EUROPEISKA
KOMMISSIONEN

Bryssel den 25.1.2017
COM(2017) 41 final

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET, EUROPEISKA RÅDET OCH RÅDET

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

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

I. INLEDNING

Detta är den fjärde månatliga rapporten om framsteg i riktning mot en effektiv och verklig säkerhetsunion och den omfattar utveckling 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.* Denna rapport är inriktad på fyra centrala områden, nämligen informationssystem och interoperabilitet, skydd av mjuka mål, it-hot och dataskydd i samband med brottsutredningar.

Attacken på julmarknaden i Berlin i december har på nytt satt fingret på allvarliga brister i vårt informationssystem som skyndsamt måste åtgärdas, i synnerhet på EU-nivå, för att hjälpa nationella myndigheter för gränskontroll och brottsbekämpning på plats att utföra sitt krävande arbete mer effektivt. Det faktum att de olika informationssystemen inte är sammankopplade – vilket gör det möjligt för förövare att använda flera identiteter för att förflytta sig utan upptäckt, inbegripet när de passerar gränserna – och att medlemsstaterna inte rutinmässigt matar in denna information i relevanta EU-databaser är praktiska brister i genomförandet som snabbt behöver åtgärdas. Mer arbete behövs också när det gäller brottsbekämpande åtgärder vid gränserna och återsändande av personer vars asylansökningar har avslagits[1].

I fråga om skydd av mjuka mål kommer kommissionen att påskynda sitt arbete för att samla experter från medlemsstaterna för att utbyta bästa praxis och enas om standardiserade riktlinjer.

Det it-hot som EU står inför får stor uppmärksamhet i medierna och i denna rapport behandlas de olika delar av arbetet på detta område som redan har påbörjats. Detta omfattar både förebyggande åtgärder – genom samarbete med branschen för att främja security by design och genomförande av direktivet om säkerhet i nätverks- och informationssystem – och främjande av samarbete mellan medlemsstaterna och med internationella organisationer och partner när det gäller att hantera it-attacker när de inträffar. Under de kommande månaderna kommer kommissionen och unionens höga representant för utrikes frågor och säkerhetspolitik att identifiera de åtgärder som krävs för en effektiv hantering av dessa hot på EU-nivå, baserat på 2013 års EU-strategi för cybersäkerhet.

Integritetsskydd och skydd av personuppgifter för enskilda är en viktig grundläggande rättighet och därmed en hörnsten i alla åtgärder i riktning mot en verklig säkerhetsunion. Direktivet om dataskydd för polisen och på det straffrättsliga området som antogs i april 2016 garanterar en gemensam hög standard för dataskydd och kommer därför att underlätta ett smidigt utbyte av relevanta data mellan medlemsstaternas brottsbekämpande myndigheter. Kommissionen har också inlett en översyn av direktivet om integritet och elektronisk kommunikation som en del av sitt datapaket för att utvidga direktivets tillämpningsområde till att omfatta alla leverantörer av elektronisk

[1] Kommissionen kommer att lägga fram en reviderad handlingsplan för återvändande under de kommande veckorna, se Rapport från kommissionen till Europaparlamentet, Europeiska rådet och rådet om det operativa genomförandet av den europeiska gräns- och kustbevakningen (COM(2017) 42).

kommunikation och anpassa bestämmelserna i det till den allmänna dataskyddsförordningen. Förslaget är utformat för att säkerställa integritet i elektronisk kommunikation samtidigt som de villkor fastställs enligt vilka begränsningar av tillämpningsområdet för förordningen om integritet och elektronisk kommunikation kan komma i fråga, inbegripet skäl förknippade med den nationella säkerheten eller brottsutredningar.

II. STÄRKA INFORMATIONSSYSTEM OCH INTEROPERABILITET

I Jean-Claude Junckers tal om tillståndet i unionen i september 2016 och i Europeiska rådets slutsatser av december 2016 påpekades vikten av att åtgärda bristerna avseende informationshantering och att förbättra **interoperabiliteten och sammankopplingen mellan befintliga informationssystem**. Händelserna på senare tid har återigen visat på det akuta behovet av att sammankoppla EU:s befintliga databaser, inte minst för att gränskontroll och brottsbekämpning på plats ska få de verktyg som behövs för att upptäcka identitetsbedrägeri. Exempelvis använde den som utförde terroristattacken i Berlin i december 2016 minst 14 olika identiteter och kunde färdas mellan medlemsstaterna utan att upptäckas. Det finns ett tydligt behov av att EU:s befintliga och framtida informationssystem ska vara simultant sökbara med hjälp av biometriska kännetecken så att denna väg kan stängas för terrorister och brottslingar.

