EUROPEISKA
KOMMISSIONEN

Bryssel den 30.10.2019
COM(2019) 552 final

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET, EUROPEISKA RÅDET OCH RÅDET

Tjugonde rapporten om framsteg i riktning mot en effektiv och verklig säkerhetsunion

I. INLEDNING

Detta är den tjugonde rapporten om ytterligare framsteg i riktning mot en effektiv och verklig säkerhetsunion. Rapporten omfattar utvecklingen inom två huvudområden: dels bekämpning av terrorism, organiserad brottslighet och stöd till sådan verksamhet, dels förstärkning av försvaret inför och förmågan att stå emot dessa hot.

Junckerkommissionen har från dag ett gjort säkerheten till sin främsta prioritering. Med utgångspunkt i den europeiska säkerhetsagendan från april 2015[1] och meddelandet om att bana väg för en effektiv och verklig säkerhetsunion från april 2016[2] har EU på ett samordnat sätt svarat på en rad terrorattacker och andra växande säkerhetsutmaningar, och gjort betydande framsteg för att förbättra vår gemensamma säkerhet[3]. Det har blivit alltmer uppenbart att dagens säkerhetsutmaningar – om det så gäller terrorism, organiserad brottslighet, cyberattacker, desinformation eller andra nya cyberbaserade hot – är gemensamma hot. Endast genom att arbeta tillsammans kan vi uppnå den nivå av kollektiv säkerhet som medborgarna kräver och förväntar sig. Denna gemensamma syn har legat till grund för de framsteg som gjorts i riktning mot en effektiv och verklig säkerhetsunion. Stödet på EU-nivå har styrts av behoven hos de nationella myndigheter som arbetar med att skydda medborgarna, och har inriktats på lagstiftningsåtgärder och operativa åtgärder på de områden där gemensamma insatser kan öka medlemsstaternas säkerhet. Arbetet har utförts i nära samarbete med Europaparlamentet och rådet och med full insyn för allmänheten. Full respekt för de grundläggande rättigheterna har genomsyrat detta arbete, eftersom unionens säkerhet enbart kan tryggas när medborgarna litar på att deras grundläggande rättigheter inte äventyras.

EU har arbetat med att **bekämpa terrorism** genom att strypa terroristernas handlingsutrymme med hjälp av nya regler som gör det svårare för dem att få tillgång till sprängämnen, skjutvapen och finansiering och genom att begränsa deras möjligheter att förflytta sig. EU har intensifierat **informationsutbytet** för att ge dem som befinner sig i frontlinjen, poliser och gränskontrolltjänstemän, effektiv tillgång till korrekta och fullständiga uppgifter så att man på bästa sätt kan utnyttja befintlig information och täppa till informationsluckor och döda vinklar. Ett starkt skydd av de yttre gränserna är en förutsättning för säkerheten inom området för fri rörlighet utan inre gränskontroller. I mars 2019 nådde Europaparlamentet och rådet en överenskommelse om en ytterligare förstärkt och fullt utrustad **europeisk gräns- och kustbevakning**. Den nya förordningen förväntas träda i kraft i början av december 2019. EU har tillhandahållit en plattform och finansiering för att de som arbetar på lokal nivå ska kunna utbyta bästa praxis om **bekämpning av radikalisering och förebyggande av våldsbejakande extremism**, och även föreslagit nya regler för att effektivt avlägsna terrorisminnehåll på nätet. EU:s stöd har hjälpt till att **göra städer motståndskraftigare** mot attacker, med handlingsplaner för att bidra till skyddet av offentliga platser och förbättra beredskapen för kemiska, biologiska, radiologiska och nukleära säkerhetsrisker. EU har bemött **cybersäkerhetshot och cyberbaserade hot** genom att införa en ny EU-strategi för cybersäkerhet och anta lämplig lagstiftning, samt genom åtgärder mot **desinformation** för att stärka skyddet av val. Arbete pågår för att stärka säkerheten i **kritisk digital infrastruktur**, bland annat genom ökat samarbete kring **cybersäkerheten i 5G-näten** i hela Europa.

---

1 COM(2015) 185 final (28.4.2015).
2 COM(2016) 230 final (20.4.2016).
3 Tidigare rapporter om framsteg i riktning mot en effektiv och verklig säkerhetsunion finns på https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en.

Det finns dock mycket kvar att göra. Den direktströmmade attacken mot en synagoga och mordet på två personer i Halle i Tyskland den 9 oktober 2019 var en chockerande påminnelse om hotet från våldsbejakande högerextremism och antisemitism. Det satte också strålkastarljuset på missbruket av internet för spridning av terroristpropaganda och därmed på **behovet av EU-övergripande regler om avlägsnande av terrorisminnehåll på nätet**. Den 7–8 oktober 2019 hade rådet (rättsliga och inrikes frågor) en debatt om våldsbejakande högerextremism och terrorism som lyfte fram behovet av ytterligare insatser, bland annat i fråga om spridning av olagligt våldsbejakande högerextremistiskt innehåll både på nätet och i andra sammanhang. Samtidigt visar mordet på tre poliser och en civilanställd i polishögkvarteret i Paris den 3 oktober 2019 att hotet från jihadistiskt inspirerad terrorism kvarstår och att de pågående insatserna för att stödja medlemsstaternas hantering av detta hot måste fortsätta. Det faktum att flera fängslade medlemmar av IS/Daish har flytt i samband med den senare tidens händelser i norra Syrien kan få allvarliga följder för säkerheten i Europa. Det är viktigt att medlemsstaterna fullt ut använder sig av befintliga informationssystem för att upptäcka och identifiera utländska terroriststridande som korsar de yttre gränserna. Arbete pågår också för att utnyttja information från slagfältet för att ställa utländska terroriststridande inför rätta.

Denna rapport beskriver de senaste framstegen i arbetet med att skapa en effektiv och verklig säkerhetsunion och lyfter fram de områden där ytterligare insatser krävs. Den ger en lägesbild av genomförandet av överenskomna åtgärder inom **cybersäkerheten i 5G-nät**, i synnerhet **EU:s riskbedömningsrapport** som offentliggjordes den 9 oktober 2019, och **bekämpandet av desinformation**.

Rapporten fokuserar framför allt på den **yttre dimensionen** av samarbetet i säkerhetsunionen, såsom undertecknandet av två bilaterala **överenskommelser om terrorismbekämpning** med Albanien och Nordmakedonien och framstegen i samarbetet med tredjelandspartner om utbyte av **passageraruppgifter**. Tillsammans med denna rapport har kommissionen även antagit en begäran om bemyndigande att inleda förhandlingar om ett avtal mellan EU och **Nya Zeeland** om utbyte av personuppgifter för att bekämpa grov brottslighet och terrorism.

II. FÖRVERKLIGANDE AV LAGSTIFTNINGSPRIORITERINGAR

1. Förebygga radikalisering på nätet och i samhället

Förebyggande av radikalisering är en hörnsten i unionens insatser mot hotet från terrorism. På detta område har internet blivit det viktigaste slagfältet för terroristaktioner under 2000-talet. Platser där radikaliserade personer kan kommunicera med varandra och dela innehåll skapar möjligheter för både våldsbejakande jihadistiska extremister och högerextremister att utveckla världsomspännande nätverk. Det är anledningen till att kommissionen fortsätter sitt dubbla angreppssätt mot radikalisering på nätet, där föreslagna regler om att avlägsna terrorisminnehåll på nätet ska förstärka det frivilliga partnerskapet med onlineplattformar.

En viktig faktor i detta sammanhang är **lagstiftningsförslaget för att förhindra spridning av terrorisminnehåll på nätet**, som innehåller tydliga bestämmelser och skyddsåtgärder som skulle göra det obligatoriskt för internetplattformar att ta bort terrorisminnehåll senast en timme efter att de mottagit en motiverad begäran från behöriga myndigheter och att vidta förebyggande åtgärder som står i proportion till graden av utsatthet för terrorisminnehåll[4].

