EUROPEISKA
KOMMISSIONEN

Bryssel den 20.3.2019
COM(2019) 145 final

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET, EUROPEISKA RÅDET OCH RÅDET

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

{SWD(2019) 140 final}

I. INLEDNING

Detta är den artonde rapporten om framsteg som gjorts i riktning mot en effektiv och verklig säkerhetsunion. Den omfattar utvecklingen på 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.

Inför valet till Europaparlamentet i maj 2019 framhäver denna rapport det viktiga arbete som gjorts på olika nivåer för att hantera och förebygga cyberhot och desinformation i valsammanhang. Som svar på Europeiska rådets uppmaning till åtgärder för att skydda unionens demokratiska system och bekämpa desinformation under förberedelserna inför det kommande valet har unionen gjort betydande framsteg i riktning mot mer samordnade insatser för att öka valrörelsernas motståndskraft. Med tanke på att det är bråttom att se till att unionen är beredd innan de europeiska väljarna går till valurnorna i maj 2019 uppmanar kommissionen emellertid alla berörda aktörer – statliga myndigheter, politiska partier och framför allt onlineplattformar – att fördubbla sina ansträngningar för att skydda valrörelserna mot desinformation. Inför Europeiska rådets kommande möte den 21–22 mars 2019, där man kommer att diskutera framstegen på detta område, uppmanar kommissionen även medlemsstaterna att stärka sin samordning kring desinformation och trygga valet till Europaparlamentet.

EU har gjort betydande framsteg i arbetet för en effektiv och verklig säkerhetsunion, och har nått överenskommelser om ett antal prioriterade lagstiftningsinitiativ som kommer att förbättra säkerheten för alla medborgare. Under de senaste månaderna[1] har Europaparlamentet och rådet nått en överenskommelse om interoperabilitet mellan EU:s informationssystem för säkerhet, gränsförvaltning och migrationshantering samt om nya EU-regler för att täppa till terroristers och brottslingars handlingsutrymme genom att göra det svårare för dem att få tillgång till sprängämnesprekursorer, finansiera sin verksamhet och resa utan upptäckt. En överenskommelse har nåtts om 15 av de 22 lagstiftningsinitiativ som kommissionen har lagt fram inom ramen för säkerhetsunionen (se förteckningen över alla initiativ inom säkerhetsunionen i *bilaga I*), vilket innebär att EU uppnår resultat på ett område som prioriteras av såväl Europaparlamentet och rådet som av kommissionen[2].

Mer arbete behövs dock fortfarande. I synnerhet måste medlagstiftarna under innevarande mandatperiod bemöta det överhängande hot som utgörs av terrorisminnehåll online genom att nå en överenskommelse om kommissionens förslag. Europaparlamentet och rådet måste också nå en överenskommelse om kommissionens förslag om en förstärkt europeisk gräns- och kustbevakning för att öka säkerheten genom förbättrat skydd av unionens yttre gränser.

De tragiska händelserna i Christchurch i Nya Zeeland den 15 mars visar att terrorismen fortfarande är ett reellt och närvarande hot, oavsett om den drivs av högerextremism eller andra extremistiska ideologier. Svårigheterna med att försöka avlägsna livestreamat innehåll från nätplattformar och förhindra att det dyker upp på nytt understryker ytterligare den oerhörda vikten av kommissionens förslag om terrorisminnehåll online. Det är avgörande att

[1] Detta är en vidareutveckling av framsteg som gjorts i arbetet för en effektiv och verklig säkerhetsunion. För en komplett översikt, se tidigare lägesrapporter om säkerhetsunionen: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en.

[2] Se den gemensamma förklaringen om EU:s lagstiftningsprioriteringar för 2018–2019: https://ec.europa.eu/commission/sites/beta-political/files/joint-declaration-eu-legislative-priorities-2018-19_en.pdf.

medlagstiftarna enas om de föreslagna reglerna om avlägsnande av terrorisminnehåll online utan dröjsmål. Det är lika viktigt för kampen mot terrorism i alla dess former att samtliga medlemsstater fullt ut genomför den lagstiftning som EU – framför allt som svar på terroristattacker i Europa – har antagit för att täppa till terroristernas handlingsutrymme, i synnerhet direktiven om bekämpning av terrorism och om kontroll av förvärv och innehav av vapen. Kommissionen har också arbetat aktivt för att bekämpa extremism och vidtagit lämpliga åtgärder mot olaglig hatpropaganda online, antimuslimskt hat och antisemitism.

I denna rapport redogörs för de framsteg som gjorts när det gäller genomförandet av andra prioriterade säkerhetsärenden, i synnerhet åtgärder för att förbättra skyddet av offentliga platser. Ett fullständigt och korrekt genomförande av överenskomna åtgärder är av yttersta prioritet för att säkerställa full nytta av en effektiv och verklig säkerhetsunion. Kommissionen stöder aktivt medlemsstaterna, även genom finansiering och genom att underlätta utbyte av bästa praxis. När det är nödvändigt utnyttjar kommissionen också sina befogenheter enligt fördragen fullt ut för att verkställa EU:s lagstiftning, även genom överträdelseförfaranden när så är lämpligt.

Uppmärksammandet av den femtonde europeiska minnesdagen för terrorismens offer den 11 mars 2019, femton år efter bomberna i Madrid den 11 mars 2004 och tre år efter de dödliga attackerna i Bryssel och Zaventem den 22 mars 2016, utgör bakgrunden till denna rapport. Stödet till offer för terroristattacker är en viktig del av arbetet för en effektiv och verklig säkerhetsunion. För att ytterligare öka detta stöd antog kommissionen den 31 januari 2019 ett beslut om finansiering av pilotprojektet ”Inrättande av EU:s expertcentrum för terrorismens offer”[3]. EU:s expertcentrum kommer att fungera som ett nav för sakkunskap och en plattform för yrkesverksamma som arbetar med offer för terrorism.

Kommissionen välkomnar Europaparlamentets rapport om slutsatser och rekommendationer från särskilda utskottet för terrorismfrågor[4] som ett värdefullt bidrag till det gemensamma arbetet för en effektiv och verklig säkerhetsunion.

II. FÖRVERKLIGANDE AV LAGSTIFTNINGSPRIORITERINGAR

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

Informationsutbyte är en central del av EU:s stöd till nationella myndigheter i kampen mot terrorism och grov brottslighet. I detta avseende innebär interoperabiliteten mellan EU-omfattande informationssystem en radikal förändring av det sätt som nationella myndigheter får uppgifter, samtidigt som det garanteras att uppgifterna är korrekta och fullständiga. Medlagstiftarna har nått en politisk överenskommelse om de sammanhängande prioriterade lagstiftningsförslagen om **interoperabilitet mellan EU:s informationssystem** för säkerhet, gränsförvaltning och migrationshantering[5]. Tack vare de föreslagna åtgärderna kommer EU:s

[3] C(2019) 636 final, 31.1.2019.

[4] Europaparlamentets resolution av den 12 december 2018 om slutsatser och rekommendationer från särskilda utskottet för terrorismfrågor (2018/2044(INI)).

[5] COM(2017) 793 final (12.12.2017), COM(2017) 794 final (12.12.2017), COM(2018) 478 final (13.6.2018) och COM(2018) 480 final (13.6.2018). Den politiska överenskommelse som nåddes den 5 februari 2019 godkändes av Ständiga representanternas kommitté den 13 februari och av Europaparlamentets utskott för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor den 19 februari.

informationssystem att samverka på ett intelligentare och mer målinriktat sätt, samtidigt som de grundläggande rättigheterna respekteras fullt ut. Med hjälp av att befintliga uppgifter används på bästa möjliga sätt kommer interoperabiliteten att täppa till informationsluckor och döda vinklar genom att göra det lättare att upptäcka multipla identiteter och bekämpa identitetsbedrägeri. När medlagstiftarna formellt antagit de nya reglerna kommer kommissionen att vara beredd att stödja medlemsstaterna i genomförandet. Nära samarbete mellan EU:s organ och alla medlemsstater och Schengenassocierade länder krävs för att det ska gå att uppnå det ambitiösa målet att uppnå full interoperabilitet mellan EU:s informationssystem för säkerhet, gränsförvaltning och migrationshantering senast 2020. I förberedelse inför detta hölls en första workshop med medlemsstaternas experter den 5 mars 2019 för att inleda en effektiv samordningsprocess.

