EUROPEISKA KOMMISSIONEN

UNIONENS HÖGA REPRESENTANT FÖR UTRIKES FRÅGOR OCH SÄKERHETSPOLITIK

Bryssel den 19.7.2017
JOIN(2017) 30 final

GEMENSAM RAPPORT TILL EUROPAPARLAMENTET OCH RÅDET

om genomförandet av den gemensamma ramen för att motverka hybridhot – Europeiska unionens insatser

1. INLEDNING

EU står inför en av de största säkerhetsutmaningarna i sin historia. Hoten tar sig i allt högre grad uttryck i okonventionella former, i vissa fall fysiska, som nya typer av terrorism, i vissa fall digitala i form av komplexa it-attacker. I ytterligare andra fall används mer subtila former av tvång och påtryckningar, inklusive vilseledande kampanjer och manipulation av media. De syftar till att underminera grundläggande europeiska värden såsom människans värdighet, frihet och demokrati. På senare tid har samordnade it-attacker runtom i världen, vilkas upphovsmän har visat sig vara svåra att identifiera, visat på sårbarheten i våra samhällen och inom våra institutioner.

I april 2016 antog Europeiska kommissionen och den höga representanten ett gemensamt meddelande om att motverka hybridhot[1] (en gemensam ram). Den gemensamma ramen utgår från hybridhotens gränsöverskridande och komplexa karaktär och föreslår ett förvaltningsövergripande tillvägagångssätt för att stärka den allmänna resiliensen i våra samhällen. Rådet välkomnade initiativet och de föreslagna åtgärderna[2], och uppmanade kommissionen och den höga representanten att i juli 2017 rapportera om framstegen. I den mån motverkandet av hybridhot rör den nationella säkerheten och det nationella försvaret ligger det främsta ansvaret hos medlemsstaterna, även om EU kan hjälpa dem att bygga upp deras resiliens mot hybridhot.

Den gemensamma ramen för att motverka hybridhot utgör en viktig del av EU:s övergripande och mer integrerade synsätt på säkerhet och försvar. Den bidrar till skapandet av ett Europa som erbjuder skydd som kommissionens ordförande Juncker efterlyste i sitt tal om tillståndet i unionen i september 2016. Under 2016 lade Europeiska unionen också grunden för en starkare europeisk försvarspolitik för att bemöta medborgarnas förväntningar på ett bättre skydd. I den globala strategin för Europeiska unionens utrikes- och säkerhetspolitik[3] utvecklas behovet av ett integrerat synsätt som kopplar ihop den interna resiliensen med EU:s yttre åtgärder, och efterlyses synergieffekter mellan försvarspolitiken och politiken vad gäller den inre marknaden, näringslivet, brottsbekämpning och underrättelsetjänster. Efter det att den europeiska handlingsplanen på försvarsområdet antogs i november 2016 lade kommissionen fram konkreta initiativ som kommer att bidra till att stärka EU:s förmåga att bemöta hybridhot genom att främja resiliensen i försvarsleveranskedjorna och stärka den inre marknaden på försvarsområdet. Framför allt inrättade kommissionen den 7 juni 2017 en europeisk försvarsfond med en föreslagen finansiering på 600 miljoner euro fram till 2020 och 1,5 miljarder euro årligen efter 2020. Kommissionen underströk i sitt meddelande om säkerhetsunionen[4] behovet av att motverka hybridhot och vikten av att säkerställa bättre samstämmighet mellan inre och yttre åtgärder på säkerhetsområdet.

EU:s ledare har satt säkerhet och försvar i centrum för debatten om Europas framtid.[5] Detta framgick av **Romförklaringen** av den 25 mars 2017 som lade fram en vision om en säker och

[1] Gemensamt meddelande till Europaparlamentet och rådet: *Gemensam ram för att motverka hybridhot – Europeiska unionens insatser*, JOIN (2016) 18 final.
[2] *Rådets slutsatser om motverkande av hybridhot*, pressmeddelande 196/16 av den 19 april 2016.
[3] Framlagd av den höga representanten för Europeiska rådet den 28 juni 2016.
[4] COM(2016) 230 final, 20.4.2016.
[5] Europeiska rådets Bratislavafärdplan av den 16 september 2016 och Romförklaringen från ledarna för 27 medlemsstater och Europeiska rådet, Europaparlamentet och Europeiska kommissionen av den 25 mars 2017.

