



Bryssel den 22 november 2019
(OR. en)

14297/19

LIMITE

COSI 239
ENFOPOL 508
ENFOCUSTOM 196
FRONT 333
DAPIX 346
CYBER 322
JAI 1217

NOT

från:	Ordförandeskapet
till:	Ständiga representanternas kommitté (Coreper)/rådet
Ärende:	Den framtida riktningen för EU:s inre säkerhet – resultatet av diskussionerna – Rapport från ordförandeskapet

Det snabbt föränderliga säkerhetsläget förutsätter en integrerad strategi för hanteringen av nya hot och utmaningar. En övergripande strategi för inre säkerhet gör det möjligt att ta itu med hot som är mer komplexa och varierande än tidigare och hantera lösningar på ett samhällsomfattande sätt.

Under genomförandet av den strategiska agendan 2019–2024 på området rättsliga och inrikes frågor har ordförandeskapet anordnat en rad tematiska diskussioner för att fördjupa reflektionerna kring den framtida riktningen för EU:s inre säkerhet. Ordförandeskapet har fastställt tre grundprinciper som vägledning för reflektionerna: ge medborgarna ett område med frihet, säkerhet och rättvisa, bekämpa social utestängning och diskriminering samt främja unionens värden.

Diskussionerna inleddes i juli 2019 vid det informella mötet i ständiga kommittén för operativt samarbete i frågor som rör den inre säkerheten, som förberedelse inför det informella mötet i rådet (rättsliga och inrikes frågor), genom att man tog upp ett antal viktiga övergripande frågor¹.

Tematiska diskussioner ägde också rum i berörda arbetsgrupper, som arbetsgruppen för brottsbekämpning, arbetsgruppen mot terrorism och arbetsgruppen för informationsutbyte, och förbereddes vidare i ständiga kommittén för operativt samarbete i frågor som rör den inre säkerheten inför ministerdebatten. Ett antal frågor diskuterades ingående, t.ex. hur ramen för det operativa samarbetet inom brottsbekämpning kan förbättras, hur ny teknik och hybridhot påverkar den inre säkerheten, vilken roll EU:s RIF-myndigheter spelar, liksom informationshantering och automatisering samt utbildning för brottsbekämpande myndigheter. I de diskussionsdokument som framställdes inför de olika mötena redogörs ingående för de olika diskussionernas inriktning. Dokumenten förtecknas i bilagan till denna rapport.

Denna rapport täcker vissa utvalda aspekter och återspeglar ordförandeskapets syn på de centrala frågor som debatterna ledde fram till och som man ska fortsätta arbeta med under lagstiftningscykeln 2019–2024.

1. Ett proaktivt förhållningssätt till ny teknik

Den tekniska utvecklingen har en betydande inverkan på EU-medborgarnas liv och följaktligen också på det brottsförebyggande arbetet. Artificiell intelligens, obemannade luftfartyg, nya kommunikationsnätverk och onlinemiljöer är bara några exempel på denna utveckling, som kan vara ett stöd för myndigheternas arbete, men också användas i kriminella syften. Till exempel kan både brottsbekämpande myndigheter och beredskapspersonal använda drönare – i arbetet med att motverka terrorism respektive i efterdyningarna av en terrorattack. Den allt snabbare innovationstakten gör det svårt för de brottsbekämpande myndigheterna att anpassa sig till den tekniska verkligheten, som utvecklas snabbt. När det gäller digitalisering behöver man bedöma om de rättsliga ramarna som gäller för brottsbekämpande myndigheter och relevanta EU-organs verksamhet överensstämmer med dagens behov². All sådan utveckling bör utgå från målet att bevara och främja grundläggande rättigheter, samtidigt som de stränga kraven på verkställighetsåtgärder som följer av dataskyddsramen respekteras. Unionen har en ledande ställning när det gäller fastställande av standarder på dataskyddsområdet.

¹ Dokument från ordförandeskapet om den framtida riktningen för inre säkerhet i EU (WK 13264/19).

² Dok. 12496/19 och 12224/19, ny teknik och inre säkerhet

Målet är att EU:s brottsbekämpande myndigheter ska spela en proaktiv roll och kunna utnyttja fördelarna med den nya tekniken och samtidigt kunna förutse och kontrollera de relaterade riskerna. Det behövs en integrerad, övergripande strategi på EU-nivå på detta område. Denna målsättning understöds av inrättandet av ett gemensamt innovationslabb med Europol för att dra nytta av teknisk utveckling och tendenser samt innovation och forskning och bedöma den eventuella relevansen för brottsbekämpningen och dialogen med industrin och den akademiska världen. För att fullständigt kunna utnyttja den nya tekniken krävs kontinuerlig forskning och utbildning. Att centralisera viss verksamhet och inom innovationslabbet samla resultatet av de befintliga nätverkens arbete skulle medföra rationalisering och kostnadseffektivitet, särskilt på områden där medlemsstaterna inte har tillräckliga resurser för att kunna agera på egen hand eller där det finns ett mervärde i att agera tillsammans och utbyta bästa praxis.