I detta skede gäller den framtida interoperabiliteten följande EU-informationssystem: det stärkta **Schengens informationssystem**[6], det befintliga **Informationssystemet för viseringar**[7], den nyss överenskomna utvidgningen av det **europeiska informationssystemet för utbyte av uppgifter ur kriminalregister**[8] till tredjelandsmedborgare samt nyinrättade **in- och utresesystemet**[9] och **EU-systemet för reseuppgifter och resetillstånd (Etias)**[10].

Som ett led i den tekniska implementeringen av EU-systemet för reseuppgifter och resetillstånd lade kommissionen den 7 januari 2019 fram ett förslag om tekniska ändringar av den relaterade förordningen[11]. De föreslagna ändringarna avser rättsakterna om de EU-informationssystem som EU-systemet för reseuppgifter och resetillstånd kommer att söka i som en del av bedömningen av vilken säkerhetsrisk eller risk för irreguljär migration tredjelandsmedborgare utgör innan de reser till Schengenområdet. De föreslagna ändringarna är nödvändiga för att EU-systemet för reseuppgifter och resetillstånd ska kunna inrättas. Kommissionen uppmanar medlagstiftarna att påskynda sitt arbete med de tekniska ändringarna för att nå en överenskommelse så snart som möjligt, så att EU-systemet för reseuppgifter och resetillstånd kan implementeras snabbt och tas i drift enligt tidtabellen i början av 2021.

I maj 2018 lade kommissionen fram ett förslag om att **stärka det befintliga Informationssystemet för viseringar**[12] för att möjliggöra noggrannare bakgrundskontroller av viseringssökande och täppa till informationsluckor genom bättre informationsutbyte mellan medlemsstaterna. Rådet antog sitt förhandlingsmandat den 19 december 2018 och den 13 mars 2019 röstade Europaparlamentets plenarförsamling igenom sitt betänkande om förslaget och avslutade därmed sin första behandling. Kommissionen uppmanar medlagstiftarna att snabbt inleda förhandlingar under Europaparlamentets nästa mandatperiod.

---

6 Förordning (EU) 2018/1860 (28.11.2018), förordning (EU) 2018/1861 (28.11.2018), förordning (EU) 2018/1862 (28.11.2018).

7 Förordning (EG) nr 767/2008, 9.7.2008.

8 Medlagstiftarna nådde en politisk överenskommelse om detta prioriterade förslag den 11 december 2018 (COM(2017) 344 final, 29.6.2017). Ständiga representanternas kommitté godkände överenskommelsen den 19 december 2018. Europaparlamentets plenarförsamling bekräftade överenskommelsen den 11 mars 2019.

9 Förordning (EU) 2017/2226, 30.11.2017.

10 Förordning (EU) 2018/1240 (12.9.2018) och förordning (EU) 2018/1241 (12.9.2018).

11 COM(2019) 4 final, 7.1.2019.

12 COM(2018) 302 final, 16.5.2018.

I maj 2016 föreslog kommissionen att **Eurodacs**[13] tillämpningsområde skulle utvidgas till att omfatta identifiering inte bara av asylsökande utan även av tredjelandsmedborgare som vistas olagligt i medlemsstaterna och av dem som tar sig in i EU på ett irreguljärt sätt. I linje med Europeiska rådets slutsatser från december 2018[14] och kommissionens meddelande av den 6 mars 2019 om framstegen i genomförandet av den europeiska migrationsagendan[15] uppmanar kommissionen medlagstiftarna att utan dröjsmål anta förslaget. Genom att detta lagstiftningsförslag antas blir det möjligt att omfatta Eurodac i den framtida arkitekturen av interoperabla EU-informationssystem och således integrera centrala uppgifter om tredjelandsmedborgare som vistas olagligt i EU och de som har rest in i EU på ett irreguljärt sätt.

Kommissionen uppmanar Europaparlamentet och rådet att göra följande för att stärka EU-informationssystemen för säkerhet, gränsförvaltning och migrationshantering:

- Anta lagstiftningsförslaget om **Eurodac**, som närmar sig en överenskommelse, före valet till Europaparlamentet. (*Prioritering från den gemensamma förklaringen*)
- Arbeta vidare för att nå en snabb överenskommelse om de föreslagna tekniska ändringar som krävs för att inrätta **EU-systemet för reseuppgifter och resetillstånd**.

2. Stärkt säkerhet genom bättre förvaltning av de yttre gränserna

Ett starkt skydd av de yttre gränserna är en förutsättning för säkerheten inom området för fri rörlighet utan inre gränskontroller. Detta är en uppgift för medlemsstaterna, som måste säkerställa förvaltningen av sina yttre gränser både för sin egen skull och för allas gemensamma intresse, med stöd från **Europeiska gräns- och kustbevakningsbyrån**. Som svar på Europeiska rådets slutsatser från juni 2018[16] föreslog kommissionen i september 2018 att den europeiska gräns- och kustbevakningens kapacitet skulle stärkas[17]. Det skulle leda byrån till en ny operativ etapp med egen utrustning och en permanent kår på 10 000 gränskontrolltjänstemän som utövar verkställande befogenheter, samtidigt som både de grundläggande rättigheterna och medlemsstaternas suveränitet respekteras fullt ut.

Lagstiftningsarbetet med förslaget är på god väg och förhandlingarna mellan medlagstiftarna har gått in i ett avgörande skede. Europaparlamentet antog sitt förhandlingsmandat den 11 februari 2019, medan rådet fick sitt mandat den 20 februari. Två trepartsmöten hölls den 27 februari och den 12 mars. Kommissionen välkomnar och stöder de framsteg som gjorts i detta prioriterade ärende och som visar att alla institutioner är fast beslutna att anta detta förslag före valet till Europaparlamentet 2019.

För att stärka säkerheten genom bättre förvaltning av de yttre gränserna, uppmanar kommissionen Europaparlamentet och rådet att göra följande:

- Anta lagstiftningsförslaget om att stärka den **europeiska gräns- och kustbevakningen** under Europaparlamentets innevarande mandatperiod. (*Initiativ från talet om tillståndet i unionen 2018*)

---

13 COM(2016) 272 final, 4.5.2016.

14 https://www.consilium.europa.eu/sv/press/press-releases/2018/12/14/european-council-conclusions-13-14-december-2018/.

15 COM(2019) 126 final, 6.3.2019.

16 https://www.consilium.europa.eu/media/35936/28-euco-final-conclusions-en.pdf.

17 COM(2018) 631 final, 12.9.2018.

3. Förebygga radikalisering

Motverkande av terrorisminnehåll online är fortfarande en viktig utmaning i kampen mot terrorism och förebyggande av radikalisering. Sådant innehåll har spelat en roll i de flesta attacker på europeisk mark under de senaste två åren, antingen genom anstiftan till angrepp och instruktioner om hur de ska genomföras eller genom förhärligande av den dödliga utgången. För att komma till rätta med den uppenbara och reella faran som sådant innehåll utgör åtföljdes Jean-Claude Junckers tal om tillståndet i unionen 2018 av ett förslag[18] till förordning om **terrorisminnehåll online**, där en rättslig ram fastställdes för att förhindra att värdtjänstleverantörer missbrukas för att sprida terrorisminnehåll på nätet. Samtidigt som yttrandefriheten och andra grundläggande rättigheter garanteras fullt ut är det mycket viktigt att de framtida reglerna föreskriver effektiva åtgärder för att avlägsna terrorisminnehåll online så snabbt som möjligt, med tanke på att den potentiella skada som orsakas av sådant innehåll ökar för varje timme det ligger ute på nätet.