I detta avseende satte kommissionen igång arbetet i april 2016 med sina förslag till ”starkare och smartare informationssystem för gränser och säkerhet”[2]. Där identifierades brister i de befintliga systemens funktioner, luckor i EU:s uppgiftshanteringsstruktur, problem med komplicerat landskap av informationssystem som administreras på olika sätt och en övergripande fragmentering på grund av att befintliga system utformats individuellt snarare än för att passa ihop. Som ett led i denna process inrättade kommissionen tillsammans med EU-organ, medlemsstater och berörda parter **högnivågruppen för informationssystem och interoperabilitet**. I en rapport från ordföranden av den 21 december 2016[3] presenteras gruppens **preliminära slutsatser** som omfattar det prioriterade alternativet att skapa en gemensam sökportal så att nationella myndigheter för gränskontroll och brottsbekämpning kan söka simultant i EU:s databaser och informationssystem. I den preliminära rapporten betonas också vikten av datakvalitet – informationssystemen är bara så effektiva som kvaliteten och formatet på de data som matas in i dem – och det rekommenderas att datakvaliteten i EU:s system förbättras genom automatiserad kvalitetskontroll.

Kommissionen kommer att snabbt följa upp alternativet att inrätta en gemensam sökportal och tillsammans med EU:s byrå för den operativa förvaltningen av stora it-system (eu-LISA) inleda sitt arbete med en portal där man kan söka parallellt i alla relevanta EU-system. En därmed sammanhängande studie bör vara färdig i juni och ligga till grund för utformning och provning av en prototyp för portalen före slutet av året. Kommissionen anser att Europol parallellt bör fortsätta sitt arbete med ett systemgränssnitt som gör det möjligt för medlemsstaternas tjänstemän i frontlinjen att, när de konsulterar sina egna nationella system, samtidigt automatiskt konsultera Europols databaser.

[2] Meddelandet *Starkare och smartare informationssystem för gränser och säkerhet*, COM(2016) 205 final.

[3] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=28994&no=1

Arbetet för interoperabilitet mellan informationssystem syftar till att åtgärda den nuvarande fragmenteringen av EU:s uppgiftshanteringsstruktur för gränskontroll och säkerhet samt relaterade brister. När databaser använder ett gemensamt centrallager för databaser med personuppgifter – vilket är tanken för EU:s föreslagna in- och utresesystem och det föreslagna EU-systemet för reseuppgifter och resetillstånd (Etias) – kan en person endast registreras under en enda identitet i de olika databaserna, vilket hindrar användningen av olika falska identiteter. Kommissionen har, vilket föreslås i högnivågruppens preliminära slutsatser som ett första steg, uppmanat eu-LISA att utreda de tekniska och operativa aspekterna av införandet av en gemensam tjänst för biometrisk matchning. En sådan tjänst skulle möjliggöra sökningar i olika databaser med biometriska uppgifter, vilket skulle kunna avslöja falska identiteter som används av personen i fråga i ett annat system. Dessutom bör högnivågruppen nu bedöma huruvida det är nödvändigt, tekniskt genomförbart och proportionellt att utvidga det **gemensamma centrallagret för databaser med personuppgifter** som planeras för in- och utresesystemet och Etias till andra system. Utöver de biometriska uppgifter som finns lagrade i tjänsten för biometrisk matchning skulle ett sådant gemensamt centrallager också innehålla alfanumeriska personuppgifter. Gruppen bör lägga fram sina slutsatser om detta i sin slutrapport senast i slutet av april 2017.