Eftersom teknisk forskning och utveckling ofta sker vid universitet och inom den privata sektorn kommer de brottsbekämpande myndigheterna in i bilden i ett relativt sent skede. För att bemöta de brottsbekämpande myndigheternas farhågor inför framtiden anser ordförandeskapet att man bör försöka involvera dem på ett proaktivt sätt redan i början av den tekniska utvecklingsprocessen. Detta kan ske genom ökat deltagande och bättre samordning av rättstillämpare i EU-finansierade forsknings- och utvecklingsprogram för säkerhet.

Ordförandeskapet uppmanar brottsbekämpande myndigheter att delta på ett proaktivt sätt i utvecklingen av ny teknik. Innovationslabbet bör fungera som ett forum till stöd för detta mål. Det är viktigt att de brottsbekämpande myndigheternas behov är kända och beaktas i ett tidigt skede vid utvecklingen av ny teknik som påverkar deras arbete eller som krävs för effektivare brottsbekämpande insatser. Dessutom bör man i lagstiftning om ny teknik i ökad utsträckning beakta intressen rörande inre säkerhet och brottsbekämpning för att minska begränsningarna i den rättsliga ramen, särskilt genom att systematiskt behandla dessa intressen i hotbedömningar.

2. Effektiv informationshantering

Samarbetet inom brottsbekämpning på EU-nivå kommer i allt större utsträckning att baseras på bättre och effektivare tekniska lösningar och informationssystem och på interoperabilitet mellan dessa³. De stora mängder digitala data som utmärker dagens samhälle gör att de brottsbekämpande myndigheterna har tillgång till mer data och information än någonsin tidigare. De tekniska lösningar och den kapacitet som erbjuds måste återspegla detta. Samtidigt saknas viktig statistik om olika brottsområden. Därför är det extra viktigt att säkerställa att informationssystemen matas med fullständiga data av hög kvalitet och att de används på ett effektivt sätt. Vi måste säkerställa att relevanta nationella myndigheter har tillgång till dessa system och har den utbildning som krävs för att kunna utnyttja dem fullt ut.

Brottsbekämpningens grund är fortfarande den kriminalrättsliga analysen. Analysen ger mervärde till rådatan och omvandlar den till information som kan utgöra underlag för åtgärder och användas både nationellt och i gränsöverskridande insatser över hela EU. Emellertid behövs det en tydlig idé om standarder på EU-nivå för detta analysarbete, eftersom en sådan saknas i nuläget. I alla händelser är analysen en komponent som ingår i alla informationsprocesser inom brottsbekämpningen. Därför krävs tillräckliga mänskliga och ekonomiska resurser för att kunna hantera och analysera information. För att analysarbetet ska kunna förbättras och standardiseras krävs ökad kunskap om vilka generella behov som finns inom brottsbekämpningen och framför allt om de olika informationsprocesser som omfattas, inbegripet brottsutredning och insamling av kriminalunderrättelser.

Förordningarna om interoperabilitet⁴ trädde i kraft den 11 juni 2019. Det är av avgörande betydelse att förordningarna genomförs på ett effektivt sätt. Den tekniska revolution som EU:s it-system genomgår kommer att kräva stora resurser och respekt av tidsplanen, både på EU-nivå och i medlemsstaterna. Det är viktigt att man vid utvecklingen av interoperabilitetsarkitekturen ser till att de tekniska lösningarna alltid tar hänsyn till slutanvändarnas behov. Dessutom är det av avgörande vikt att slutanvändarna får lämplig och kontinuerlig utbildning så att de kan använda de nya informationssystemen och göra dem helt interoperabla. Det står klart att interoperabilitet är mycket mer än utveckling av it-system – det handlar om ett nytt perspektiv. Därför kräver ett lyckat genomförande också en förändring av våra operativa och administrativa kulturer.

³ Dok. 13510/19 *EU Information management – automation, access to, exchange of, and analysis of information.*

⁴ (EU) 2019/817 och (EU) 2019/818.