[4] COM(2018) 640 final (12.9.2018).

Interinstitutionella förhandlingar pågår mellan Europaparlamentet och rådet, och ett första trepartsmöte hölls den 17 oktober 2019. Med tanke på hotet från terrorisminnehåll på nätet uppmanar kommissionen medlagstiftarna att nå en överenskommelse om den föreslagna lagstiftningen senast vid slutet av 2019.

Den föreslagna lagstiftningen kompletterar det frivilliga partnerskapet med internetbranschen och andra berörda parter inom ramen för **EU:s internetforum**. Sedan forumet skapades 2015 har det varit pådrivande för internetföretagens förebyggande arbete med att hitta och avlägsna terrorisminnehåll på nätet och banat vägen för branschinitiativet om en ”gemensam databas över hasher”[5] och inrättandet av det globala internetforumet för terrorismbekämpning. EU-enheten för anmälan av innehåll på internet, som ingår i EU:s brottsbekämpningsmyndighet Europol, har varit central för att stärka samarbetet med internetföretagen och har bidragit till att uppnå de övergripande målen för EU:s internetforum. Vid det senaste ministermötet inom EU:s internetforum den 7 oktober 2019 utfäste sig EU:s medlemsstater och högt uppsatta företrädare för internetföretagen att samarbeta inom ramen för det så kallade **EU-krisprotokollet**. EU-krisprotokollet fastställer tröskelvärden för ökat samarbete och nya metoder för förbättrad krishantering. Detta utgör en del av det internationella arbetet för att genomföra Christchurch-uppmaningen[6] och försöka säkerställa samordnade och snabba insatser för att begränsa spridningen av viralt terrorisminnehåll eller våldsbejakande extremistiskt innehåll på nätet.

Utöver dessa åtgärder mot radikalisering på nätet fortsätter kommissionen att stödja nationella och lokala insatser för att **förebygga och motverka radikalisering i praktiken**. Baserat på en mängd erfarenheter och sakkunskap som samlats in genom nätverket för kunskapsspridning om radikalisering erbjuder EU riktat stöd till lokala aktörer, däribland städer[7], och möjlighet till utbyten mellan yrkesverksamma, forskare och beslutsfattare. Nätverket har till exempel tagit fram särskild vägledning och arrangerat workshoppar för att stödja behöriga myndigheter i behandlingen av barn från konfliktområden[8]. För att säkerställa kontinuiteten i den verksamhet som nätverket för kunskapsspridning om radikalisering bedriver har kommissionen inlett förfarandet för ett nytt ramavtal till ett uppskattat värde av 61 miljoner euro under en period på fyra år, med början 2020[9].

För att motverka hotet från terrorisminnehåll på nätet uppmanar kommissionen Europaparlamentet och rådet att

---

5 Ett verktyg som tagits fram av ett företagskonsortium för att underlätta samarbete i syfte att förhindra spridning av terrorisminnehåll mellan plattformar.

6 Som ett svar på attackerna i Christchurch på Nya Zeeland den 15 mars 2019 bjöd Frankrikes president Emmanuel Macron och Nya Zeelands premiärminister Jacinda Ardern in stats- och regeringschefer och onlineplattformar till Paris den 15 maj 2019 för att lansera initiativet Christchurch-uppmaningen. Ordförande Jean-Claude Juncker ställde sig bakom uppmaningen och tillkännagav utarbetandet av ett krisprotokoll för EU.

7 Se även avsnitt V.2 om beredskap och skydd för mer information om samarbete med städer i säkerhetsfrågor, i synnerhet informationen om skydd av offentliga platser.

8 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/ran-papers/docs/issue_paper_child_returnees_from_conflict_zones_112016_en.pdf

9 Ramavtalet är uppdelat i två delkontrakt: 29 000 000 euro för stöd till verksamheten inom nätverket för kunskapsspridning om radikalisering under de kommande fyra åren och 32 000 000 euro för att stärka medlemsstaters, nationella, regionala och lokala myndigheters och prioriterade tredjeländers kapacitet att effektivt bekämpa radikalisering, i synnerhet genom att erbjuda nätverksmöjligheter, riktade och behovsstyrda tjänster samt forskning och analys.

- slutföra förhandlingarna om lagstiftningsförslaget för att förebygga spridning av **terrorisminnehåll på nätet** före årets slut.

2. Starkare och smartare informationssystem för säkerhet, gränsförvaltning och migrationshantering

EU har intensifierat informationsutbytet och gjort det lättare att bekämpa identitetsbedrägeri[10], förstärkt gränskontrollerna[11], moderniserat gemensamma europeiska databaser för brottsbekämpning[12], täppt till informationsluckor[13] och förstärkt EU:s brottsbekämpningsmyndighet Europol[14]. **Interoperabilitet mellan EU:s informationssystem**[15] är en central faktor för att åstadkomma detta och innebär att befintlig information utnyttjas på bästa sätt och att döda vinklar täpps till. Interoperabiliteten möter behoven hos de som arbetar i frontlinjen och leder till snabbare och mer systematisk tillgång till information för tjänstemän inom brottsbekämpningen, gränskontrolltjänstemän och migrationstjänstemän, och bidrar därmed till att förbättra den interna säkerheten och gränsförvaltningen.

Interoperabiliteten och all innovation som den för med sig kommer dock bara att spela någon roll för säkerhet, gränsförvaltning och migrationshantering om medlemsstaterna genomför den berörda lagstiftningen fullt ut. **Genomförandet** av interoperabiliteten har därför högsta prioritet inom säkerhetsunionen, både på politisk och teknisk nivå. Kommissionen och Europeiska unionens byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (eu-LISA) stöder medlemsstaterna med sakkunskap och utbyte av bästa praxis genom ett nätverk med nationella samordnare och genom att utveckla en resultattavla för effektiva övervaknings- och samarbetsarrangemang. Nära samarbete mellan EU:s byråer och alla medlemsstater och Schengenassocierade länder kommer att vara av

---

10 Förordning (EU) 2019/1157 av den 20 juni 2019 om säkrare identitetskort för unionsmedborgare och uppehållshandlingar som utfärdas till unionsmedborgare och deras familjemedlemmar när de utövar rätten till fri rörlighet.

11 Införande av systematiska kontroller av alla medborgare vid de yttre gränserna med hjälp av Schengens informationssystem. Alla Schengenstater, samt Rumänien, Bulgarien, Kroatien och Cypern, tillämpar de regler som infördes i april 2017 om systematiska kontroller i relevanta databaser vid de yttre gränserna. Enligt dessa regler kan tillfälliga undantag göras vid land- eller sjögränser men endast i fråga om EU-medborgare, med hänsyn till oproportionell påverkan på trafikflödena. Hittills har sex medlemsstater/Schengenassocierade länder anmält sådana undantag (Finland, Kroatien, Lettland, Norge, Slovenien och Ungern). För luftgränser löpte möjligheten till undantag från bestämmelserna om systematiska kontroller ut i april 2019.

12 Förstärkningen av Schengens informationssystem (förordning (EU) 2018/1860 (28.11.2018), förordning (EU) 2018/1861 (28.11.2018), förordning (EU) 2018/1862 (28.11.2018)) och utökningen av det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister till att omfatta tredjelandsmedborgare (förordning (EU) 2019/816 (17.4.2019)). Förstärkningen av Schengens informationssystem innefattar en allmän skyldighet att lägga in terrorismrelaterade registreringar i systemet.

13 EU:s in- och utresesystem (förordning (EU) 2017/2226 (30.11.2017)) och EU-systemet för reseuppgifter och resetillstånd (förordning (EU) 2018/1240 (12.9.2018) och förordning (EU) 2018/1241 (12.9.2018)).