Den senaste tidens säkerhetsrelaterade händelser understryker behovet av att ompröva frågan om **obligatoriskt utbyte av information** mellan medlemsstaterna. Kommissionens förslag från december 2016 om att stärka **Schengens informationssystem** innehåller – för första gången – en skyldighet för medlemsstaterna att utfärda varningar om personer med anknytning till terroristbrott. Det är viktigt att medlagstiftarna nu verkar för ett snabbt antagande av de föreslagna åtgärderna. Kommissionen är redo att undersöka om en tvingande skyldighet för informationsutbyte bör införas för andra EU-databaser.

III. SKYDDA VÅRA MJUKA MÅL MOT TERRORISTATTACKER

Attacken i Berlin var den senaste i EU mot så kallade mjuka mål, som vanligen är civila platser där människor samlas i stora grupper (t.ex. offentliga platser, sjukhus, skolor, idrottsarenor, kulturcentrum, kaféer och restauranger, köpcentrum och transportnav). Dessa platser är av sin natur sårbara och svåra att skydda, och kännetecknas också av hög sannolikhet för ett stort antal offer i händelse av en attack. De är därför mål som terrorister föredrar. Hotet om framtida angrepp mot mjuka mål, inklusive transporter, är fortfarande starkt, vilket bekräftas av tillgängliga bedömningar, bland annat Europols rapport om förändringar i Isils arbetssätt[4].

I den europeiska säkerhetsagendan från 2015 och i 2016 års meddelande om en säkerhetsunion betonas behovet av att intensifiera arbetet för att förbättra säkerheten och att använda innovativ utrustning och teknik för detektering i skyddet av mjuka mål. Kommissionen har arbetat för att stödja och uppmuntra utbyte av bästa praxis mellan medlemsstaterna när det gäller att utveckla bättre verktyg för att förebygga och reagera på angrepp mot mjuka mål. Detta arbete har mynnat ut i operativa handböcker och

[4] Europol, *Changes in modus operandi of Islamic State (IS) revisited*, november 2016 – offentlig information från Europol: https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited

vägledningar. Kommissionen håller för närvarande på att, i nära samarbete med medlemsstaternas experter, utveckla en omfattande manual om säkerhetsförfaranden och säkerhetsmallar för olika mjuka mål (t.ex. gallerior, sjukhus samt idrotts- och kulturevenemang). Syftet är att tillhandahålla medlemsstaterna en guide om skydd av mjuka mål i början av 2017, på grundval av bästa praxis i medlemsstaterna.

I februari kommer kommissionen samtidigt att sammankalla till det första seminariet med nationella myndigheter om skydd av mjuka mål, i syfte att utbyta information och utveckla bästa praxis om den komplicerade frågan om skydd av mjuka mål och allmänhetens säkerhet. Kommissionen finansierar också ett pilotprojekt som Belgien, Nederländerna och Luxemburg driver inom ramen för Fonden för inre säkerhet i syfte att inrätta ett regionalt kompetenscentrum för särskilda brottsbekämpande insatser, som kommer att erbjuda fortbildning för poliser, vilka ofta är de som är först på plats i händelse av en attack.

Att reagera på angrepp mot mjuka mål är en viktig del av kommissionens arbete med civilskydd. I december tillkännagav kommissionen de åtgärder som man har för avsikt att vidta med medlemsstaterna i syfte att skydda EU:s medborgare och minska sårbarheten i de omedelbara efterdyningarna av terroristattacker. Dessa åtgärder kommer att stärka samordningen mellan alla aktörer som arbetar med att hantera konsekvenserna av attacker, och kommissionen har åtagit sig att stödja medlemsstaternas insatser genom att underlätta gemensamma utbildningar och övningar samt genom att säkerställa en fortlöpande dialog via befintliga kontaktpunkter och expertgrupper. Kommissionen kommer också att stödja utvecklingen av specialiserade moduler för att reagera på terroristattacker inom ramen för unionens civilskyddsmekanism och initiativ för att dela erfarenheter och öka medvetenheten hos allmänheten.

Tillsammans med medlemsstaterna kommer kommissionen även att undersöka vilka EU-stöd som skulle kunna tas i anspråk för att bidra till att bygga upp motståndskraft och stärka säkerheten kring potentiella mjuka mål. Medlemsstaterna skulle också kunna ansöka om finansiering från Europeiska investeringsbanken (EIB) (inbegripet Europeiska fonden för strategiska investeringar), i linje med EU:s och EIB-gruppens riktlinjer. Varje projekt skulle bli föremål för de normala beslutsförfaranden som fastställs i lagstiftningen.