På en mer övergripande nivå handlar ett förbättrat informationsutbyte inte bara om teknisk utveckling. För att man ska kunna uppnå de önskade fördelarna måste det säkerställas att kompetenser, resurser och användargränssnitt på nationell nivå är ändamålsenliga. Information är inte ett absolut värde; informationen måste kunna användas och leda till åtgärder. Om genomförandet inte görs på rätt sätt kan denna utveckling och dess fördelar äventyras.

Utöver effektiva utredningar bör de brottsbekämpande myndigheternas arbete i lika hög grad inriktas på att förebygga och förhindra brott. Information av hög kvalitet på rätt plats och i rätt tid bidrar till detta mål. När det gäller underrättelsestyrd brottsbekämpning är Europol och Frontex väl lämpade att stödja detta arbete med sin analytiska kapacitet, bland annat genom en utökad tillgång till Schengens informationssystem (SIS), så länge som medlemsstaterna systematiskt förser dem med rådata av hög kvalitet.

Ordförandeskapet efterlyser en övergripande EU-ram för informationshantering, så att det kan säkerställas att all nödvändig befintlig information är tillgänglig och kan bearbetas och delas snabbt och effektivt och därmed leda till åtgärder på ett underrättelsestyrt sätt.

3. Sektorsövergripande gränsöverskridande samarbete

En förstärkning av det sektorsövergripande operativa samarbetet, genom reducering av dubbelarbete och en effektivare samordning, är nyckeln till framgångsrika insatser. Mot bakgrund av den ständigt föränderliga och sektorsövergripande karaktären hos olika säkerhetshot, såsom kemiska, biologiska, radiologiska och nukleära vapen och hybridverksamhet, krävs en övergripande strategi för de åtgärder som vidtas för att bemöta och förhindra denna verksamhet, samtidigt som medlemsstaternas behörighet i frågor som rör den nationella säkerheten beaktas. Det finns ett behov av en integrerad och enhetlig strategi för att säkerställa sektorsövergripande operativt samarbete som sträcker sig längre än det gränsöverskridande brottsbekämpningssamarbetet och som därmed även inbegriper andra myndigheter, t.ex. civilskyddsaktörer.

Skillnader i nationella beslutsprocesser, lagstiftning och operativa modeller är stora utmaningar för det gränsöverskridande operativa samarbetet. Bristande överensstämmelse mellan nationell praxis för insamling och behandling av uppgifter, som beror på skillnader mellan enskilda medlemsstater när det gäller administrativa system, tekniska lösningar och funktionella arrangemang, hindrar det gränsöverskridande samarbetet. En annan utmaning är identifieringen och undanröjandet av hinder för det operativa samarbetet mellan brottsbekämpande myndigheter, t.ex. inkompatibla radiofrekvenser i gränsområden, språkliga hinder och behovet av att komplettera befintliga rättsliga grunder med mer detaljerade bilaterala avtal. I akuta situationer är det möjligt att nationella enheter inte är medvetna om de operativa alternativ som finns, och som är uppdelade i flera olika EU-instrument, och de tillgängliga kanalerna för informationsutbyte.

Det sektorsövergripande operativa samarbetet mellan brottsbekämpande myndigheter bör intensifieras genom att man utvecklar och använder nya metoder för samarbete och informationsutbyte, med hjälp av nya tekniska tillämpningar och verktyg. Dessa tillämpningar kan t.ex. omfatta obemannade autonoma system, teknik för automatisk avläsning av registreringsskyltar eller gränssnitt för gemensam sökning i tillgängliga databaser. Det finns en tydlig drivkraft och en möjlighet att fortsätta och ytterligare stödja denna utveckling.

Livslångt lärande är ännu viktigare när det gäller att utnyttja alla befintliga möjligheter och förbereda sig inför framtiden. Den utbildning som tillhandahålls av EU-organen måste användas på ett effektivt sätt. Samtidigt måste man se till att EU-organens verksamheter kompletterar varandra och att man undanröjer överlappningar.

Vi måste ta hänsyn till regionala skillnader och nationella särdrag, samtidigt som vi strävar efter en gemensam brottsbekämpningskultur bland EU:s brottsbekämpande myndigheter. Bättre språkkunskaper, kunskap om varandras kulturer och utbyte av bästa praxis bidrar till en bättre förståelse av regionala och kulturella skillnader och stöder det gemensamma målet.

Bilaterala och multilaterala överenskommelser förblir viktiga för lokalt och regionalt samarbete och flexibilitet krävs för att säkerställa respekt för regional mångfald och olika operativa intressen. I all framtida utveckling måste man beakta uppdelningen av ansvarsområden, jurisdiktion och suveränitet.