14 Under de senaste åren har Europol getts en betydligt mer omfattande och djupgående roll. Byrån har förstärkts genom antagandet av Europolförordningen 2016 (förordning (EU) 2016/794 (11.5.2016)). De uppgifter som medlemsstaterna delar med sig av till och via Europol har ökat betydligt. Inrättandet av Europols centrum mot terrorism har förstärkt Europols analyskapacitet i terrorismärenden. Europols budget har ökat kontinuerligt under de senaste åren, från 82 miljoner euro 2014 till 138 miljoner euro 2019. Förhandlingar om budgeten för 2020 pågår.

15 Förordning (EU) 2019/817 (20.5.2019) och förordning (EU) 2019/818 (20.5.2019).

största vikt för att uppnå det ambitiösa målet att uppnå full interoperabilitet mellan EU:s informationssystem för säkerhet, gränsförvaltning och migrationshantering senast 2020.

Samtidigt behöver Europaparlamentet och rådet fortfarande **slutföra det lagstiftningsarbete** som krävs för detta. Att snabbt nå en överenskommelse om alla ännu inte antagna lagstiftningsförslag är avgörande för att interoperabiliteten ska kunna genomföras fullt ut utan dröjsmål. För det första krävs, som ett led i den tekniska implementeringen av **EU-systemet för reseuppgifter och resetillstånd**, tekniska ändringar av de relaterade förordningarna[16] för att systemet ska kunna inrättas fullt ut. Kommissionen uppmanar Europaparlamentet att påskynda sitt arbete med dessa tekniska ändringar för att kunna påbörja interinstitutionella förhandlingar så snart som möjligt. För det andra pågår fortfarande interinstitutionella förhandlingar om förslaget från maj 2018 om att förstärka och uppgradera det befintliga **informationssystemet för viseringar**[17]. Kommissionen uppmanar, på grundval av det trepartsmöte som ägde rum den 22 oktober 2019, båda medlagstiftarna att snabbt slutföra förhandlingarna. För det tredje har ännu ingen överenskommelse nåtts om kommissionens förslag från maj 2016 om att utöka tillämpningsområdet för **Eurodac**[18] genom att lagra inte bara fingeravtryck och berörda uppgifter om asylsökande och personer som grips i samband med att de olagligen passerar den yttre gränsen, utan även om tredjelandsmedborgare som vistas olagligt i unionen. De föreslagna ändringarna skulle även förlänga lagringsperioden för fingeravtryck och berörda uppgifter för de som olagligt reser in i EU. Kommissionen uppmanar medlagstiftarna att gå vidare med antagandet av förslaget.

För att stärka EU-informationssystemen för säkerhet, gränsförvaltning och migrationshantering uppmanar kommissionen Europaparlamentet och rådet att

- arbeta vidare för att nå en snabb överenskommelse om de föreslagna tekniska ändringar som krävs för att inrätta **EU-systemet för reseuppgifter och resetillstånd**,
- snabbt genomföra och slutföra förhandlingarna om förslaget att stärka det befintliga **informationssystemet för viseringar**,
- anta lagstiftningsförslaget om **Eurodac** (*prioritering från den gemensamma förklaringen*).

3. Minimerat handlingsutrymme för terrorister

EU har vidtagit kraftfulla åtgärder för att strypa terroristernas handlingsutrymme med hjälp av nya regler som gör det svårare för terrorister och andra brottslingar att få tillgång till sprängämnen[19], skjutvapen och finansiering[20], och genom att begränsa deras möjlighet att röra sig[21].

För att stärka de rättsliga åtgärderna mot terrorism inrättade Europeiska unionens byrå för straffrättsligt samarbete (Eurojust) den 1 september 2019 ett **europeiskt rättsligt**

16 Förordning (EU) 2018/1240 (12.9.2018) och förordning (EU) 2018/1241 (12.9.2018).
17 COM(2018) 302 final (16.5.2018).
18 COM(2016) 272 final (4.5.2016).
19 Förordning (EU) 2019/1148 av den 20 juni 2019 om saluföring och användning av sprängämnesprekursorer. Förordningen trädde i kraft den 31 juli 2019 och ska börja tillämpas 18 månader efter ikraftträdandet.
20 Direktiv (EU) 2019/1153 av den 11 juli 2019 om fastställande av bestämmelser för att underlätta användning av finansiell information och andra uppgifter för att förebygga, upptäcka, utreda eller lagföra vissa brott.
21 Införande av systematiska kontroller av alla medborgare vid de yttre gränserna med hjälp av Schengens informationssystem.

terrorismbekämpningsregister. Registret kommer att samla in rättslig information för att identifiera kopplingar i pågående förfaranden mot personer misstänkta för terroristbrott, vilket kommer att förstärka samordningen mellan åklagare i utredningar av misstänkt terrorism som kan ha gränsöverskridande konsekvenser.

Ytterligare insatser krävs emellertid för att stödja och underlätta utredningar i gränsöverskridande ärenden, framför allt när det gäller **tillgång till elektroniska bevis** för brottsbekämpande organ. När det gäller lagstiftningsförslaget från april 2018 om att förbättra den gränsöverskridande tillgången till elektroniska bevis i straffrättsliga förfaranden[22] måste Europaparlamentet anta sin förhandlingsposition innan medlagstiftarna kan påbörja förhandlingarna. Kommissionen uppmanar Europaparlamentet att gå vidare med detta lagstiftningsförslag så att medlagstiftarna kan arbeta vidare mot ett snabbt antagande. Med utgångspunkt i förslaget om EU-interna bestämmelser för kommissionen även **internationella förhandlingar** för att förbättra den gränsöverskridande tillgången till elektroniska bevis. Den 25 september 2019 höll kommissionen och myndigheter i Förenta staterna sin första förhandlingsrunda om ett **avtal mellan EU och Förenta staterna om gränsöverskridande tillgång till elektroniska bevis**. En ytterligare förhandlingsrunda är planerad till den 6 november 2019. I samband med de pågående förhandlingarna om ett **andra tilläggsprotokoll till Europarådets Budapestkonvention om it-brottslighet** deltog kommissionen på unionens vägnar i de tre förhandlingsmötena i juli, september och oktober 2019. Även om stora framsteg har gjorts i förhandlingarna återstår fortfarande flera viktiga frågor för unionen som behöver lösas, såsom dataskyddsgarantier. Förhandlingarna om ett andra tilläggsprotokoll kommer att fortsätta i november 2019 och under hela 2020. Det är viktigt att snabbt gå vidare med förhandlingarna för att främja det internationella samarbetet kring utbyte av elektroniska bevis, i överensstämmelse med EU:s lagstiftning och medlemsstaternas skyldigheter enligt denna samt med hänsyn tagen till den framtida utvecklingen av EU-lagstiftningen.

Mot bakgrund av den kvarvarande oron över penningtvätt antog Europaparlamentet den 19 september 2019 en **resolution om läget i genomförandet av EU:s lagstiftning mot penningtvätt**[23] som ett svar på det paket med fyra rapporter om bekämpning av penningtvätt som kommissionen antog den 24 juli 2019[24]. Europaparlamentet uppmanade medlemsstaterna att snabbt och på ett korrekt sätt genomföra direktiven om bekämpning av penningtvätt. Europaparlamentet uppmanade också kommissionen att utvärdera om en förordning om bekämpning av penningtvätt vore en lämpligare rättsakt än ett direktiv och att utvärdera behovet av en samordnings- och stödmekanism för finansunderrättelseenheter.

---

22 COM(2018) 225 final (17.4.2018) och COM(2018) 226 final (17.4.2018).

23 http://www.europarl.europa.eu/doceo/document/TA-9-2019-0022_SV.html

24 Rapport om bedömningen av risker för penningtvätt och finansiering av terrorism som påverkar den inre marknaden och berör gränsöverskridande verksamhet (COM(2019) 370 final (24.7.2019)), rapport om sammankoppling av medlemsstaternas nationella centraliserade automatiserade mekanismer (centrala register eller centrala elektroniska datasöksystem) med uppgifter om bankkonton (COM(2019) 372 final (24.7.2019)), rapport om bedömningen av nyligen uppdagade fall av misstänkt penningtvätt i kreditinstitut i EU (COM(2019) 373 final (24.7.2019)), rapport om bedömning av ramen för samarbete mellan finansunderrättelseenheter (COM(2019) 371 final).