Rådet antog sitt förhandlingsmandat i december 2018, men arbetet i Europaparlamentet pågår fortfarande och kommer förhoppningsvis att göra det möjligt för parlamentet att anta sitt förhandlingsmandat under mars 2019[19]. Kommissionen uppmanar båda medlagstiftarna att nå en överenskommelse om den föreslagna lagstiftningen under Europaparlamentets innevarande mandatperiod, med tanke på den oerhörda vikten av ett EU-regelverk för avlägsnande av terrorisminnehåll online med tydliga regler och skyddsåtgärder.

Parallellt med detta fortsätter kommissionen att stödja medlemsstaterna i deras insatser för att **förebygga radikalisering**. En särskild EU-samarbetsmekanism som samlar nationella företrädare bidrar till att se till att EU-stödet motsvarar medlemsstaternas behov[20]. Exempel från senare tid är en konferens om ”EU:s städer mot radikalisering” som anordnades tillsammans med Regionkommittén den 26 februari 2019. Den 13 mars 2019 anordnade kommissionen ett expertmöte med nationella beslutsfattare för att identifiera praktiska åtgärder som ytterligare stöder fångvårds- och kriminalvårdsväsendet. Resultatet av detta arbete kommer att bli en del av en handbok som EU:s nätverk för kunskapsspridning om radikalisering håller på att utarbeta om rehabilitering och återanpassning av terrorbrottslingar, återvändande utländska terroristtridande och personer som radikaliserats i fängelset (se även avsnitt IV.4 om externa åtgärder).

För att förebygga radikalisering uppmanar kommissionen Europaparlamentet att göra följande:

- Som en prioriterad fråga anta sitt förhandlingsmandat om lagstiftningsförslaget om att förhindra spridning av **terrorisminnehåll online**, så att medlagstiftarna kan nå en överenskommelse om lagstiftningen under Europaparlamentets innevarande mandatperiod. (*Initiativ från talet om tillståndet i unionen 2018*)

[18] COM(2018) 640 final, 12.9.2018.

[19] Europaparlamentets utskott för den inre marknaden och konsumentskydd röstade om sitt yttrande den 4 mars 2019. Europaparlamentets utskott för kultur och utbildning röstade igenom sitt betänkande den 11 mars 2019. Europaparlamentets utskott för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor förväntas rösta om sitt betänkande den 21 mars 2019.

[20] Medlemsstaternas behov när det gäller att förebygga radikalisering har för första gången identifierats i de s.k. strategiska riktlinjerna för EU:s förebyggande åtgärder för 2019. De strategiska riktlinjerna finns här: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3626&news=1&mod_groups=1&month=08&year=2018.

4. Ökad cybersäkerhet

Klassiska cyberhot mot system och data fortsätter att öka, med ökad aktivitet från fientliga aktörer mot många olika mål och offer under 2018. Att motverka it-brottslighet och förbättra cybersäkerheten är därför fortfarande en prioriterad fråga för EU. EU har gjort påtagliga framsteg när det gäller att förbättra cybersäkerheten och genomföra de åtgärder som angavs i det gemensamma meddelandet *Resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU*[21] från september 2017.

Den 12 mars 2019 bekräftade Europaparlamentets plenarförsamling den politiska överenskommelse som medlagstiftarna nått om **cybersäkerhetsakten**. Akten förväntas träda i kraft i maj och kommer att öka cybersäkerhetskapaciteten och medlemsstaternas och företagens beredskap. Genom cybersäkerhetsakten inrättas en EU-ram för cybersäkerhetscertifiering för produkter, system och tjänster inom informations- och kommunikationsteknik. Den kommer även att förbättra samarbetet och samordningen mellan medlemsstaterna och EU:s institutioner, byråer och organ, i synnerhet den omdöpta EU:s cybersäkerhetsbyrå.

Ytterligare framsteg krävs dock när det gäller kommissionens förslag om ett **europeiskt kompetenscentrum för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentraler** från september 2018[22]. Förslaget syftar till att stödja teknisk och industriell kapacitet på cybersäkerhetsområdet och öka konkurrenskraften för unionens cybersäkerhetsbransch. Europaparlamentet och rådet antog sina förhandlingsmandat den 13 mars 2019. Det första trepartsmötet ägde också rum samma dag. Kommissionen uppmanar medlagstiftarna att nå en snabb överenskommelse om den föreslagna lagstiftningen.

EU har gjort betydande framsteg när det gäller att ytterligare förverkliga sin **gemensamma diplomatiska respons mot skadlig it-verksamhet** (”verktygslådan för cyberdiplomati”), som ett svar på Europeiska rådets uppmaning[23] att fortsätta arbetet med kapaciteten att reagera på och avskräcka från cyberattacker genom restriktiva åtgärder på EU-nivå. Den 8 mars 2019 lade unionens höga representant för utrikes frågor och säkerhetspolitik och kommissionen fram ett gemensamt förslag till rådets förordning om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater. Kommissionen och den höga representanten efterlyser snabbt antagande av detta förslag för att stärka unionens motståndskraft mot cyberattacker.

För att förbättra cybersäkerheten uppmanar kommissionen och den höga representanten rådet att göra följande:
• Anta rådets förordning om **restriktiva åtgärder mot cyberattacker** som hotar unionen eller dess medlemsstater.

5. Minimerat handlingsutrymme för terrorister

[21] JOIN(2017) 450 final, 13.9.2017.
[22] COM(2018) 630 final, 12.9.2018.
[23] Se rådets slutsatser från juni och oktober 2018.

EU har vidtagit ytterligare åtgärder för att hindra terrorister och brottslingar från att agera genom att göra det svårare för dem att få tillgång till sprängämnesprekursorer, finansiera sin verksamhet och resa utan att bli upptäckta.

Europaparlamentet och rådet nådde en politisk överenskommelse den 14 februari 2019 om den föreslagna förordningen om **restriktioner mot marknadsföring och användning av sprängämnesprekursorer**[24]. När förordningen blir tillämplig kommer den att förbättra den gällande rättsliga ramen på ett betydande sätt, genom att begränsa tillgången till farliga sprängämnesprekursorer som kan missbrukas för att bygga hemmagjorda bomber. Den kommer att täppa till säkerhetsluckor med åtgärder såsom förbud mot ytterligare kemikalier, obligatoriska kontroller av brottsregistret för personer som ansöker om tillstånd för inköp av begränsade ämnen samt förtydligande av att de regler som gäller ekonomiska aktörer också gäller företag som bedriver verksamhet på nätet.

Dessutom har medlagstiftarna, som en del av insatserna för att bekämpa finansiering av terrorism, nått en överenskommelse om det föreslagna direktivet om att **underlätta användningen av finansiell och annan information** för att förebygga, upptäcka, utreda eller lagföra allvarliga brott[25]. När direktivet formellt har antagits och genomförts kommer det att ge utsedda brottsbekämpande myndigheter och kontor för återvinning av tillgångar direkt tillgång till bankkontouppgifter i nationella centraliserade bankkontoregister. Direktivet kommer också att stärka samarbetet mellan nationella finansunderrättelseenheter och brottsbekämpande myndigheter och underlätta Europols tillgång till finansiell information.

Med utgångspunkt i detta kommer kommissionen att ytterligare överväga samarbete mellan finansunderrättelseenheter i olika medlemsstater, bland annat i den kommande rapporten om samarbetet mellan finansunderrättelseenheter i enlighet med det femte penningtvättsdirektivet[26]. Dessutom utvärderar kommissionen aspekter som rör eventuell sammankoppling av nationella centraliserade bankkontoregister och dataåtervinningssystem i EU, även detta i enlighet med det femte penningtvättsdirektivet. Kommissionen analyserar också åtgärder för förverkande utan föregående fällande dom i unionen. Slutligen kommer kommissionen, som ett svar på ännu en uppmaning från Europaparlamentet[27], att fortsätta att bedöma nödvändigheten, den tekniska genomförbarheten och proportionaliteten av ytterligare åtgärder för att spåra finansiering av terrorism i EU.