EU:s RIF-myndigheter fortsätter att spela en viktig roll när det gäller att stödja medlemsstaternas insatser inom sina respektive mandat. Det är allmänt accepterat att ett verkligt gränsöverskridande samarbete mellan medlemsstaternas myndigheter, med starkt stöd från relevanta EU-organ, är det mest gångbara sättet att gå vidare mot en säkerhetsunion och att hantera både befintliga och nya hot i en ständigt föränderlig miljö på ett hållbart sätt.⁵

Den framtida utvecklingen på området för inre säkerhet skulle därför kräva att byråerna har en fortsatt aktiv roll, med bland annat en förväntad ökning i antal för befintliga uppgifter samt nya ansvarsområden som härrör från både politiska och operativa behov. Med tanke på de begränsade resurserna finns det ett behov av att diskutera i vilket sammanhang byråerna kan skapa mervärde mest effektivt, t.ex. områden där medlemsstaterna kan behöva få tillgång till resurser eller teknisk utrustning genom sammanslagning av resurser, där kapaciteten för dataanalys skulle kunna förbättras och där ett starkare operativt stöd kan tillhandahållas. Det bör fastställas tydliga kriterier för beslut om de områden där medlemsstaterna behöver mest stöd, med beaktande av tekniska framsteg och specifika behov av material eller andra resurser. Vid utvecklingen av organens roll bör målet vara en balanserad lösning som tar hänsyn till medlemsstaternas behov. Det är mycket viktigt att tillämpa ett samordnat och holistiskt synsätt i syfte att stärka varje organs kärnkompetens och starka sidor och skapa mervärde på ett kostnadseffektivt sätt och utan att det uppstår överlappningar i fråga om uppgifter och funktioner.

Det finns ett behov av ett fördjupat informationsutbyte och samarbete mellan organen eftersom de befintliga och framväxande hoten mot den inre säkerheten blir allt mer komplexa och gränsöverskridande till sin natur. Det finns också ett behov av effektivare samverkan med privata parter när det gäller informationsutbyte. Det finns i synnerhet ett behov av att utvärdera Europols rättsliga grund för att begära och ta emot personuppgifter direkt från privata parter.⁶

⁵ EU-organens roll har särskilt behandlats vid de informella mötena i ständiga kommittén för inre säkerhet och rådet i juli (WK 13271/19 och WK 13266/19) och varit ett övergripande tema i alla diskussioner.

⁶ Diskussioner om Europols samarbete med privata parter har ägt rum i arbetsgruppen för brottsbekämpning: dok. 10494/19, 11832/19, 12858/1/19.

För att stärka Europols sektorsövergripande strategi för brottsbekämpning på lång sikt bör samarbetet mellan tullmyndigheter och Europol vidareutvecklas genom att man ökar antalet tullsambandsmän vid Europol, uppmuntrar tullmyndigheterna i alla EU-medlemsstater att använda Siena och ökar det regelbundna och strukturerade informationsutbytet mellan parterna, vilket omfattar riskhantering och underrättelseinformation. Ett mål på kort sikt bör vara att stärka tullens bidrag och integrera detta i genomförandet av Empacts operativa åtgärdsplaner. Dessa åtgärder skulle utgöra en fortsättning på de senaste årens positiva utveckling av samarbetet mellan tullen och Europol.

Utmaningarna i fråga om samarbetet mellan Europeiska unionen och Interpol måste hanteras. Det är viktigt att databaser som fungerar som informationskällor för samarbetet med tredjeländer på området för brottsbekämpning även i framtiden fortsätter att användas i praktiken av EU-medlemsstaternas myndigheter. Samtidigt måste naturligtvis den tillämpliga dataskyddslagstiftningen fullständigt respekteras.

Ordförandeskapet framhåller behovet av en översyn av den rättsliga ramen för gränsöverskridande samarbete inom brottsbekämpning samt av Europols mandat för att anpassa det till det aktuella läget och framtida utmaningar. Fortsatt stöd bör ges till utvecklingen av en gemensam brottsbekämpningskultur hos EU:s brottsbekämpande myndigheter.

4. Övergripande säkerhetsstrategi

Inom den närmsta framtiden kan vi förvänta oss att ett antal tendenser och utvecklingar kommer att ändra hotbilden i EU. Det är efterfrågan och möjligheterna till kriminella företag som styr den brottsliga verksamheten. Dessutom utgör ändrade säkerhetsförhållanden i grannskapet och olika former av våldsamt radikaliserings i Europa fortfarande ett hot mot vår inre säkerhet. En övergripande säkerhetsstrategi med bättre samordning, mer resurser och ökad teknisk kapacitet förutsätter en bättre lägesuppfattning och beredskap inför ett antal olika utmaningar.