För att förbättra brottsbekämpande myndigheters tillgång till elektroniska bevis uppmanar kommissionen Europaparlamentet att

- snabbt anta lagstiftningsförslaget om **elektroniska bevis** (*prioritering från den gemensamma förklaringen*).

4. Ökad cybersäkerhet

Ökad cybersäkerhet är en viktig aspekt i arbetet för en effektiv och verklig säkerhetsunion. Genom genomförandet av EU:s strategi för cybersäkerhet från 2017[25] har EU stärkt sin motståndskraft genom försvårande av attacker och snabbare återhämtning. Strategin har även stärkt den avskräckande förmågan genom förbättrade möjligheter att få tag på och straffa angripare, bland annat genom en ram för ett gemensamt diplomatiskt svar från EU på skadlig it-verksamhet. Unionen stöder även medlemsstaternas it-försvar genom genomförandet av ramen för EU:s politik för it-försvar[26].

Genom ikraftträdandet av cybersäkerhetsakten[27] i juni 2019 är **EU:s ramverk för cybersäkerhetscertifiering** på väg att realiseras. Certifiering är viktig för att öka förtroendet och säkerheten när det gäller produkter och tjänster som behövs för den digitala inre marknaden. Certifieringsramverket kommer att tillhandahålla EU-övergripande ordningar för cybersäkerhetscertifiering i form av en vittomfattande uppsättning regler, tekniska krav, standarder och förfaranden. Det inbegriper två expertgrupper, närmare bestämt den europeiska gruppen för cybersäkerhetscertifiering, som företräder medlemsstaternas myndigheter, och intressentgruppen för cybersäkerhetscertifiering, som företräder branschen. Den senare sammanför både efterfrågesidan och utbudssidan när det gäller IKT-produkter och IKT-tjänster, och innefattar små och medelstora företag, leverantörer av digitala tjänster, europeiska och internationella standardiseringsorgan, nationella ackrediteringsorgan, tillsynsmyndigheter med ansvar för dataskydd och organ för bedömning av överensstämmelse.

Samtidigt behöver Europaparlamentet och rådet fortfarande nå en överenskommelse om lagstiftningsinitiativet[28] om ett **europeiskt kompetenscentrum för cybersäkerhet inom näringsliv, teknik och forskning och ett nätverk av nationella samordningscentrum**. Syftet med förslaget är att stärka unionens kapacitet på cybersäkerhetsområdet genom att stimulera det europeiska ekosystemet för cybersäkerhet inom näringsliv och teknik samt samordna och slå samman relevanta resurser. Kommissionen uppmanar båda medlagstiftarna att återuppta och snabbt slutföra de interinstitutionella förhandlingarna om detta prioriterade initiativ för att förbättra cybersäkerheten.

Arbetet med att stärka cybersäkerheten innefattar stöd till både de nationella och regionala nivåerna[29].

Utöver cyberhot mot system och data fortsätter EU också att ta itu med de komplexa och

[25] JOIN(2017) 450 final (13.9.2017).

[26] Ram för EU:s politik för it-försvar (uppdaterad 2018) som antogs av rådet den 19 november 2018 (14413/18).

[27] Förordning (EU) 2019/881 (17.4.2019).

[28] COM(2018) 630 final (12.9.2018).

[29] Kommissionen stöder t.ex. ett interregionalt innovationspartnerskap om cybersäkerhet mellan Bretagne, Castilla y León, Nordrhein-Westfalen, Mellersta Finland och Estland som ska utveckla en värdekedja för cybersäkerhet med inriktning på kommersialisering och uppskalning.

mångfasetterade utmaningar som **hybridhot** utgör. Inom rådet har en övergripande arbetsgrupp för att bekämpa hybridhot inrättats för att stärka EU:s och medlemsstaternas motståndskraft mot hybridhot och stödja insatser för att stärka samhällenas motståndskraft mot kriser. Kommissionen och Europeiska utrikestjänsten stöder dessa insatser i enlighet med 2016 års gemensamma ram för att motverka hybridhot[30] och 2018 års gemensamma meddelande[31] om att öka motståndskraften och stärka kapaciteten att hantera hybridhot. Dessutom arbetar det gemensamma forskningscentrumet med att ta fram ett ramverk för en ”konceptuell modell” för att beskriva hybridhot med målet att hjälpa medlemsstaterna och deras behöriga myndigheter att identifiera den typ av hybridattacker de kan komma att utsättas för. Modellen undersöker hur en statlig eller icke-statlig aktör använder en rad verktyg (från desinformation till spionage eller fysiska operationer) inom olika områden (ekonomiska, militära, sociala, politiska) för att påverka ett mål i syfte att uppnå olika målsättningar.

För att förbättra cybersäkerheten uppmanar kommissionen Europaparlamentet och rådet att

- nå en snabb överenskommelse om lagstiftningsförslaget om ett **europeiskt kompetenscentrum för cybersäkerhet inom näringsliv, teknik och forskning och ett nätverk av nationella samordningscentrum**.

III. ÖKAD SÄKERHET I DEN DIGITALA INFRASTRUKTUREN

5G-nät kommer att utgöra den framtida ryggraden i våra alltmer digitaliserade ekonomier och samhällen. Miljardtals uppkopplade föremål och system berörs, t.ex. i kritiska sektorer som energi, transport, bankverksamhet och hälso- och sjukvård. Det gäller även industrins styrsystem som innehåller känslig information, samt stödjande säkerhetssystem. Att trygga cybersäkerheten och motståndskraften hos 5G-näten är därför centralt.

Som ett led i en samordnad strategi offentliggjorde medlemsstaterna den 9 oktober 2019 en rapport om **EU:s samordnade riskbedömning av cybersäkerheten i 5G-nät** med stöd av kommissionen och Europeiska unionens cybersäkerhetsbyrå[32]. Detta är ett viktigt led i genomförandet av kommissionens rekommendation från mars 2019 för att säkerställa en hög cybersäkerhet i 5G-näten i hela EU[33]. Rapporten bygger på resultaten av alla medlemsstaternas nationella riskbedömningar av cybersäkerheten. Den anger de största hoten, de huvudsakliga fientliga aktörerna, de känsligaste tillgångarna, de främsta sårbarheterna (både tekniska och andra typer av sårbarheter) och ett antal strategiska risker. Bedömningen ger ett underlag för att identifiera vilka riskreducerande åtgärder som kan vidtas på nationell och europeisk nivå.

I rapporten identifieras ett antal viktiga **cybersäkerhetsutmaningar** som sannolikt kommer att uppstå eller bli mer framträdande i 5G-nät. Säkerhetsutmaningarna är i huvudsak kopplade till *innovationer* som är centrala i 5G-tekniken, i synnerhet programvarans betydelse och de

[30] JOIN(2016) 18 final (6.4.2016).
[31] JOIN(2018) 16 final (13.6.2018).
[32] EU:s samordnade riskbedömning av cybersäkerheten i 5G-nät genomfördes av samarbetsgruppen med behöriga myndigheter som inrättats genom direktivet om säkerhet i nätverks- och informationssystem (direktiv (EU) 2016/1148 (6.7.2016)) med stöd av kommissionen och Europeiska unionens cybersäkerhetsbyrå: https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.
[33] C(2019) 2355 final (26.3.2019).

många olika tjänster och tillämpningsområden som 5G-tekniken möjliggör, samt till *leverantörernas* roll för att bygga och driva 5G-näten och beroendet av enskilda leverantörer. Det innebär att leverantörernas produkter, tjänster och verksamhet i allt högre grad blir en del av 5G-nätens ”angreppsyta”. Riskprofilen för enskilda leverantörer kommer att vara av särskild betydelse, bland annat sannolikheten för att leverantören utsätts för inblandning från länder utanför EU.