trygg union fast besluten att stärka den gemensamma säkerhets- och försvarspolitiken. Ordförandena för Europeiska rådet och Europeiska kommissionen samt Natos generalsekreterare undertecknade i Warszawa den 8 juli 2016 ett gemensamt uttalande i syfte att ge ny drivkraft och nytt innehåll till det strategiska partnerskapet mellan EU och Nato. I det gemensamma uttalandet anges sju konkreta områden, däribland att motverka hybridhot, där samarbetet mellan de två organisationerna bör förstärkas. Både EU och Nato godkände därefter en gemensam uppsättning med 42 förslag att genomföra och en första rapport, som visar betydande framsteg, utfärdades i juni 2017[6].

I kommissionens diskussionsunderlag om det europeiska försvarets framtid[7] som presenterades i juni 2017 beskrivs olika scenarier för hur man ska möta de växande säkerhetshot som EU står inför och stärka EU:s egen försvarskapacitet fram till 2025. I alla tre scenarierna betraktas säkerhet och försvar som integrerade delar av det europeiska projektet, i syfte att skydda och främja våra intressen här hemma och utomlands. EU måste bli en säkerhetsgarant och successivt säkerställa sin egen säkerhet. Ingen enskild medlemsstat kan möta de kommande utmaningarna på egen hand, i synnerhet när det gäller att motverka hybridhot. Samarbete om försvar och säkerhet är därför inte ett alternativ; det är en nödvändighet för att skapa ett Europa som erbjuder skydd.

Syftet med denna rapport är att redogöra för framstegen och för kommande åtgärder att genomföra inom de fyra områden som föreslås i den gemensamma ramen: förbättring av situationsmedvetenheten, ökning av resiliensen, förstärkning av medlemsstaternas och unionens förmåga att förebygga och reagera på kriser och samordna återhämtning, och utökning av samarbetet med Nato för att säkerställa komplementaritet mellan åtgärder. Den bör läsas tillsammans med de månatliga lägesrapporterna om utvecklingen mot en effektiv och genuin säkerhetsunion.

2. KÄNNA IGEN HYBRIDHOT

Hybridverksamhet håller på att bli ett vanligt förekommande inslag i den europeiska säkerhetsmiljön. Intensiteten i denna verksamhet ökar och medför en större oro för manipulerade val, desinformationskampanjer, fientlig it-verksamhet och för att utövarna av hybridhot försöker att radikalisera utsatta i samhället som proxyaktörer. Sårbarheten för hybridhot begränsas inte av nationella gränser. Hybridhot kräver ett samordnat bemötande också på EU- och Nato-nivå. Utvecklingen sedan april 2016 visar att även om hoten fortfarande ofta bedöms enskilt finns det inom unionen en ökande medvetenhet och förståelse för hybridkaraktären på en del av den verksamhet som iakttas och behovet av samordnade åtgärder. EU kommer att fortsätta sina ansträngningar för att förbättra situationsmedvetenheten och samarbetet.

***Åtgärd 1*: Medlemsstaterna, med lämpligt stöd av kommissionen och den höga representanten, uppmanas att genomföra en undersökning av risker i samband med hybridhot för att identifiera centrala svagheter som kan påverka nationella och alleuropeiska strukturer och nätverk, samt ta fram särskilda indikatorer med anknytning till hybridhot.**

[6] http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-conclusions-eu-nato-cooperation
[7] Diskussionsunderlag om det europeiska försvarets framtid, 7.6.2017, https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_en.pdf

Rådet har inrättat gruppen Ordförandeskapets vänner med experter från medlemsstaterna för att skapa en allmän undersökning som skulle göra det möjligt att bättre identifiera viktiga indikatorer för hybridhot, införliva dessa i system för tidig varning och befintliga system för riskbedömning samt sprida dem på lämpligt sätt. Man har kommit överens om gruppens mandat och arbetet har redan inletts. Den allmänna undersökningen bör vara färdig i slutet av 2017 och de faktiska undersökningarna inledas därefter. Skydden mot hybridhot bör vara ömsesidigt förstärkande. Medlemsstaterna uppmanas därför att utföra dessa undersökningar snarast möjligt eftersom de kommer att ge värdefull information om sårbarheten och beredskapen i hela EU.