När det gäller specifika mjuka mål förknippade med offentliga platser i samband med transporter, t.ex. de delar av flygplatser eller järnvägsstationer som är öppna för allmänheten, framhölls vid det särskilda seminarium med många olika intressenter som kommissionen anordnade i november 2016 behovet av att bibehålla balans mellan säkerhetsbehov, passagerarnas bekvämlighet och transportverksamhet. I slutsatserna framhålls betydelsen av att bygga upp en säkerhetskultur som inte bara omfattar personal utan också passagerare, vikten av lokala riskbedömningar som en grund för att fastställa lämpliga motåtgärder och behovet av att förbättra kommunikationen mellan alla berörda parter.

IV. HANTERA IT-HOTEN

It-brottslighet och it-angrepp är stora utmaningar som unionen står inför, och där åtgärder på EU-nivå kan bidra till att stärka vår gemensamma motståndskraft. It-säkerhetsincidenter får varje dag allvarliga negativa konsekvenser i människors liv och orsakar stora ekonomiska skador för ekonomin och företagen i Europa. It-attacker är en

av de viktigaste delarna av hybridhoten – om de utförs exakt samtidigt som fysiska hot, till exempel i samband med terrorism, kan de ha förödande verkan. De kan också bidra till att destabilisera ett land eller utmana politiska institutioner och grundläggande demokratiska processer. Eftersom vi i allt större utsträckning förlitar oss på online-teknik kommer vår kritiska infrastruktur (från sjukhus till kärnkraftverk) att bli allt mer sårbar.

EU-strategin för cybersäkerhet från 2013 utgör en del av de viktigaste strategiska åtgärderna inför utmaningarna på området för it-säkerhet. Den centrala åtgärden är direktivet om nät- och informationssäkerhet[5] som antogs i juli. Det ligger till grund för bättre samarbete på EU-nivå och motståndskraft mot it-angrepp och it-incidenter genom stöd till samarbete och utbyte av information mellan medlemsstaterna och genom främjande av operativt samarbete i samband med specifika it-incidenter och utbyte av information om risker. För att säkerställa ett enhetligt genomförande inom olika sektorer och över gränserna kommer kommissionen att hålla det första sammanträdet för samarbetsgruppen för nät- och informationssäkerhet med medlemsstaterna i februari.

I april 2016 antog kommissionen och EU:s höga representant en gemensam ram för att motverka hybridhot[6] där 22 åtgärder föreslås för att öka medvetenheten, stärka resiliensen, hantera kriser bättre och öka samarbetet mellan EU och Nato. I enlighet med uppmaningen från rådet kommer kommissionen och den höga representanten att senast i juli 2017 lägga fram en rapport för att bedöma framstegen.

Kommissionen främjar och stöder även teknisk innovation, bl.a. med hjälp av EU:s forskningsmedel, för att driva fram nya lösningar och skapa ny teknik som kan bidra till att stärka vår motståndskraft mot it-angrepp (t.ex. ”security by design”). Förra sommaren lanserade vi ett offentligt-privat partnerskap om it-säkerhet med branschen, värt 1,8 miljarder euro[7].

Inom transportsektorn håller digitaliseringen på att bli en viktig faktor för den nödvändiga omvandlingen av dagens transportsystem. Den snabba digitaliseringen skapar många fördelar, men bidrar också till att göra transporterna mer sårbara för it-säkerhetsrisker. Många åtgärder vidtas för att minska hotet på olika nivåer, särskilt för luftfart men också för transporter till sjöss, på inre vattenvägar, järnväg och på väg[8]. Den återstående utmaningen är att ytterligare klargöra, harmonisera och komplettera den verksamhet som bedrivs av olika aktörer som deltar i arbetet med att förbättra motståndskraften mot it-angrepp och it-incidenter på olika sätt.