I enlighet med det förfarande som fastställs i kommissionens rekommendation från mars 2019 ska medlemsstaterna senast den 31 december 2019 enas om en **verktygslåda med motåtgärder** för att hantera de identifierade cybersäkerhetsriskerna på nationell nivå och unionsnivå. Kommissionen och Europeiska utrikestjänsten kommer även att fortsätta sitt utbyte med likasinnade partner om 5G-nätens cybersäkerhet och motståndskraft. På detta område håller kommissionen kontakt med Nato om EU:s samordnade riskbedömning av 5G-nätens cybersäkerhet.

IV. MOTVERKA DESINFORMATION OCH SKYDDA VAL MOT ANDRA CYBERBASERADE HOT

EU har inrättat en **ram för samordnade insatser mot desinformation**, med full respekt för europeiska värden och grundläggande rättigheter[34]. Insatserna för att minimera handlingsutrymmet för desinformation fortsätter inom ramen för åtgärdsplanen mot desinformation[35], bland annat i syfte att skydda valsystemens integritet.

Av central betydelse i detta sammanhang är det arbete som bedrivs tillsammans med branschen genom den självreglering i form av **uppförandekoden om desinformation** för onlineplattformar och reklambranschen som började gälla i oktober 2018[36]. Kommissionen har utvärderat effekten av uppförandekoden efter det första år den varit i kraft, baserat på årliga självutvärderingsrapporter som onlineplattformarna och andra som undertecknat uppförandekoden lämnat och som offentliggjordes den 29 oktober 2019 tillsammans med kommissionens uttalande.[37] Generellt sett visar rapporterna att undertecknarna gjort stora ansträngningar för att genomföra sina åtaganden.

Hur snabba och omfattande de åtgärder är som de undertecknande plattformarna vidtar varierar mellan uppförandekodens fem olika åtgärdspelare. Generellt sett har större framsteg gjorts när det gäller åtaganden som rör 2019 års val till Europarlamentet, närmare bestämt att störa reklamincitament och ekonomiska incitament för att sprida desinformation (första pelaren), att säkerställa insyn i politisk och sakfrågebaserad reklam (andra pelaren) och att säkerställa tjänsters integritet mot icke-autentiska konton och beteenden (tredje pelaren). Mindre framsteg, eller inga alls, har däremot gjorts när det gäller åtaganden om att stärka konsumenternas inflytande (fjärde pelaren) och åtaganden för att stärka forskarsamhällets inflytande, bland annat genom att plattformar ger tillgång till relevanta data för forskningsändamål i enlighet med reglerna om skydd av personuppgifter (femte pelaren). Omfattningen av de åtgärder som varje plattform vidtar för att genomföra sina åtaganden varierar också, och det finns skillnader mellan medlemsstaterna i genomförandet av de enskilda strategierna. Kommissionen fortsätter att arbeta tillsammans med undertecknarna av uppförandekoden för att intensifiera åtgärderna mot desinformation.

I enlighet med åtgärdsplanen mot desinformation har kommissionen och EU:s utrikesrepresentant, i samarbete med medlemsstaterna, inrättat ett **system för tidig varning** för att bemöta desinformationskampanjer. Genom systemet för tidig varning kunde EU:s institutioner och medlemsstater utbyta information och analyser inför Europaparlamentsvalet 2019 och samordna sin respons. Efter valet har arbetet intensifierats ytterligare genom dagliga

---

34 Se åtgärdsplanen mot desinformation (JOIN(2018) 36 final (5.12.2018)).

35 JOIN(2019) 12 final (14.6.2019).

36 Enligt uppförandekoden har onlineplattformarna Google, Facebook, Twitter och Microsoft åtagit sig att förhindra att illasinnade aktörer använder deras tjänster på ett otillbörligt sätt, att skapa insyn i och offentliggöra information om politisk reklam samt att vidta andra åtgärder för att stärka insynen, ansvarsskyldigheten och tillförlitligheten i ekosystemen på nätet. Branschorganisationer från reklambranschen har också åtagit sig att samarbeta med plattformarna för att förbättra granskningen av annonsplaceringar och utveckla säkerhetsverktyg för att begränsa placeringen av reklam på webbplatser som sprider desinformation.

37 https://ec.europa.eu/commission/presscorner/detail/sv/statement_19_6166. Utöver Google, Facebook, Twitter och Microsoft har uppförandekoden även undertecknats av Mozilla, sju organisationer på europeisk eller nationell nivå som företräder reklambranschen och av EDiMA, en europeisk organisation som företräder plattformar och andra teknikföretag verksamma i onlinesektorn.

utbyten i det fortlöpande arbetet och tre möten mellan kontaktpunkterna i systemet för tidig varning som arrangerats av olika medlemsstater.

En annan praktisk åtgärd för att identifiera desinformation är det arbete som bedrivs av **gruppen för strategisk kommunikation**, framför allt arbetsgruppen East Stratcom, som har drivit projektet ”EUvsDisinfo” för att övervaka, analysera och motverka Kremlvänlig desinformation[38]. Sedan början av 2019 har den första särskilda budgeten på 3 miljoner euro gjort det möjligt att intensifiera och utöka arbetet till att omfatta övervakning och analys av Kremlvänlig desinformation på webben, i etermedier och i sociala medier till 19 språk, från engelska till serbiska och arabiska. Tack vare förbättrad övervakningskapacitet har mängden desinformationsaktiviteter som avslöjats mer än fördubblats, till omkring 2 000 fall av desinformation hittills under 2019 jämfört med 765 fall under samma period 2018. Arbetsgruppen East Stratcom har spelat en avgörande roll i övervakningen och avslöjandet av Kremlvänlig desinformation riktad mot Europaparlamentsvalet 2019. Parallellt med forskningen genomfördes en kampanj för att öka medvetenheten om försök till valmanipulation runt om i världen. Kampanjen, som genomfördes i nära samarbete med Europaparlamentet och kommissionen, resulterade i mer än 20 intervjuer i medier och involverade mer än 300 journalister.

Kommissionen har även vidtagit åtgärder för att **minska spridningen av desinformation och rykten om EU:s institutioner och politik**. Kommissionen har inrättat ett nätverk av kommunikationsexperter med en onlineportal som innehåller interaktivt informationsmaterial om EU:s politik och utmaningen med desinformation och dess effekt på samhället. Kommissionen har också, i nära samarbete med Europaparlamentet och Europeiska utrikestjänsten, lanserat en rad mediekampanjer inriktade på att bekämpa desinformation[39].

V. GENOMFÖRANDE AV ANDRA PRIORITERADE SÄKERHETSÄRENDEN

1. Genomförande av lagstiftningsåtgärder inom säkerhetsunionen

Förutsättningen för att dra full nytta av de åtgärder som man kommit överens om inom säkerhetsunionen är att alla medlemsstater genomför dem snabbt och fullständigt. Kommissionen stöder därför aktivt medlemsstaterna i deras genomförande av EU:s lagstiftning, bland annat genom finansiering och genom att underlätta utbyte av bästa praxis. Kommissionen utnyttjar sina befogenheter enligt fördragen fullt ut för att verkställa EU:s lagstiftning, även genom överträdelseförfaranden när så är lämpligt.

Tidsfristen för införlivandet av **EU-direktivet om passageraruppgifter**[40] löpte ut den 25 maj 2018. Hittills har 25 medlemsstater anmält fullständigt införlivande[41], vilket är ett betydande framsteg sedan juli 2018, då kommissionen inledde överträdelseförfaranden mot 14 medlemsstater[42]. Två medlemsstater har ännu inte anmält fullständigt införlivande trots

38 www.euvsdisinfo.eu

39 https://europa.eu/euprotects/content/homepage_sv

40 Direktiv (EU) 2016/681 (27.4.2016). Danmark deltar inte i antagandet av detta direktiv, som inte är bindande för eller tillämpligt på Danmark.

41 Hänvisningarna till fullständigt införlivande avser medlemsstaternas anmälningar och påverkar inte kommissionens kontroll av införlivandet (läget den 17 oktober 2019).