a. ÖKA MEDVETENHETEN

Utbyte av underrättelseanalys och bedömningsarbete är ett viktigt verktyg för att minska osäkerheten och förbättra situationsmedvetenheten. Betydande framsteg har gjorts under det senaste året. EU:s gemensamma enhet för hybridhot har etablerats och fungerar nu fullt ut, arbetsgruppen East Stratcom är inrättad och Finland har börjat arbetet med det europeiska centrumet för motverkande av hybridhot. Mycket arbete har inriktats på att analysera verktyg och medel för propaganda eller desinformation i gott samarbete mellan EU:s arbetsgrupp East Stratcom, EU:s gemensamma enhet för hybridhot och Nato. Detta utgör en god grund för att fortsätta att bygga upp en djupare förankrad kultur av analys och bedömning av hot mot vår inre och yttre säkerhet utifrån ett hybridperspektiv.

EU:s gemensamma enhet för hybridhot

Åtgärd 2: Inom ramen för Europeiska unionens underrättelseanalyscentrum inrätta EU:s gemensamma enhet för hybridhot som kan ta emot och analysera säkerhetsskyddsklassificerad information och information från öppna källor om hybridhot. Medlemsstaterna uppmanas att upprätta nationella kontaktpunkter för hybridhot för att säkerställa samarbete och säker kommunikation med EU:s gemensamma enhet för hybridhot.

EU:s gemensamma enhet för hybridhot har inrättats inom Europeiska unionens underrättelseanalyscentrum för att ta emot och analysera säkerhetsskyddsklassificerad information och information från öppna källor om hybridhot från olika berörda parter. Analysen ska därefter delas inom EU och mellan medlemsstaterna och ligger därefter till grund för EU:s beslutsprocesser, inbegripet de säkerhetsriskbedömningar som utförs på EU-nivå. Direktoratet för underrättelseverksamhet vid Europeiska unionens militära stab bidrar till enhetens arbete med militär analys. Hittills har mer än 50 bedömningar och briefingar om ämnen som rör hybridhot gjorts. Sedan januari 2017 har enheten utarbetat en periodisk hybridbulletin med analyser av aktuella hot och hybridrelaterade frågor som distribueras inom EU:s institutioner och organ och nationella kontaktpunkter[8]. Enhetens fullständiga operativa kapacitet uppnåddes som planerat i maj 2017. Slutligen pågår direkta kontakter på tjänstemannanivå med Natos nya sektion för hybridanalys, både när det gäller att dela med sig av erfarenheter från inrättandet av enheten och av information (med full respekt för EU:s bestämmelser om utbyte av säkerhetsskyddsklassificerade uppgifter). EU:s gemensamma enhet för hybridhot håller för närvarande på att kartlägga ytterligare initiativ för att förbättra det framtida samarbetet och kommer att spela en viktig roll i de parallella övningar EU och

[8] Hittills har 21 medlemsstater utsett nationella kontaktpunkter. Dessa är fysiska personer som arbetar i medlemsstaternas huvudstäder i en politisk roll eller en roll som rör resiliensen mot hybridhot.

Nato planerar till hösten 2017 då enhetens reaktionsförmåga kommer att prövas och lärdomar dras.

Strategisk kommunikation

Åtgärd 3: Den höga representanten ska tillsammans med medlemsstaterna undersöka sätt att uppdatera och samordna sin förmåga att kommunicera på ett proaktivt och strategiskt sätt och optimera användningen av mediebevakning och språkspecialister.

Desinformationskampanjer och systematisk spridning av falska nyheter i sociala medier ingår i ett spektrum av åtgärder som under de senaste månaderna i ökad utsträckning har använts för att undergräva motståndare. Sociala medier är den lämpligaste plattformen för att förmedla uppgifter som förefaller tillförlitliga och legitima och kan förändra den allmänna opinionen till förmån för vissa enskilda personer, organisationer eller myndigheter. Det huvudsakliga målet med dessa hybridmetoder är att skapa oreda i våra samhällen och att misskreditera demokratiska regeringar och våra strukturer, institutioner och val. Falska nyheter sprids ofta via nätplattformar (se även åtgärd 17). Kommissionen och den höga representanten välkomnar de åtgärder som nyligen vidtagits av nätplattformar och nyhetsmedier för att komma till rätta med felaktig information. Kommissionen kommer att fortsätta att uppmuntra sådana frivilliga åtgärder.