Som en del av arbetet med att bekämpa dokumentförfalskning nådde medlagstiftarna den 19 februari 2019 en preliminär överenskommelse om den föreslagna förordningen om **säkrare identitetskort för unionsmedborgare och uppehållshandlingar**[28] så att brottslingar och

---

24 COM(2018) 209 final, 17.4.2018.

25 Medlagstiftarna nådde en politisk överenskommelse om kommissionens förslag den 12 februari 2019 (COM(2018) 213 final, 17.4.2018). Överenskommelsen godkändes av Ständiga representanternas kommitté den 20 februari och av Europaparlamentets utskott för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor den 26 februari.

26 Enligt artikel 65.2 i direktiv (EU) 2018/843 (19.6.2018) ska kommissionen senast den 1 juni 2019 utvärdera ramen för finansunderrättelseenheternas samarbete med tredjeländer och hinder och möjligheter när det gäller att förbättra samarbetet mellan finansunderrättelseenheter i unionen, inbegripet möjligheten att inrätta en mekanism för samordning och stöd.

27 Europaparlamentets särskilda utskott för terrorism efterlyste i sin slutrapport, som antogs i december 2018, inrättandet av ett EU-system för att spåra finansiering av terrorism, inriktat på transaktioner som görs av enskilda personer med kopplingar till terrorism och deras finansiering inom det gemensamma eurobetalningsområdet.

28 COM(2018) 212 final, 17.4.2018.

terrorister inte kan använda dem på ett bedrägligt sätt. Europaparlamentets utskott för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor bekräftade överenskommelsen den 11 mars 2019. När förordningen har antagits inför den framför allt minimikrav på säkerhetsdetaljer för id-kort, som måste innehålla biometriska kännetecken (ansiktsbild och två fingeravtryck) på ett kontaktlöst chipp. Detta kommer att göra nationella identitetskort och uppehållshandlingar betydligt säkrare och göra det svårare för terrorister och andra brottslingar att missbruka eller förfalska sådana dokument för att ta sig in i eller förflytta sig inom EU. Säkrare identitetshandlingar kommer att bidra till att stärka förvaltningen av EU:s yttre gränser. Samtidigt kommer säkrare och tillförlitligare handlingar göra det lättare för EU-medborgarna att utöva sin rätt till fri rörlighet.

Ytterligare framsteg krävs dock i fråga om kommissionens förslag om **tillgång till elektroniska bevis** från april 2018, med tanke på att över hälften av alla brottsutredningar i dag inbegriper en gränsöverskridande begäran om tillgång till elektroniska bevis[29]. Rådet har antagit sitt förhandlingsmandat om förslagen till en förordning[30] om att förbättra den gränsöverskridande tillgången till elektroniska bevis i brottsutredningar och till ett direktiv[31] om fastställande av harmoniserade bestämmelser för utseende av rättsliga företrädare för insamling av bevisning i straffrättsliga förfaranden. I Europaparlamentet har framstegen med förslagen dock varit mycket försiktiga sedan kommissionen antog dem i april 2018. Med tanke på hur oerhört viktigt det är med effektiv tillgång till elektroniska bevis för lagföring av gränsöverskridande brott såsom terrorism eller it-brottslighet uppmanar kommissionen Europaparlamentet enträget att gå vidare med detta förslag.

Parallellt med detta arbetar kommissionen på sina **internationella initiativ om tillgång till elektroniska bevis** i samband med de pågående förhandlingarna om ett andra tilläggsprotokoll till Europarådets Budapestkonvention om it-brottslighet och med Förenta staterna. Därför antog kommissionen rekommendationer[32] om förhandlingsmandat för båda dessa internationella initiativ den 5 februari 2019. Rådet håller på att diskutera utkasten till mandat, bland annat vid mötet i rådet (rättsliga och inrikes frågor) den 7–8 mars 2019. Kommissionen uppmanar rådet att anta beslutet om bemyndigande att delta i förhandlingar om ett andra tilläggsprotokoll till Europarådets Budapestkonvention om it-brottslighet, samt beslutet om bemyndigande att inleda förhandlingar med Förenta staterna om gränsöverskridande tillgång till elektroniska bevis. 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.

För att minimera terroristernas handlingsutrymme uppmanar kommissionen Europaparlamentet och rådet att göra följande:

- **Europaparlamentet** bör som ett brådskande ärende anta sitt förhandlingsmandat om lagstiftningsförslagen om **elektroniska bevis** för att inleda trepartsdiskussioner med rådet

[29] Elektroniska bevis behövs i omkring 85 % av alla brottsutredningar, och i två tredjedelar av dessa utredningar måste bevisen begäras från onlinetjänsteleverantörer baserade i en annan jurisdiktion. Se den konsekvensbedömning som åtföljer lagstiftningsförslaget (SWD(2018) 118 final, 17.4.2018).

[30] COM(2018) 225 final, 17.4.2018. Rådet antog sitt förhandlingsmandat om den föreslagna förordningen vid sitt möte (rättsliga och inrikes frågor) den 7 december 2018.

[31] COM(2018) 226 final, 17.4.2018. Rådet antog sitt förhandlingsmandat om det föreslagna direktivet vid sitt möte (rättsliga och inrikes frågor) den 8 mars 2019.

[32] COM(2019) 70 final, 5.2.2019, och COM(2019) 71 final, 5.2.2019.

utan dröjsmål. (*Prioritering från den gemensamma förklaringen*)

- **Rådet** bör anta besluten om bemyndigande att delta i förhandlingar om ett **andra tilläggsprotokoll till Europarådets Budapestkonvention om it-brottslighet**, samt om bemyndigande att inleda **förhandlingar med Förenta staterna** om gränsöverskridande tillgång till elektroniska bevis.

III. MOTVERKA DESINFORMATION OCH SKYDDA VAL MOT ANDRA CYBERBASERADE HOT

Externa och interna aktörers möjligheter att blanda sig i offentliga debatter och manipulera val är verkligare än någonsin och kan öka ytterligare i samband med det kommande valet till Europaparlamentet. De konsekvenser som detta kan få – att demokratiska institutioner undergrävs eller förlorar sin legitimitet – är ett allvarligt, strategiskt och växande hot. Detta är en nyckeldel av EU:s säkerhetsutmaningar över de nationella gränserna i dagens läge och kräver gemensamma, gränsöverskridande insatser.

Kampanjerna inför Europaparlamentsvalet inleds på allvar i mars. Inför Europeiska rådets möte den 21–22 mars uppmanar kommissionen medlemsstaterna att öka sin samordning och sitt informationsutbyte för att motverka desinformation och skydda valen mot cyberbaserade hot. Medlemsstaterna bör till fullo utnyttja de verktyg och informationskanaler som EU tillhandahåller, i synnerhet det nyinrättade systemet för snabb varning[33]. På grund av oro för den nuvarande situationen uppmanar kommissionen dessutom onlineplattformarna att påskynda sina ansträngningar i alla medlemsstater för att säkra integriteten för valet till Europaparlamentet i maj 2019.

För att stödja och uppmuntra dessa insatser fortsätter kommissionen och den höga representanten att vidta åtgärder på två kompletterande områden för att avvärja cyberbaserade hot, nämligen genom att motverka desinformation och stärka valrörelsernas motståndskraft.

1. Åtgärder mot desinformation

Att allmänheten blir utsatt för desinformation i stor skala, t.ex. missvisande eller fullständigt falska uppgifter, är en annan allvarlig typ av cyberbaserat hot som kan bli en stor utmaning vid EU-valet i vår. Kommissionen övervakar noga genomförandet av de åtgärder som anges i meddelandet ***Bekämpande av desinformation online***[34] **i april 2018**.

Kommissionen övervakar också noga de framsteg som görs enligt den **uppförandekod om desinformation** som undertecknats av företrädare för onlineplattformar, ledande sociala nätverk, marknadsförare och reklambranschen i oktober 2018 (se nedan). Kommissionen kommer att helhetsutvärdera tillämpningen av uppförandekoden efter de första tolv månaderna. Om uppförandekoden inte följs eller resultaten inte är tillfredsställande kan kommissionen föreslå fler åtgärder, bland annat någon sorts regelverk.