42 Se den sextonde rapporten om framsteg i riktning mot en effektiv och verklig säkerhetsunion (COM(2018) 690 final (10.10.2018)).

pågående överträdelseförfaranden som inleddes den 19 juli 2018[43]. Parallellt med detta fortsätter kommissionen att stödja samtliga medlemsstater i deras arbete med att slutföra utvecklingen av sina system för passageraruppgifter, bland annat genom att underlätta utbytet av information och bästa praxis.

Tidsfristen för införlivandet av **direktivet om bekämpande av terrorism**[44] löpte ut den 8 september 2018. Hittills har 22 medlemsstater anmält fullständigt införlivande, vilket är ett betydande framsteg sedan november 2018, då kommissionen inledde överträdelseförfaranden mot 16 medlemsstater[45]. Tre medlemsstater har ännu inte anmält fullständigt införlivande trots de pågående överträdelseförfarandena[46]. Den 25 juli 2019 skickade kommissionen motiverade yttranden till två medlemsstater som inte har anmält fullständigt införlivande av direktivet[47]. Som svar tillkännagav båda medlemsstaterna att lagstiftningsarbetet kommer att slutföras före utgången av innevarande år.

Tidsfristen för införlivandet av **direktivet om kontroll av förvärv och innehav av vapen**[48] löpte ut den 14 september 2018. Hittills har 13 medlemsstater anmält ett fullständigt införlivande. 15 medlemsstater har ännu inte anmält fullständigt införlivande trots pågående överträdelseförfaranden som inleddes den 22 november 2018[49]. Den 25 juli 2019 skickade kommissionen motiverade yttranden till 20 medlemsstater som inte har anmält fullständigt införlivande av direktivet. Som svar anmälde fem medlemsstater fullständigt införlivande av direktivet[50].

Tidsfristen för införlivandet av **dataskyddsdirektivet för brottsbekämpning**[51] löpte ut den 6 maj 2018. Hittills har 25 medlemsstater anmält fullständigt införlivande, vilket är ett betydande framsteg sedan juli 2018, då kommissionen inledde överträdelseförfaranden mot 19 medlemsstater[52]. Tre medlemsstater har ännu inte anmält fullständigt införlivande trots de pågående överträdelseförfarandena[53]. Den 25 juli 2019 beslutade kommissionen att väcka talan vid domstolen mot två medlemsstater[54] för underlåtenhet att införliva direktivet och skickade en formell underrättelse till en medlemsstat[55] för att denna inte fullständigt införlivat

---

43 Slovenien har anmält delvis införlivande. Spanien har inte anmält införlivande (läget den 17 oktober 2019).

44 Direktiv (EU) 2017/541 (15.3.2017). Direktivet är inte tillämpligt i Förenade kungariket, Irland och Danmark.

45 Se den sjuttonde rapporten om framsteg i riktning mot en effektiv och verklig säkerhetsunion (COM(2018) 845 final (11.12.2018)).

46 Grekland och Luxemburg har inte anmält nationella åtgärder för införlivande. Polen har anmält nationella åtgärder som motsvarar delvis införlivande (läget den 17 oktober 2019).

47 Grekland och Luxemburg.

48 Direktiv (EU) 2017/853 (17.10.2019).

49 Belgien, Estland, Förenade kungariket, Polen, Slovakien, Sverige och Tjeckien har anmält införlivandeåtgärder för delar av de nya bestämmelserna. Cypern, Grekland, Luxemburg, Rumänien, Slovenien, Spanien, Tyskland och Ungern har inte anmält några införlivandeåtgärder (läget den 17 oktober 2019).

50 Finland, Irland, Litauen, Nederländerna och Portugal (läget den 17 oktober 2019).

51 Direktiv (EU) 2016/680 (27.4.2016).

52 Se den sextonde rapporten om framsteg i riktning mot en effektiv och verklig säkerhetsunion (COM(2018) 690 final (10.10.2018)).

53 Slovenien har anmält delvis införlivande. Spanien har inte anmält införlivande. Även om Tyskland har anmält fullständigt införlivande anser kommissionen att detta införlivande inte är fullständigt (läget den 17 oktober 2019).

54 Grekland och Spanien.

55 Tyskland.

direktivet[56].

Kommissionen bedömer införlivandet av det **fjärde penningtvättsdirektivet**[57] samtidigt som den också kontrollerar att medlemsstaterna genomför reglerna. Medlemsländerna skulle ha införlivat direktivet i nationell rätt senast den 26 juni 2018. Kommissionen driver överträdelseförfaranden mot 21 medlemsstater eftersom den har bedömt att de meddelanden som mottagits från medlemsstaterna inte motsvarar ett fullständigt införlivande av direktivet[58].

Kommissionen har bedömt överensstämmelsen hos införlivandet av **direktiven om it-brottslighet**. Kommissionen inledde i juli och oktober 2019 överträdelseförfaranden mot 23 medlemsstater[59] eftersom den bedömde att den nationella genomförandelagstiftning som dessa medlemsstater anmält inte utgjorde ett korrekt införlivande av **direktivet om bekämpande av sexuellt utnyttjande av barn**[60]. Kommissionen inledde i juli och oktober 2019 även överträdelseförfaranden mot fyra medlemsstater[61] eftersom den bedömde att den nationella genomförandelagstiftning som dessa medlemsstater anmält inte utgjorde ett korrekt införlivande av **direktivet om angrepp mot informationssystem**[62].

Kommissionen uppmanar medlemsstaterna att snarast möjligt vidta de åtgärder som krävs för att fullt ut införliva följande direktiv i den nationella lagstiftningen och anmäla dem till kommissionen:

- **EU-direktivet om passageraruppgifter** – en medlemsstat måste ännu anmäla införlivande i den nationella lagstiftningen och en medlemsstat måste ännu komplettera anmälan av införlivande[63].
- **Direktivet om bekämpande av terrorism** – två medlemsstater måste ännu anmäla införlivande i den nationella lagstiftningen och en medlemsstat måste ännu komplettera anmälan av införlivande[64].
- **Direktivet om kontroll av förvärv och innehav av vapen** – åtta medlemsstater måste ännu anmäla införlivande i den nationella lagstiftningen och sju medlemsstater måste ännu komplettera anmälan av införlivande[65].
- **Dataskyddsdirektivet för brottsbekämpning** – en medlemsstat måste ännu anmäla införlivande i den nationella lagstiftningen och två medlemsstater måste ännu komplettera

56 Grekland har anmält fullständigt införlivande, vilket kommissionen håller på att bedöma.
57 Direktiv (EU) 2015/849 (20.5.2015).
58 Belgien, Bulgarien, Tjeckien, Danmark, Tyskland, Estland, Irland, Frankrike, Italien, Cypern, Lettland, Litauen, Ungern, Nederländerna, Österrike, Polen, Rumänien, Slovakien, Finland, Sverige och Förenade kungariket (läget den 17 oktober 2019). Sju överträdelseförfaranden rörande direktivet har tidigare avslutats.
59 Belgien, Bulgarien, Tjeckien, Tyskland Estland, Grekland, Spanien, Frankrike, Kroatien, Italien, Lettland, Litauen, Luxemburg, Ungern, Malta, Österrike, Polen, Portugal, Rumänien, Slovenien, Slovakien, Finland och Sverige.
60 Direktiv 2011/93/EU (13.12.2011).
61 Bulgarien, Italien, Portugal och Slovenien.
62 Direktiv 2013/40/EU (12.8.2013).
63 Slovenien har anmält delvis införlivande. Spanien har inte anmält införlivande (läget den 17 oktober 2019).
64 Grekland och Luxemburg har inte anmält införlivande. Polen har anmält delvis införlivande (läget den 17 oktober 2019).
65 Belgien, Estland, Förenade kungariket, Polen, Slovakien, Sverige och Tjeckien har anmält införlivandeåtgärder för delar av de nya bestämmelserna. Cypern, Grekland, Luxemburg, Rumänien, Slovenien, Spanien, Tyskland och Ungern har inte anmält några införlivandeåtgärder (läget den 17 oktober 2019).

anmälan av införlivande[66].