Mer allmänt, och med tanke på den snabba utvecklingen av hotet, kommer kommissionen och EU:s höga representant under de kommande månaderna att kartlägga

---

5 Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

6 JOIN(2016) 18.

7 Enligt meddelandet om cyberresiliens från 2016, COM(2016) 410 final.

8 Som exempel kan nämnas internationella riktlinjer, t.ex. de som har tagits fram av Internationella sjöfartsorganisationen eller genom en resolution som Icao nyligen antagit, på EU:s och Förenta staternas gemensamma initiativ; rapportering av händelser där ett mer reaktivt sätt för närvarande utvecklas av Europeiska byrån för luftfartssäkerhet, och security by design på it-området, som är tillämpligt på nya system under utveckling, t.ex. det gemensamma företaget Sesars generalplan för flygledningstjänst.

vilka åtgärder som krävs för att effektivt hantera dessa hot på EU-nivå, på grundval av 2013 års EU-strategi för cybersäkerhet.

V. SKYDDA PERSONUPPGIFTER OCH SAMTIDIGT FRÄMJA EFFEKTIVA BROTTSUTREDNINGAR

Direktivet om dataskydd för polisen och på det straffrättsliga området[9] är en byggsten i kampen mot terrorism och grov brottslighet. På grundval av en gemensam standard för dataskydd som fastställs i direktivet kommer medlemsstaternas brottsbekämpande myndigheter att kunna utbyta relevanta uppgifter på ett smidigt sätt, medan uppgifter om offer, vittnen och misstänkta för brott ges vederbörligt skydd.

För att säkerställa en hög konfidentialitetsnivå vid kommunikation för både enskilda och företag och lika villkor för alla aktörer på marknaden, enligt vad som anges i strategin för den digitala inre marknaden från april 2015, antog kommissionen förslaget till **förordning om integritet och elektronisk kommunikation** (som ersätter direktiv 2002/58/EG) den 11 januari[10]. I likhet med det nuvarande direktivet preciserar den reviderade förordningen om integritet och elektronisk kommunikation den allmänna dataskyddsförordningen[11] och fastställer en ram för skyddet av personlig integritet och personuppgifter inom sektorn för elektronisk kommunikation.

Genom denna översyn ska all data för elektronisk kommunikation, även när kommunikationen är underordnad, betraktas som confidential/restricted – oavsett om den går via traditionella telekommunikationstjänster eller andra s.k. over-the-top-tjänster som är funktionellt likvärdiga (t.ex. Skype och WhatsApp) och för många användare utbytbara i förhållande till vanliga teleoperatörer[12]. Skyldigheterna för tjänsteleverantörerna – utöver att respektera sina kunders integritetsval vid användning, lagring och behandling av deras uppgifter – inbegriper även skyldigheten för tjänsteleverantörer baserade utanför EU att utse en företrädare i en medlemsstat. Detta kommer också att ge medlemsstaterna möjlighet att underlätta för de brottsbekämpande och rättsliga myndigheterna att samarbeta med tjänsteleverantörerna för att få tillgång till elektroniska bevis (se nedan).

Precis som enligt de nuvarande reglerna om integritet och elektronisk kommunikation kommer brottsbekämpande och rättsliga myndigheters tillgång till relevant elektronisk

---

9 Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF. Direktivet trädde i kraft den 5 maj 2016 och ska införlivas av medlemsstaterna senast den 6 maj 2018. Kommissionen har inrättat en expertgrupp med medlemsstaterna för att utbyta åsikter om införlivandet av polisdirektivet.

10 Förordning om integritet och elektronisk kommunikation, COM(2017) 10.

11 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), som ska tillämpas från och med den 25 maj 2018.

12 Detta ligger i linje med strategin i förslaget till direktiv om inrättande av en europeisk kodex för elektronisk kommunikation som kommissionen lade fram den 14 september 2016 (telekompaketet), COM(2016) 590 final.