---

[33] Som en del av den handlingsplan mot desinformation som kommissionen och den höga representanten lade fram i december 2018 (se nedan) kommer systemet för snabb varning att vara ett nav för medlemsstaterna, EU-institutionerna och olika partner att utbyta information om pågående desinformationskampanjer och ge dem möjlighet att samordna sina insatser. Systemet kommer att baseras enbart på oklassificerade uppgifter från öppna källor.

[34] COM(2018) 236 final, 26.4.2018, och uppföljande genomföranderapport (COM(2018) 794 final, 5.12.2018).

Med utgångspunkt i detta arbete och som svar på uppmaningen från ledarna vid Europeiska rådet i juni 2018 att skydda unionens demokratiska system lade kommissionen och den höga representanten i december 2018 fram en **gemensam handlingsplan mot desinformation**[35]. I handlingsplanen framhålls att desinformation från Ryska federationen enligt **EU:s gemensamma enhet för hybridhot** utgör det största hotet mot EU. Den är systematisk och välfinansierad och av en helt annan omfattning än andra länders. För att komma till rätta med det hot som desinformation utgör föreskriver handlingsplanen en ökning av de resurser som avsätts för kampen mot desinformation, mer specifikt for Europeiska utrikestjänstens **arbetsgrupper för strategisk kommunikation**, inklusive arbetsgruppen för strategisk kommunikation i öst[36]. I handlingsplanen föreskrivs också ökade resurser för denna fråga, och man efterlyser en förstärkning under de kommande två åren.

I handlingsplanen fastställs konkreta åtgärder för att motverka desinformation, bland annat skapandet av ett **system för snabb varning**. Inför valet till Europaparlamentet inrättades systemet för snabb varning i mars 2019 av EU-institutionerna och medlemsstaterna för att underlätta utbyte av uppgifter och bedömningar av desinformationskampanjer och för att larma om desinformationshot.

I handlingsplanen föreskrivs också en noggrann övervakning av genomförandet av den ovannämnda uppförandekod som undertecknats av onlineplattformarna. Den 29 januari offentliggjorde kommissionen **rapporter från uppförandekodens undertecknare**, dvs. Google, Facebook, Twitter, Mozilla och de branschorganisationer som företräder reklambranschen. Kommissionen välkomnade de framsteg som gjorts men uppmanade också undertecknarna att intensifiera sina ansträngningar inför valet till Europaparlamentet i vår[37].

Den 28 februari 2019 offentliggjorde EU-kommissionen **rapporter från Facebook, Google och Twitter** om hur väl de lyckades i januari med att förverkliga de åtaganden de gjort för att bekämpa desinformation. I dessa rapporter lämnade plattformarna inte tillräckligt detaljerade uppgifter som visar att nya strategier och verktyg sätts in i god tid och med tillräckliga resurser i alla medlemsstater. Det finns helt klart utrymme för förbättringar för alla undertecknare[38]. Mer specifikt uppmanar kommissionen plattformarna att se till att de politiska annonserna är fullständigt transparenta i alla medlemsstater när kampanjerna kör i gång inför EU-valet. Man behöver också ge tillgång till plattformarnas data för forskningsändamål och faktagranskning och se till att plattformarna och enskilda medlemsstater har ett fungerande samarbete genom kontaktpunkterna i systemet för snabb varning.

Kommissionen kommer att rapportera igen den 20 mars 2019 om genomförandet av ovan nämnda uppförandekod.

2. Stärka valrörelsernas motståndskraft

---

35 JOIN(2018) 36 final, 5.12.2018.

36 Sedan arbetsgruppen för strategisk kommunikation i öst inrättades 2015 har den katalogiserat, analyserat och satt strålkastarljuset på nästan 5 000 exempel på desinformation från Ryssland, uppdagat talrika desinformationsnarrativ samt ökat medvetenheten om och avslöjat verktyg, metoder och avsikter som ligger bakom desinformationskampanjerna.

37 Läs mer på http://europa.eu/rapid/press-release_IP-19-746_sv.htm.

38 Läs mer på http://europa.eu/rapid/press-release_STATEMENT-19-1379_sv.htm.

Den 12 september 2018 antog kommissionen ett åtgärdspaket för att stärka motståndskraften i våra valsystem. Paketet riktar sig till medlemsstaterna och europeiska och nationella politiska partier och stiftelser och innehåller bland annat en rekommendation om nätverk för samarbete i samband med val, transparens på nätet, skydd mot cybersäkerhetsincidenter och bekämpning av desinformationskampanjer, riktlinjer om tillämpningen av EU:s dataskyddslagstiftning[39] samt en lagändring för att skärpa reglerna om finansiering av europeiska politiska partier.

Europaparlamentet välkomnade paketet i sin resolution den 28 oktober 2018. Rådet välkomnade paketet i sina slutsatser av den 19 februari 2019 om att säkra fria och rättvisa val till Europaparlamentet, där alla medlemsstaterna gemensamt åtog sig en samordnad europeisk strategi för att skydda det kommande EU-valets integritet. Rådet (rättsliga och inrikes frågor) diskuterade läget den 7 mars 2019.

Genom ändringen av förordningen om **stadgar för och finansiering av europeiska politiska partier och stiftelser**[40] införs möjligheten att ålägga sanktioner om personuppgifter används på ett olagligt sätt för att avsiktligt påverka resultatet av valet till Europaparlamentet. Efter en politisk överenskommelse[41] i januari 2019 godkände Europaparlamentets plenarförsamling den ändrade texten den 12 mars. Ändringen planeras få laga kraft innan valet till Europaparlamentet i vår.

Rekommendationen om **valsamarbetsnätverk, onlinetransparens, skydd mot cybersäkerhetsincidenter och bekämpning av desinformationskampanjer i samband med val till Europaparlamentet**[42] riktar sig till medlemsstaterna och till nationella och europeiska politiska partier och stiftelser, och innehåller konkreta åtgärder för relevanta aktörer på dessa områden. I ett försök att genomföra rekommendationen har nationella valnätverk utsett kontaktpunkter för att delta i ett **europeiskt valsamarbetsnätverk** som syftar till att larma om hot, utbyta bästa praxis mellan nationella nätverk, diskutera gemensamma lösningar på konstaterade problem och uppmuntra gemensamma projekt och övningar mellan nationella nätverk. Vid nätverkets första möte den 21 januari 2019 enades deltagarna om att en övergripande strategi är viktig för att säkerställa valintegriteten och samtidigt bibehålla en öppen demokratisk debatt och lika villkor för alla inom politiken. Det andra mötet inom det europeiska valsamarbetsnätverket ägde rum den 27 februari, med fokus på frågor kring övervakning och genomdrivande i samband med valet, bland annat dataskydd, medieregler, brottsbekämpning, transparens och sociala medier samt olika berörda parters deltagande i övervakningen. Där lades grunden för medlemmarnas deltagande i en cyberresiliensövning direkt efter nätverkets nästa planerade möte den 5 april.

En **workshop om förbättrad cyberresiliens i valrörelserna** ordnades gemensamt av Europaparlamentet och kommissionen den 19 februari för att förbättra valsystemens och valinfrastrukturernas säkerhet och resiliens mot cyberbaserade hot som ständigt förändras. Nationella cybersäkerhetsmyndigheter från medlemsstaterna, Europeiska unionens byrå för nät- och informationssäkerhet och onlineplattformar diskuterade åtgärder, framför allt sådana som är brådskande och relevanta för att skydda integriteten för valet till Europaparlamentet 2019.

---

39 COM(2018) 638 final, 12.9.2018.

40 COM(2018) 636 final, 12.9.2018.

41 Medlagstiftarna nådde en politisk överenskommelse den 16 januari 2018. Överenskommelsen godkändes av Ständiga representanternas kommitté den 25 januari 2019 och av Europaparlamentets utskott för konstitutionella frågor den 29 januari.