- **Det fjärde penningtvättsdirektivet** – 21 medlemsstater måste ännu komplettera anmälan av införlivande[67].
- **Direktivet om bekämpande av sexuellt utnyttjande av barn** – överträdelseförfaranden om felaktigt införlivande har inletts mot 23 medlemsstater[68].
- **Direktivet om angrepp mot informationssystem** – överträdelseförfaranden om felaktigt införlivande har inletts mot fyra medlemsstater[69].

2. Beredskap och skydd

En viktig aspekt av arbetet för en effektiv och verklig säkerhetsunion är att bygga upp motståndskraften mot säkerhetshot. Kommissionen stöder medlemsstaterna och lokala myndigheter i att förbättra skyddet av offentliga platser genom att genomföra handlingsplanen från oktober 2017 och partnerskapet för säkerhet på offentliga platser från januari 2019 inom ramen för EU-agendan för städer. Detta arbete rör de städer som kontaktat kommissionen och bett om stöd för att hantera de utmaningar de ställts inför när det gäller skyddet av offentliga platser.

Utbyte av bästa praxis mellan lokala myndigheter och med privata aktörer är mycket viktigt för att stärka säkerheten på offentliga platser. Detta stod i centrum under den **europeiska säkerhetsveckan** i Nice i Frankrike, som ägde rum den 14–18 oktober 2019 och arrangerades av det EU-finansierade projektet för skyddet av städer i samverkan mot terrorism genom att trygga säkerheten på offentliga platser (*Protect Allied Cities against Terrorism in Securing Urban Areas*). Arrangemanget samlade 500 deltagare från städer i hela Europa, nationella myndigheter och forskningsinstitut och lyfte fram vikten av nära samarbete mellan alla berörda parter, offentliga som privata, och betydelsen av ny teknik för att förbättra skyddet av städer. Skyddet av offentliga platser togs också upp under den **europeiska veckan för regioner och städer** i Bryssel den 7–10 oktober 2019 genom en workshop för EU:s partnerskap för säkerhet på offentliga platser om EU-agendan för städer. Workshoppen fokuserade på lokala myndigheters roll på det säkerhetspolitiska området, EU:s lagstiftning och finansiering för att möta säkerhetsutmaningar på offentliga platser i städer och centrala teman som innovation genom smarta lösningar och smart teknik, bland annat begreppet inbyggd säkerhet, säkerhet genom förebyggande och säkerhet genom social inkludering. Kommissionen bidrar också till att främja städernas innovation på dessa områden genom sin senaste ansökningsomgång inom ramen för Innovativa åtgärder i städerna, vars resultat offentliggjordes i augusti 2019. Bland de projekt som valts ut finns tre städer (Pireus i

[66] Slovenien har anmält delvis införlivande. Spanien har inte anmält införlivande. Även om Tyskland har anmält ett fullständigt införlivande anser kommissionen att detta införlivande inte är fullständigt (läget den 17 oktober 2019).

[67] Belgien, Bulgarien, Tjeckien, Danmark, Tyskland, Estland, Irland, Frankrike, Italien, Cypern, Lettland, Litauen, Ungern, Nederländerna, Österrike, Polen, Rumänien, Slovakien, Finland, Sverige och Förenade kungariket (läget den 17 oktober 2019).

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

[69] Bulgarien, Italien, Portugal och Slovenien.

Grekland, Tammerfors i Finland och Turin i Italien) som kommer att testa nya lösningar på säkerhetsfrågor i städer[70].

För att förbättra **skyddet av gudstjänstlokaler** och undersöka behovet hos olika religiösa grupper arrangerade kommissionen den 7 oktober 2019 ett möte med företrädare för judiska, muslimska, kristna och buddistiska grupper. Mötet, som ingick i genomförandet av handlingsplanen från oktober 2017 till stöd för skyddet av offentliga platser, visade att medvetenheten och beredskapen varierar betydligt mellan olika religiösa grupper och betonade vikten av ett fortsatt utbyte av bästa praxis. Mötet visade också att det går att införa grundläggande säkerhetsåtgärder och öka säkerhetsmedvetenhet samtidigt som gudstjänstlokalernas öppenhet och tillgänglighet bibehålls. Kommissionen kommer att sammanställa information om bästa praxis och ökad medvetenhet på sin elektroniska expertplattform och informera medlemsstaternas säkerhetsmyndigheter i frågan via det offentlig-privata forumet om skydd av offentliga platser.

Ett område som måste uppmärksammas ytterligare är det ökande säkerhetshotet mot kritisk infrastruktur från **drönare**. För att komplettera den senaste EU-lagstiftningen[71] om säker drift av drönare i luftrum som används för bemannad luftfart utan att möjligheterna till ändamålsenlig användning av drönare undergrävs, hjälper kommissionen medlemsstaterna att följa utvecklingen av drönaranvändning för illvilliga syften genom att finansiera relevant forskning och underlätta tester av motåtgärder. Utbyte av erfarenheter och bästa praxis är avgörande, vilket framgick av den internationella högnivåkonferensen om bemötande av hoten från obemannade luftfartygssystem som hölls i Bryssel den 17 oktober 2019. Vid konferensen, som arrangerades av kommissionen, samlades 250 deltagare från medlemsstaterna, internationella organisationer, tredjelandspartner, industrin, den akademiska världen och det civila samhället för att diskutera de säkerhetsutmaningar som drönare medför och hur dessa kan bemötas. Mötet visade på behovet av regelbundna riskbedömningar i samband med drönare och av nära samarbete mellan luftfartsmyndigheter och brottsbekämpande myndigheter för att vidareutveckla den europeiska lagstiftningen om säker drift av drönare. Det behövs även en samordnad europeisk strategi för ytterligare tester av motåtgärder mot drönare. Deltagarna var också överens om att en nära samverkan mellan myndigheter och industrin är avgörande för en säker och tillförlitlig drift av drönare som försvårar användning för illvilliga syften.

3. Yttre dimension

Eftersom säkerhetshoten mot unionen inte är begränsade till EU:s territorium utan utgör globala hot är samarbetet med partnerländer, organisationer och berörda aktörer avgörande för att skapa en effektiv och verklig säkerhetsunion.

Informationsutbyte spelar en central roll i detta samarbete. Tillsammans med denna rapport har kommissionen antagit en rekommendation till rådet om bemyndigande att inleda förhandlingar om ett **avtal mellan EU och Nya Zeeland om utbyte av personuppgifter för att bekämpa grov brottslighet och terrorism** mellan Europol och behöriga myndigheter på

[70] Innovativa åtgärder i städerna är ett instrument som medfinansieras av Europeiska regionala utvecklingsfonden. För ytterligare information, se https://www.uia-initiative.eu/en/call-proposals/4th-call-proposals.

[71] Kommissionens genomförandeförordning (EU) 2019/947 av den 24 maj 2019 om regler och förfaranden för drift av obemannade luftfartyg.

Nya Zeeland. Ett sådant avtal kommer att ytterligare stärka Europols kapacitet att samarbeta med Nya Zeeland för att förhindra och bekämpa brottslighet som omfattas av Europols mål. Även om samarbetsavtalet från april 2019 mellan Europol och polisen i Nya Zeeland ger en ram för ett strukturerat strategiskt samarbete skapar det ingen rättslig grund för utbyte av personuppgifter. Utbyte av personuppgifter med fullt beaktande av EU:s lagstiftning och grundläggande rättigheter är en grundförutsättning för ett effektivt operationellt polissamarbete. Kommissionen har tidigare identifierat åtta prioriterade länder i Mellanöstern och Nordafrika på grundval av terroristhot, migrationsrelaterade utmaningar och Europols operativa behov med vilka förhandlingar behöver inledas.[72] Mot bakgrund av de operativa behoven hos brottsbekämpande myndigheter runtom i EU och de potentiella fördelarna med närmare samarbete på detta område, vilket uppföljningen av attacken i Christchurch i mars 2019 också visade, ser kommissionen det som nödvändigt att Nya Zeeland betraktas som ett prioriterat land att inleda förhandlingar med inom en snar framtid.