information som behövs för att utreda brott att omfattas av undantaget i artikel 11 i den föreslagna förordningen om integritet och elektronisk kommunikation[13]. Denna bestämmelse ger möjlighet att i unionsrätten eller i nationell rätt begränsa konfidentialiteten vid kommunikation, där så är nödvändigt och proportionellt, för att skydda nationell säkerhet, försvar eller allmän säkerhet samt förebyggande, förhindrande, utredning, avslöjande och lagföring av brott eller verkställande av straffrättsliga påföljder. Denna bestämmelse är särskilt relevant för de nationella bestämmelserna om **datalagring**, dvs. för att göra det obligatoriskt för teletjänstföretag att lagra kommunikationsuppgifter under en bestämd tid för brottsbekämpande myndigheters eventuella åtkomst, till följd av domstolens ogiltigförklaring av datalagringsdirektivet 2014[14]. Sedan dess har det inte funnits något EU-instrument för datalagring och vissa medlemsstater har antagit egna nationella lagar om datalagring. De svenska och brittiska lagarna om datalagring anmäldes till domstolen, som avkunnade sin dom i fallet *Tele2*den 21 december[15]. Domstolen fann att nationell lagstiftning som i brottsbekämpande syfte föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter avseende abonnenter och användare avseende samtliga elektroniska kommunikationsmedel strider mot unionsrätten. Avgörandets konsekvenser håller på att analyseras och kommissionen kommer att ta fram riktlinjer för hur nationella lagar om datalagring kan utformas i överensstämmelse med avgörandet.

Brott lämnar digitala spår som kan användas som bevis i domstol; elektronisk kommunikation mellan misstänkta personer ofta är de enda spår som brottsbekämpande myndigheter och åklagare kan fånga upp. Att få tillgång till **elektroniska bevis** – i synnerhet om de lagras i utlandet eller i ett moln – kan vara både tekniskt och juridiskt komplicerat och ofta innebära besvärliga förfaranden, vilket hindrar utredarnas möjligheter att agera snabbt. För att ta itu med dessa svårigheter håller kommissionen för närvarande på att utvärdera lösningar för att utredarna ska kunna få tillgång till gränsöverskridande elektroniska bevis, bland annat genom att göra den ömsesidiga rättsliga hjälpen effektivare, hitta vägar för direkt samarbete med internetleverantörer, och föreslå kriterier för fastställande av jurisdiktion och för verkställande jurisdiktion i cyberrymden, i full överensstämmelse med tillämpliga regler för dataskydd.[16] Kommissionen rapporterade till rådet (rättsliga och inrikes frågor) den 9 december 2016 om vilka framsteg som gjorts[17].

En omfattande (fortfarande pågående) process med expertrådgivning har gjort det möjligt för kommissionen att definiera de olika ofta komplicerade problem som uppkommer i samband med åtkomsten till elektroniska bevis, bättre förstå nuvarande regler och praxis

---

[13] Se klausulen om datalagring i artikel 11.1, som förblir oförändrad i förhållande till artikel 15 i direktivet om integritet och elektronisk kommunikation och anpassas till kraven i den allmänna dataskyddsförordningen. Sådana restriktioner måste respektera det väsentliga innehållet i de grundläggande rättigheterna och vara nödvändiga, lämpliga och proportionerliga.

[14] Domstolens dom av den 8 april 2014 i de förenade målen C-293/12 och C-594/12, *Digital Rights Ireland*.

[15] Domstolens dom av den 21 december 2016 i de förenade målen C−203/15 och C−698/15, *Tele2*.

[16] Enligt de åtaganden som gjorts i den europeiska säkerhetsagendan, COM(2015) 185 final, och kommissionens meddelande om att genomföra den europeiska säkerhetsagendan mot terrorism och bana väg för en säkerhetsunion, COM(2016) 230 final.

[17] I sina slutsatser om förbättrad straffrätt i cyberrymden av den 9 juni 2016 uppmanade rådet kommissionen att vidta konkreta åtgärder, utveckla ett gemensamt tillvägagångssätt inom EU och lägga fram resultaten senast i juni 2017.

i medlemsstaterna, och kartlägga möjliga strategiska alternativ. Lägesrapporten innehåller en översikt över idéer som kommit fram hittills under processen med insamling av information och samråd med experter, och som kommissionen, i samråd med berörda parter, nu kommer att undersöka ytterligare under de kommande månaderna. Som aviserats i kommissionens arbetsprogram avser kommissionen att lägga fram ett initiativ under 2017.

VI. SLUTSATS

Nästa rapport, som ska läggas fram den 1 mars, blir ett tillfälle att se över vilka framsteg som gjorts med genomförandet av dessa och andra viktiga delar av arbetet.