42 C(2018) 5949 final, 12.9.2018.

EU-institutionerna och medlemsstaterna samarbetar också nära kring andra **medvetandehöjande åtgärder** som syftar till att skydda integriteten i valprocessen och kring engagemang från aktörer från den privata och offentliga sektorn, inklusive medier, onlineplattformar och det civila samhället.

För att motverka desinformation och säkra valrörelsernas motståndskraft uppmanar kommissionen och den höga representanten medlemsstaterna att

- snabbt och beslutsamt genomföra åtgärderna i den **gemensamma handlingsplanen mot desinformation** från december 2018.

IV. GENOMFÖRANDE AV ANDRA PRIORITERADE SÄKERHETSÄRENDEN

1. Genomförande av lagstiftningsåtgärder inom säkerhetsunionen

Ett fullständigt och korrekt genomförande av överenskomna åtgärder är av yttersta prioritet för att säkerställa full nytta av en effektiv och verklig säkerhetsunion. Kommissionen stöder aktivt medlemsstaterna, även genom finansiering och genom att underlätta utbyte av bästa praxis. När det är nödvändigt utnyttjar kommissionen också sina befogenheter enligt fördragen fullt ut för att verkställa EU:s lagstiftning, även genom överträdelseförfaranden när så är lämpligt.

Vad gäller genomförandet av **EU-direktivet om passageraruppgifter**[43] inledde kommissionen den 19 juli 2018 överträdelseförfaranden mot 14 medlemsstater för att de inte anmält antagande av nationell lagstiftning som fullständigt införlivar direktivet[44] – ett avgörande verktyg i kampen mot terrorism och grov brottslighet. Nio av dessa medlemsstater har sedan dess anmält fullständigt införlivande[45]. De medlemsstater som fortfarande inte har införlivat direktivet fullt ut har fått motiverade yttranden (Spanien den 24 januari och Nederländerna och Finland den 7 mars 2019). 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**[46] löpte ut den 8 september 2018. Den 22 november 2018 inledde kommissionen överträdelseförfaranden mot 16 medlemsstater som inte har anmält antagande av nationell lagstiftning som fullständigt införlivar direktivet. Nio av dessa medlemsstater har sedan dess anmält fullständigt införlivande[47]. Kommissionen uppmanar de återstående sju medlemsstaterna att vidta nödvändiga åtgärder så snart som möjligt[48].

---

43 Direktiv (EU) 2016/681, 27.4.2016.

44 Bulgarien, Tjeckien, Estland, Grekland, Spanien, Frankrike, Cypern, Luxemburg, Nederländerna, Österrike, Portugal, Rumänien, Slovenien och Finland.

45 Bulgarien, Estland, Grekland, Frankrike, Cypern, Luxemburg, Österrike, Portugal och Rumänien (läget den 11 mars 2019).

46 Direktiv (EU) 2017/541, 15.3.2017.

47 Bulgarien, Tjeckien, Tyskland, Estland, Spanien, Frankrike, Kroatien, Italien, Lettland, Litauen, Ungern, Malta, Nederländerna, Österrike, Portugal, Slovakien, Finland och Sverige har anmält införlivande (läget den 11 mars 2019).

48 Belgien, Polen, Rumänien och Slovenien har anmält delvis införlivande. Grekland, Cypern och Luxemburg har inte gjort någon anmälan alls (läget den 11 mars 2019).

Tidsfristen för införlivande av **direktivet om kontroll av förvärv och innehav av vapen**[49] löpte ut den 14 september 2018. Hittills har sex medlemsstater anmält fullständigt införlivande[50] och fem medlemsstater har anmält delvis införlivande[51]. 22 medlemsstater[52], inklusive de som har anmält delvis införlivande, mottog kommissionens formella underrättelse den 22 november 2018.

Vad gäller införlivandet i nationell lagstiftning av **dataskyddsdirektivet för brottsbekämpning**[53] inledde kommissionen den 19 juli 2018 överträdelseförfaranden mot 19 medlemsstater på grund av att de inte hade meddelat att de antagit nationell lagstiftning som säkerställer ett fullständigt införlivande av direktivet[54]. För närvarande har 17 medlemsstater anmält fullständigt införlivande och fem medlemsstater har anmält delvis införlivande[55]. Hittills har förfaranden mot sex medlemsstater avslutats[56], medan nio medlemsstater mottog ett motiverat yttrande den 25 januari 2019[57].

Kommissionen förväntas rapportera om huruvida identifieringen av leverantörer av samhällsviktiga tjänster är konsekvent senast den 9 maj 2019. Utgående från medlemsstaternas anmälningar har det konstaterats att **direktivet om säkerhet i nätverks- och informationssystem**[58] har införlivats fullt ut i 25 medlemsstater och delvis i en medlemsstat[59]. I januari 2019 avslutade kommissionen överträdelseförfaranden för underlåtenhet att anmäla åtgärder mot sex medlemsstater[60]. Nio medlemsstater[61] är föremål för ett överträdelseförfarande för underlåtenhet att anmäla ett fullständigt införlivande av direktivet. Som ett led i införlivandet av direktivet om säkerhet i nätverks- och informationssystem var medlemsstaterna skyldiga att senast den 9 november 2018 lämna information till kommissionen om operatörer av samhällsviktiga tjänster som identifierats på

---

49 Direktiv (EU) 2017/853, 17.5.2017.

50 Danmark, Frankrike, Kroatien, Italien, Malta och Österrike (läget den 11 mars 2019).

51 Tjeckien, Estland, Litauen, Portugal och Förenade kungariket (läget den 11 mars 2019).

52 Belgien, Bulgarien, Tjeckien, Tyskland, Estland, Irland, Grekland, Spanien, Cypern, Lettland, Litauen, Luxemburg, Ungern, Nederländerna, Polen, Portugal, Rumänien, Slovenien, Slovakien, Finland, Sverige och Förenade kungariket (läget den 11 mars 2019).

53 Direktiv (EU) 2016/680, 27.4.2016.

54 Belgien, Bulgarien, Tjeckien, Estland, Grekland, Spanien, Frankrike, Kroatien, Cypern, Lettland, Litauen, Luxemburg, Ungern, Nederländerna, Polen, Portugal, Rumänien, Slovenien och Finland. Kommissionen har mottagit svar från medlemsstater, även anmälningar av berörd lagstiftning, och dessa håller som bäst på att analyseras (läget den 11 mars 2019).

55 Belgien, Tyskland, Estland, Irland, Frankrike, Kroatien, Italien, Litauen, Luxemburg, Ungern, Malta, Österrike, Polen, Rumänien, Slovakien, Sverige och Förenade kungariket har anmält fullständigt införlivande. Tjeckien, Portugal, Finland, Slovenien och Nederländerna har anmält delvis införlivande. Dessutom har Danmark slutfört införlivandet (läget den 11 mars 2019).

56 Belgien, Frankrike, Kroatien, Litauen, Luxemburg och Ungern (läget den 11 mars 2019).
Grekland, Cypern, Spanien, Slovenien, Portugal, Tjeckien, Bulgarien, Lettland och Nederländerna (läget den 11 mars 2019).

58 Direktiv (EU) 2016/1148, 27.4.2016.

59 Bulgarien, Tjeckien, Danmark, Tyskland, Grekland, Estland, Irland, Spanien, Frankrike, Kroatien, Italien, Cypern, Lettland, Litauen, Malta, Nederländerna, Österrike, Polen, Portugal, Rumänien, Slovenien, Slovakien, Finland, Sverige och Förenade kungariket har anmält fullständigt införlivande. Ungern har anmält delvis införlivande. Belgien och Luxemburg har inte anmält några nationella införlivandeåtgärder till kommissionen (läget den 11 mars 2019).

60 Irland, Spanien, Frankrike, Kroatien, Nederländerna och Portugal (läget den 11 mars 2019).

61 Bulgarien, Belgien, Danmark, Lettland, Litauen, Luxemburg, Ungern, Österrike och Rumänien (läget den 11 mars 2019).

deras territorium. Kommissionen håller nu på att utvärdera den information som medlemsstaterna lämnat[62].

