verktygen i en operativ situation. Dessutom bör alla ansträngningar göras för att öka jämställdhetsintegrering och stärka kvinnors deltagande i brottsbekämpningen.

Centrala åtgärder
• Stärka Europols mandat • Undersöka en EU-kod för polissamarbete och polissamordning vid krislägen • Stärka Eurojust för att koppla samman straffrättsliga och brottsbekämpande myndigheter • Se över direktivet om förhandsinformation om passagerare • Meddelande om den externa dimensionen av passageraruppgifter • Stärka samarbetet mellan EU och Interpol • Ett ramverk för att förhandla med viktiga tredjeländer om informationsutbyte • Bättre säkerhetsnormer för resehandlingar • Undersöka en europeisk innovationsknutpunkt för inre säkerhet

V. Slutsatser

I en allt mer turbulent värld betraktas Europeiska unionen fortfarande allmänt som en av de säkraste och tryggaste platserna. Det är dock ingenting man kan ta för givet.

Den nya strategin för säkerhetsunionen lägger grunden för ett säkerhetsekosystem som täcker hela det europeiska samhället. Den bygger på insikten att säkerheten är ett gemensamt ansvar. Säkerhet är en fråga som berör alla. Alla offentliga organ, företag, sociala organisationer, institutioner och medborgare måste ta sitt ansvar för att göra samhället säkrare.

Säkerhetsfrågor måste nu ses ur ett mycket bredare perspektiv än tidigare. En felaktig åtskillnad mellan det fysiska och det digitala måste undanröjas. I EU:s säkerhetsunion

[130] Se *Jämställdhetsstrategin*, COM(2020) 152, *EU-strategi för brottsoffers rättigheter*, COM(2020) 258 och *EU:s strategi för ett bättre internet för barn*, COM(2012) 196.

sammanförs hela skalan av säkerhetsbehov och den inriktas på de områden som är mest kritiska för EU:s säkerhet under de närmaste åren. I den framhålls också att säkerhetshot inte respekterar de geografiska gränserna och att det finns en allt större koppling mellan inre och yttre säkerhet[131]. I det sammanhanget kommer det att vara viktigt för EU att samarbeta med internationella partner för att skydda alla EU-medborgare och upprätthålla ett nära samarbete med EU:s yttre åtgärder när den här strategin genomförs.

Vår säkerhet är kopplad till våra grundläggande värden. Alla åtgärder och initiativ som föreslås i denna strategi kommer fullt ut att respektera de grundläggande rättigheterna och våra europeiska värden. De utgör grundvalen för vår europeiska livsstil och måste förbli kärnan i allt vårt arbete.

Slutligen är kommissionen fortfarande fullt medveten om det faktum att ingen politik eller åtgärd är bättre än sitt genomförande. Det krävs därför ett oförtröttligt arbete med att genomföra och efterleva den nuvarande och framtida lagstiftningen på rätt sätt. Detta kommer att övervakas genom regelbundna rapporter om säkerhetsunionen och kommissionen kommer att hålla Europaparlamentet, rådet och berörda parter fullt informerade och delaktiga i alla relevanta åtgärder. Dessutom är kommissionen redo att delta i och organisera gemensamma debatter med institutionerna om säkerhetsunionen för att göra en samlad bedömning av de framsteg som görs samtidigt som man tillsammans tittar på kommande utmaningar.

Kommissionen uppmanar Europaparlamentet och rådet att godkänna denna strategi för en säkerhetsunion som en grund för samarbete och gemensamma åtgärder för säkerhet under de kommande fem åren.

[131] Se EU:s globala strategi