En annan hörnsten i unionens säkerhetssamarbete med tredjelandspartner är överföring av **passageraruppgifter**. Den 27 september 2019 antog kommissionen en rekommendation till rådet om bemyndigande att inleda förhandlingar om ett avtal mellan **EU och Japan** om överföring av passageraruppgifter för att förhindra och bekämpa terrorism och grov gränsöverskridande brottslighet med fullt beaktande av dataskyddsgarantier och grundläggande rättigheter[73]. Rekommendationen granskas på arbetsgruppsnivå i rådet, och kommissionen uppmanar rådet att snabbt anta ett mandat för förhandlingar med Japan. Att få en överenskommelse på plats före de olympiska spelen 2020 skulle innebära en verklig säkerhetsvinst.

På global nivå stöder kommissionen det arbete som **Internationella civila luftfartsorganisationen** bedriver för att etablera en standard för behandling av passageraruppgifter. Detta är ett svar på FN:s säkerhetsråds resolution 2396 som uppmanar alla FN:s medlemsstater att utveckla kapaciteten att samla in, bearbeta och analysera passageraruppgifter. Den 13 september 2019 lade kommissionen fram ett förslag[74] till rådets beslut om den ståndpunkt som ska intas på Europeiska unionens vägnar i Internationella civila luftfartsorganisationen vad gäller standarder och rekommenderade förfaranden för registrering av passageraruppgifter. Förslaget granskas på arbetsgruppsnivå i rådet och kommissionen uppmanar rådet att snabbt anta rådets beslut. Unionens och medlemsstaternas ståndpunkt angavs också i ett informationsdokument om standarder och principer för insamling, användning, bearbetning och skydd av passageraruppgifter som lades fram vid det 40:e sammanträdet i Internationella civila luftfartsorganisationen.

Vad gäller arbetet med att ta fram ett nytt avtal om passageraruppgifter med **Kanada** strävar kommissionen efter att snabbt slutföra avtalet. Samtidigt inleddes den kombinerade gemensamma översynen och gemensamma utvärderingen av avtalet om passageraruppgifter med **Australien** och den gemensamma utvärderingen av avtalet om passageraruppgifter med **Förenta staterna** under den gångna sommaren genom besök i Canberra och Washington i augusti respektive september 2019. Kommissionen informerade Europaparlamentets utskott för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor under ett slutet

[72] Se den elfte rapporten om framsteg i riktning mot en effektiv och verklig säkerhetsunion (COM(2017) 608 final (18.10.2017)). De prioriterade länderna är Algeriet, Egypten, Israel, Jordanien, Libanon, Marocko, Tunisien och Turkiet.

[73] COM(2019) 420 final (27.9.2019).

[74] COM(2019) 416 final (13.9.2019).

sammanträde den 14 oktober 2019 om läget i arbetet med Japan, Australien och Kanada om passageraruppgifter.

Framsteg har också gjorts i samarbetet med EU:s partner på **västra Balkan** genom genomförandet av den gemensamma handlingsplanen om terrorismbekämpning för västra Balkan. Den 9 oktober undertecknade kommissionen två icke-bindande bilaterala överenskommelser om terrorismbekämpning med Albanien och Nordmakedonien[75]. I dessa överenskommelser fastställs specialanpassade prioriterade åtgärder som ska vidtas av myndigheterna i varje partnerland. Åtgärderna omfattar de fem målen för den gemensamma handlingsplanen[76] och anger vilket stöd kommissionen planerar att tillhandahålla. Liknande överenskommelser med övriga partner på västra Balkan ska enligt planerna undertecknas under de kommande veckorna. Den 7 oktober 2019 undertecknade kommissionen även ett avtal med Montenegro om ett gränsförvaltningssamarbete mellan Montenegro och Europeiska gräns- och kustbevakningsbyrån (Frontex). Avtalet ger byrån möjlighet att bistå Montenegro i gränsförvaltningen för att försöka komma till rätta med irreguljär migration och gränsöverskridande brottslighet och därmed förbättra säkerheten vid EU:s yttre gräns.

För att stärka samarbetet med partnerländer när det gäller att ta itu med gemensamma säkerhetshot uppmanar kommissionen rådet att

- anta bemyndigandet att inleda förhandlingar om ett avtal mellan EU och **Nya Zeeland** om utbyte av personuppgifter för att bekämpa grov brottslighet och terrorism,
- anta bemyndigandet att inleda förhandlingar om ett avtal mellan EU och **Japan** om överföring av passageraruppgifter,
- anta förslaget till **rådets beslut om den ståndpunkt som ska intas på EU:s vägnar i Internationella civila luftfartsorganisationen** vad gäller standarder och rekommenderade förfaranden för registrering av passageraruppgifter.

VI. SLUTSATS

I denna rapport redovisas en mängd olika åtgärder som EU har vidtagit för att hantera gemensamma hot i Europa och stärka vår kollektiva säkerhet. De framsteg som gjorts i riktning mot en effektiv och verklig säkerhetsunion har styrts av en gemensam insikt om att det bästa sättet att lösa dagens säkerhetsutmaningar är genom att arbeta tillsammans och med tredjeländer, och är resultatet av ett nära samarbete mellan flera olika aktörer för att skapa förtroende, dela resurser och bemöta hot gemensamt: på alla offentliga nivåer, från städer och andra lokala aktörer, regioner och nationella myndigheter, till den europeiska nivån med Europaparlamentet och rådet; med deltagande från offentliga myndigheter, EU:s byråer, privata aktörer och det civila samhället; och med hjälp av sakkunskap, verktyg och resurser från alla politikområden, såsom transportpolitiken, den digitala inre marknaden och sammanhållningspolitiken. På detta sätt integreras arbetet inom säkerhetsunionen med skyddet av grundläggande rättigheter och garanteras och främjas våra gemensamma värderingar.

[75] https://ec.europa.eu/home-affairs/news/news/20191009_security-union-implementing-counter-terrorism-arrangements-albania-north-macedonia_en

[76] I den gemensamma handlingsplanen fastställs åtgärder för följande fem mål: en stabil ram för bekämpning av terrorism, effektivt förebyggande och effektiv bekämpning av våldsbejakande extremism, effektivt informationsutbyte och operativt samarbete, kapacitetsuppbyggnad för att bekämpa penningtvätt och finansiering av terrorism, förstärkning av skyddet för medborgare och infrastruktur.

Arbetet för en effektiv och verklig säkerhetsunion måste fortsätta. Överenskommelser behöver snabbt nås för en rad pågående initiativ, i synnerhet 1) lagstiftningsförslaget om att avlägsna terrorisminnehåll på nätet, 2) lagstiftningsförslaget om att förbättra brottsbekämpande myndigheters tillgång till elektroniska bevis, 3) lagstiftningsförslaget om att inrätta ett europeiskt kompetenscentrum för cybersäkerhet inom näringsliv, teknik och forskning och ett nätverk av nationella samordningscentrum, och 4) de ännu ej antagna lagstiftningsförslagen om starkare och smartare informationssystem för säkerhet, gränsförvaltning och migrationshantering. Alla medlemsstater måste snabbt och till fullo genomföra EU:s lagstiftning för att överenskomna åtgärder och instrument ska kunna förvandlas till praktisk verklighet och medlemsstaterna dra full nytta av dem för sin säkerhet. Det är särskilt viktigt att alla medlemsstater genomför den nyligen antagna lagstiftningen om interoperabilitet mellan EU:s informationssystem för säkerhet, gränsförvaltning och migrationshantering för att det ambitiösa målet om att uppnå full interoperabilitet senast 2020 ska kunna uppnås. Slutligen måste Europa förbli vaksamt på andra framväxande och förändrade hot och arbeta tillsammans för att öka säkerheten för alla medborgare.