Kommissionen håller dessutom på att bedöma införlivandet av det **fjärde penningtvättsdirektivet**[63], och arbetar samtidigt med att kontrollera att medlemsstaterna tillämpar reglerna. Kommissionen har inlett överträdelseförfaranden mot samtliga 28 medlemsstater eftersom den har bedömt att de meddelanden som mottagits från medlemsstaterna inte motsvarar ett fullständigt införlivande av direktivet[64]. Den kommer att fortsätta att använda sina befogenheter när det krävs för att säkerställa ett fullständigt genomförande av detta direktiv.

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** – tre medlemsstater måste ännu anmäla införlivande i den nationella lagstiftningen och två medlemsstater måste komplettera anmälan av införlivande[65].
- **Direktivet om säkerhet i nätverks- och informationssystem** – två medlemsstater måste ännu anmäla införlivande i den nationella lagstiftningen och en medlemsstat måste komplettera anmälan av införlivande[66].
- **Direktivet om bekämpande av terrorism** – tre medlemsstater måste ännu anmäla införlivande i den nationella lagstiftningen och fyra medlemsstater måste komplettera anmälan av införlivande[67].
- **Direktivet om kontroll av förvärv och innehav av vapen** – 17 medlemsstater måste ännu anmäla införlivande i den nationella lagstiftningen och fem medlemsstater måste komplettera anmälan av införlivande[68].
- **Dataskyddsdirektivet för brottsbekämpning** – fem medlemsstater måste ännu anmäla införlivande i den nationella lagstiftningen och fem medlemsstater måste komplettera anmälan av införlivande[69].

---

62 Bulgarien, Cypern, Tjeckien, Tyskland, Danmark, Estland, Spanien, Finland, Frankrike, Kroatien, Ungern, Irland, Italien, Litauen, Malta, Nederländerna, Polen, Portugal, Slovakien, Sverige och Förenade kungariket (läget den 11 mars 2019).

63 Direktiv (EU) 2015/849, 20.5.2015.

64 Kommissionen har inlett överträdelseförfaranden mot alla medlemsstater för att de inte har anmält nationell lagstiftning som fullt ut införlivar direktivet, eftersom kommissionen bedömde att vissa bestämmelser i direktivet inte har införlivats.

65 Spanien, Nederländerna och Finland har ännu inte meddelat införlivande. Tjeckien och Slovenien har meddelat delvis införlivande och ska ännu komplettera anmälan av införlivande (läget den 11 mars 2019). Hänvisningarna till fullständigt införlivande avser medlemsstaternas anmälningar och påverkar inte kommissionens kontroll av införlivandet.

66 Belgien och Luxemburg har ännu inte meddelat införlivande. Ungern har meddelat delvis införlivande och ska ännu komplettera anmälan av införlivande (läget den 11 mars 2019).

67 Grekland, Cypern och Luxemburg har ännu inte meddelat införlivande. Belgien, Polen, Rumänien och Slovenien har meddelat delvis införlivande och ska ännu komplettera anmälan av införlivande (läget den 11 mars 2019).

68 Belgien, Bulgarien, Tyskland, Irland, Grekland, Spanien, Cypern, Lettland, Luxemburg, Ungern, Nederländerna, Polen, Rumänien, Slovenien, Slovakien, Finland och Sverige har ännu inte meddelat införlivande. Tjeckien, Estland, Litauen, Portugal och Förenade kungariket har meddelat delvis införlivande och ska ännu komplettera anmälan av införlivande (läget den 11 mars 2019). Hänvisningarna till fullständigt införlivande avser medlemsstaternas anmälningar och påverkar inte kommissionens kontroll av införlivandet.

- Det **fjärde penningtvättsdirektivet** – en medlemsstat måste ännu komplettera anmälan av införlivande[70].

2. Skydda offentliga platser: rekommenderad god praxis

Som en del av det praktiska arbetet med att förbättra skyddet och motståndskraften mot terrorism fortsätter kommissionen att stödja medlemsstaterna och deras lokala myndigheter med att **skydda offentliga platser**. Arbetet följer handlingsplanen från oktober 2017 om att skydda offentliga platser[71] och fokuserar på att utveckla och samla vägledning och god praxis. I samarbete med myndigheter och privata operatörer av offentliga platser inom ramen för det så kallade operatörsforumet[72] har kommissionen identifierat exempel på god praxis för flera åtgärder som alla operatörer och myndigheter som är involverade i skyddet av offentliga platser kan vidta för att stärka säkerheten[73]. De utgör de grundläggande stegen för att vägleda det framtida arbetet inom alla berörda sektorer för att skydda offentliga platser (se rutan nedan).

God praxis för myndigheter och privata operatörer för att stärka säkerheten på offentliga platser

Bedömning och planering

- Fastställa och genomföra sårbarhetsanalyser för att identifiera potentiella sårbarheter mot externa eller interna angrepp.
- Utarbeta och genomföra en säkerhetsplan för anläggningen eller evenemanget, inklusive förberedelse-, nöd- och återställningsåtgärder, och identifiera lämpliga säkerhetsåtgärder för anläggningens eller evenemangets omgivning. Säkerhetsåtgärderna måste vara effektiva, diskreta, proportionerliga och skräddarsydda för olika miljöer, med beaktande av deras särdrag.
- Utse och utbilda en person som ansvarar för att samordna och genomföra åtgärderna i säkerhetsplanen.
- Utarbeta och genomföra en krishanteringsplan.

Medvetenhet och utbildning

69 Bulgarien, Grekland, Spanien, Cypern och Lettland har ännu inte meddelat införlivande. Tjeckien, Portugal, Nederländerna, Finland och Slovenien har meddelat delvis införlivande och ska ännu komplettera anmälan av införlivande (läget den 11 mars 2019).

70 Rumänien har hittills bara meddelat delvis införlivande och måste ännu komplettera anmälan. Alla övriga medlemsstater har anmält fullständigt införlivande. Enligt kommissionens bedömning finns det dock fortfarande vissa bestämmelser i direktivet som inte verkar ha införlivats fullständigt (läget den 11 mars 2019).

71 COM(2017) 612 final, 18.10.2017.

72 Det offentlig-privata operatörsforumet, som inrättades inom ramen för handlingsplanen från oktober 2017 om skyddet av offentliga platser, samlar medlemsstaternas beslutsfattare och operatörer från olika sektorer, bland annat massevenemang och underhållning, hotellnäringen, shoppingcentrum, idrotts- och kulturarenor och transportknutpunkter.

73 För mer information om god praxis, se arbetsdokumentet från kommissionens avdelningar *Good practices to support the protection of public spaces*, (SWD(2019) 140, 20.3.2019).

- Ta initiativ till informationskampanjer till allmänheten om att rapportera misstänkt beteende och om hur man ska agera i händelse av ett angrepp som äventyrar säkerheten för en anläggning eller ett evenemang.
- Utarbeta och genomföra ett internt program för säkerhetsmedvetenhet för alla anställda.
- Utarbeta och genomföra ett internt program för medvetenhet om insiderhot, som bidrar till att skydda anläggningar eller evenemang mot olika typer av interna hot, såsom sabotage, kommersiell stöld eller terroristattacker.
- Utarbeta grundläggande säkerhetsutbildningsprogram för alla anställda och genomföra särskilda säkerhetsutbildningar som ska bidra till att utveckla en säkerhetsmedveten företagskultur. Utarbeta åtgärder som motiverar de anställda att tillämpa en sund säkerhetspraxis och upprätthålla en hög grad av säkerhetsmedvetenhet.
- Genomföra regelbundna säkerhetsövningar som hjälper till att identifiera hur beredda man är att avskräcka och reagera på en attack.

Fysiskt skydd

- Ta frågor om säkerhet och fysiskt skydd i beaktande redan från början av utformningen av en ny anläggning eller ett nytt evenemang.
- Bedöma vilka tillträdeskontroller och hinder som behövs och undvika att skapa nya sårbarheter. Tillträdeskontrollerna och hindren bör inte överflytta riskerna någon annanstans och skapa nya mål.
- Bedöma den lämpligaste detektionstekniken för sprängämnen, skjutvapen och eggvapen samt kemiska, biologiska, radiologiska och nukleära ämnen.