Berörda myndigheter inom bland annat brottsbekämpning och civilskydd bör fortsätta att utveckla sin beredskap att motverka hybridhot. Samarbetet mellan berörda nationella myndigheter, med utgångspunkt i deras respektive mandat, och EU:s institutioner, organ och byråer på området för förebyggande och motverkande av hybridhot, inbegripet kopplingen mellan inre och yttre säkerhet, måste kontinuerligt förbättras och harmoniseras. Samtidigt är det viktigt att synergier ökar och att dubbelarbete undviks, bland annat genom horisontella arbetssätt, ökat informationsutbyte och sektorsövergripande kurser och övningar.

Det finns ett starkt behov av att fortsätta diskussionerna om hybridhotens inre dimension, särskilt RIF-myndigheternas roll för att främja EU:s och medlemsstaternas kapacitet att identifiera hybridåtgärder och källor till sådana.

Dessutom behövs en övergripande strategi för att effektivt kunna bekämpa desinformation. I detta avseende bör brottsbekämpande myndigheters deltagande, även i befintliga EU-mekanismer som systemet för snabb varning, beaktas. Brottsbekämpande myndigheter ökar EU:s och medlemsstaternas motståndskraft och kampen mot desinformation måste beaktas⁷.

Ordförandeskapet framhåller behovet av att utnyttja befintliga verktyg bättre och förbättra den övergripande samordningen på EU-nivå. RIF-myndigheternas stöd till medlemsstaterna måste också behandlas i detta sammanhang.

Teknik och internet kommer att användas i allt större utsträckning för att iscensätta brottslig verksamhet. Till exempel förväntas användningen av onlineplattformar för handel med en mängd olagliga varor öka på både det vanliga nätet och på den mörka webben. Onlinemiljön kan missbrukas för att radikaliserar, rekrytera och uppvigla till våld. Spridningen av terrorisminnehåll och innehåll med övergrepp mot barn på nätet bör förebyggas på ett effektivt sätt och sådant innehåll bör snabbt tas bort.

⁷ *Hybrid threats and internal security: Law Enforcement Strategic Communication and Tackling Disinformation* (dok. 11831/19).

Ordförandeskapet betonar att förebyggande av våldsamt radikaliserande är en integrerad del av en övergripande strategi för terrorismbekämpning. Att samarbeta med och stödja yrkesutövare i frontlinjen är fortfarande av avgörande vikt för att kunna förebygga och bekämpa våldsamt extremism. Det finns ett behov av att ta itu med alla former av politiskt eller ideologiskt motiverad våldsamt extremism. Framöver bör fokus för arbetet med att motverka och förebygga våldsamt extremism och terrorism fortsätta att utgå från en bred bas där man också beaktar nya tendenser inom våldsamt extremism.

Hotet från våldsamt högerextremism och terrorism måste hanteras genom upprättandet av en bättre lägesbild, kontinuerligt utbyte av god praxis, samarbete med viktiga tredjeländer och genom att ta itu med spridningen av olagligt högerextremistiskt innehåll både online och offline. Problemet med återvändande terroriststridande bör hanteras bland annat genom en effektivare användning av SIS.

Ordförandeskapet betonar att vi behöver en övergripande och samhällsomfattande säkerhetsstrategi för att kunna ta itu med de olika hoten mot den inre säkerheten. Dessutom framhålls vikten av att arbeta över alla berörda politiska sektorer på ett mer strategiskt, samordnat och enhetligt sätt.

Subject	Meeting	Reference Number
Future Direction of internal security in the EU	Informal COSI meeting on 8-9 July 2019, The Hague	WK 13264/19
Hybrid threats and internal security	Informal COSI meeting on 8-9 July 2019, The Hague	WK 13265/19
Twenty Years of Europol - what next?	Informal COSI meeting on 8-9 July 2019, The Hague	WK 13266/19
The future of EU Internal Security	Informal Council meeting on 18-19 July 2019, Helsinki	WK 13271/19
The future direction of EU internal security: new technologies and internal security	JHA Council on 2 October 2019	12496/19
Hybrid threats and Internal Security	JHA Council on 2 October 2019	12495/19
Right-wing violent extremism and terrorism	JHA Council on 2 October 2019	12494/19
EU Information Management - Automation, access to, sharing of, and analysis of information	COSI meeting on 19 November 2019	13510/19
The future of EU law enforcement: Training for law enforcement	COSI meeting on 19 November 2019	13973/19