Samarbete

- Utse kontaktpunkter och klargöra respektive roller och ansvarsområden i det offentlig-privata samarbetet kring säkerhetsfrågor (t.ex. mellan operatörer, privata säkerhetsorgan och brottsbekämpande myndigheter) och inför regelbunden kommunikation och regelbundet samarbete.
- Etablera tillförlitlig kommunikation och samverkan i god tid som möjliggör informationsutbyte om specifika risker och hot mellan ansvariga myndigheter, lokala brottsbekämpande myndigheter och den privata sektorn.
- Samordna arbetet med att skydda offentliga platser på lokal, regional och nationell nivå, och kommunicera och utbyta god praxis på alla nivåer, även på EU-nivå.
- Myndigheterna bör tillsammans med operatörerna utarbeta och tillhandahålla praktiska rekommendationer och riktlinjer om hur man upptäcker, hindrar och reagerar på säkerhetshot.

3. Sårbarhet hos digitala infrastrukturer

Digital resiliens är avgörande för att skydda den bredare statliga verksamheten, industriell forskning, immateriella rättigheter och verksamhetsplaner samt våra val, demokratiska institutioner och egna personuppgifter. En av de mest aktuella cybersäkerhetsfrågor som fått stor uppmärksamhet i den offentliga debatten runtom i EU rör 5G-nätverk. Vid det informella ministerrådet för telekommunikation i Bukarest den 1 mars 2019 uttryckte ministrarna sitt stöd för en samordnad europeisk strategi för att stärka den digitala resiliensen i EU vad gäller 5G-näten. 5G-nätverksinfrastrukturen är en viktig grund för den digitala ekonomin. Utöver konsumenttjänster är 5G-tekniken utformad och förväntas tillhandahålla tjänster av kritisk betydelse för vertikala sektorer, såsom rörlighet, energi och hälsa. 5G-nätverksstandarderna är globala och utrustningen kommer att erbjudas av ett antal internationella leverantörer.

Utbyggnaden av 5G-näten under de kommande åren innebär en radikal förändring jämfört med tidigare nätverk. Lagringen av uppgifter i molntjänster kommer att göra det möjligt att ansluta miljardtals enheter till sakernas internet, och driva nya innovationer inom artificiell intelligens, vilket öppnar möjligheter för privatpersoner och företag. Därför är cybersäkerheten särskilt viktig eftersom sårbarheter kan utnyttjas och potentiellt orsaka mycket allvarliga skador. Med tanke på att internet är gränslöst kan en säkerhetsöverträdelse i en medlemsstat påverka många andra.

För att skydda mot potentiella allvarliga konsekvenser för säkerheten för kritisk digital infrastruktur behövs det en gemensam EU-strategi för säkerheten i 5G-nät. För att sätta igång detta arbete kommer kommissionen efter Europeiska rådets möte den 21–22 mars att anta en rekommendation om en gemensam EU-strategi för säkerhetsrisker avseende 5G-nät, med utgångspunkt i en samordnad riskbedömning och riskhanteringsåtgärder på EU-nivå, en effektiv ram för samarbete och informationsutbyte och gemensam situationsmedvetenhet som omfattar kritiska kommunikationsnät. Diskussionen om möjliga åtgärder bör inbegripa införande av kvantteknik för nätsäkerhet och för skydd av lagrade uppgifter[74].

Den 12 mars 2019 antog Europaparlamentet en resolution om säkerhetshot i samband med den ökande kinesiska tekniska närvaron i EU och möjliga åtgärder på EU-nivå för att stävja dem.

4. Externa åtgärder

Förhandlingarna mellan EU och Kanada om ett **reviderat avtal om passageraruppgifter** är på god väg. Det kommande toppmötet mellan EU och Kanada i Montreal den 11–12 april skulle kunna ge förhandlingarna en knuff i rätt riktning.

Kommissionen förbereder tillsammans med de amerikanska myndigheterna en gemensam utvärdering av **avtalet mellan EU och Förenta staterna om passageraruppgifter**[75], i linje med bestämmelserna i avtalet mellan EU och USA om passageraruppgifter. Arbetet pågår redan med den femte gemensamma översynen av **avtalet om programmet för att spåra finansiering av terrorism mellan EU och Förenta staterna**[76]. Vid översynen kommer man att bedöma avtalets bestämmelser om skyddsåtgärder, kontroller och ömsesidighet samt programmets värde som ett verktyg för att bekämpa terrorism i både EU och Förenta staterna.

Den pågående utvecklingen på plats i Syrien har satt rampljuset på diskussionen om **utländska terroriststridande** som för närvarande befinner sig i eller är frihetsberövade i konfliktområden. EU kan ge stöd till medlemsstaterna på begäran, i synnerhet vad gäller informationsutbyte och stöd till brottsutredningar, framför allt samarbete med internationella partner och genom Europol, samt på grundval av den sakkunskap och bästa praxis om rehabilitering och återanpassning som utvecklats inom ramen för nätverket för kunskapsspridning om radikalisering. EU kan också tillhandahålla stöd för kapacitetsuppbyggnad i tredjeländer som är särskilt påverkade av återvändande utländska terroriststridande. Beslutet om huruvida man ska repatriera utländska terroriststridande och deras familjer från konfliktområden fattas av de berörda medlemsstaterna.

---

74 Se även meddelandet *Europeiskt initiativ för molnbaserade tjänster – Att skapa en konkurrenskraftig data- och kunskapsekonomi i Europa* (COM(2016) 178 final, 19.4.2016).

75 EUT L 215, 11.8.2012, s. 5.

76 EUT L 195, 27.7.2010, s. 5.

EU och Egypten ledde plenarmötet i arbetsgruppen för Östafrika inom **globala forumet för terroristbekämpning** i Nairobi den 20 februari 2019 med många deltagande från rättsväsendet och polisen i Somalia, Kenya, Sudan, Uganda, Djibouti, Etiopien, Jemen och Tanzania.

V. SLUTSATS

EU har gjort betydande framsteg i det gemensamma arbetet för en effektiv och verklig säkerhetsunion, och Europaparlamentet och rådet har antagit flera prioriterade lagstiftningsinitiativ under de senaste veckorna och månaderna. Det behövs dock mer arbete inför valet till Europaparlamentet i maj för att ta itu med brådskande säkerhetsbehov. I synnerhet uppmanar kommissionen medlagstiftarna att inleda förhandlingar om de föreslagna reglerna för att avlägsna terrorisminnehåll online så snart som Europaparlamentet har antagit sitt förhandlingsmandat, i syfte att nå en överenskommelse ännu under Europaparlamentets innevarande mandatperiod. Förhandlingarna om förslaget att stärka den europeiska gräns- och kustbevakningen har redan nått trepartsskedet, vilket visar att alla institutionerna är beslutna att anta detta förslag före valet till Europaparlamentet. Kommissionen uppmanar också medlemsstaterna att genomföra alla överenskomna åtgärder i säkerhetsunionen för att se till att de i full grad påverkar alla medborgares säkerhet.

Med tanke på att det är bråttom att se till att unionen är beredd innan de europeiska väljarna går till valurnorna i maj 2019 uppmanar kommissionen dessutom alla berörda aktörer att fördubbla sina ansträngningar för att stärka valrörelsernas motståndskraft mot desinformation. Inför Europeiska rådets möte den 21 och 22 mars 2019 måste medlemsstaterna utöka sin samordning och sitt informationsutbyte för att motverka desinformation och skydda valen mot andra cyberbaserade hot, genom att fullt ut utnyttja de verktyg som EU tillhandahåller för detta. Samtidigt måste onlineplattformarna påskynda sina insatser runtom i medlemsstaterna för att hjälpa till att garantera integriteten för valet till Europaparlamentet i maj. Kommissionen kommer att fortsätta att stödja och uppmuntra detta arbete under de närmaste veckorna och månaderna för att skydda integriteten för valet till Europaparlamentet.