Den höga representanten har inrättat arbetsgruppen East Stratcom som gör prognoser och bekämpar vilseledande information och kampanjer. Detta ger en betydligt bättre kommunikation om unionens politik i det östra grannskapet och stärker samtidigt medieklimatet i dessa länder. Arbetsgruppen har under de senaste två åren upptäckt mer än 3 000 enskilda fall av vilseledande information på 18 språk. Den förestående lanseringen av en ny webbplats *# EUvsdisinformation* med sökfunktion kommer att avsevärt förbättra tillgången för användarna. Forskning och analyser visar dock att antalet medier för vilseledande information och antalet meddelanden som sprids dagligen är betydligt högre. I projektet EU-Strat, som finansieras genom Horisont 2020, analyseras politiken och medierna i länderna i det östra grannskapet.

Den höga representanten uppmanar medlemsstaterna att stödja det arbete som utförs av Stratcom-arbetsgrupperna för att på ett effektivare sätt motverka framväxten av hybridhot. Detta kommer att hjälpa arbetsgruppen South att förbättra kommunikationen, även på arabiska, och den utåtriktade verksamheten i arabvärlden, och slå hål på myter och framföra fakta om Europeiska unionen och dess politik. Samarbetet med lokala journalister kommer att säkerställa att nyhetsprodukterna är kulturellt anpassade. Båda arbetsgrupperna, som stöds av EU:s gemensamma enhet för hybridhot, syftar till att stödja och komplettera medlemsstaternas insatser på området. Dessutom samfinansierar kommissionen Europeiska nätverket för strategisk kommunikation, som är ett samarbetsnätverk för 26 medlemsstater som delar analyser, bästa praxis och idéer om användningen av strategisk kommunikation i kampen mot våldsbejakande extremism och vilseledande information.

Kompetenscentrum för motverkande av hybridhot

Åtgärd 4: Medlemsstaterna uppmanas att överväga att inrätta ett kompetenscentrum för motverkande av hybridhot.

Finland hörsammade uppmaningen att inrätta ett kompetenscentrum och inledde i april 2017 arbetet med det europeiska centrumet för motverkande av hybridhot. Tio EU-medlemsstater[9], Norge och Förenta staterna är medlemmar, medan både EU och Nato har uppmanats att stödja styrelsen[10]. Centrumets uppdrag är att uppmuntra en strategisk dialog samt bedriva forskning och analys i samarbete med intressegrupper för att öka resiliensen och reaktionsförmågan för att bidra till bekämpningen av hybridhot. Centrumet förväntas också fungera som en plats för framtida hybridövningar. Centrumet har redan upprättat en nära kontakt med EU:s gemensamma enhet för hybridhot och de båda organisationernas arbete bör komplettera varandra. EU håller för närvarande på att göra en bedömning av på vilka sätt man kan erbjuda konkret stöd till centrumet.

b. ÖKA RESILIENSEN

I den gemensamma ramen placeras resiliens (t.ex. vad gäller transporter, kommunikationer, energi, finans eller regional säkerhetsinfrastruktur) i centrum för EU:s insatser för att motverka propaganda och informationskampanjer, försök att undergräva företag, samhällen och ekonomiska flöden samt angrepp mot it-relaterad infrastruktur. En förstärkning av resiliensen anses vara en förebyggande och avskräckande åtgärd för att stabilisera samhällen och undvika en upptrappning av kriser både i och utanför EU. Mervärdet i EU:s insatser ligger i att bistå medlemsstater och partner med att bygga upp deras resiliens med hjälp av ett brett spektrum av befintliga instrument och program. Betydande framsteg har gjorts när det gäller åtgärder för att stärka resiliensen på områden som it-säkerhet, kritisk infrastruktur, skydd mot olaglig användning av det finansiella systemet och insatser för att motverka våldsbejakande extremism och radikalisering.

Skydd av kritisk infrastruktur

Åtgärd 5: Kommissionen kommer i samarbete med medlemsstaterna och berörda aktörer att identifiera gemensamma verktyg, bl.a. indikatorer, för att stärka den kritiska infrastrukturens skydd och resiliens mot hybridhot inom berörda sektorer.

Inom ramen för det europeiska programmet för skydd av kritisk infrastruktur fortsatte kommissionen arbetet med att identifiera gemensamma verktyg, bl.a. indikatorer på sårbarhet, för att stärka den kritiska infrastrukturens resiliens mot hybridhot inom berörda sektorer. I maj 2017 anordnade kommissionen en workshop om hybridhot mot kritisk infrastruktur med deltagare från nästan alla medlemsstater, operatörer av kritisk infrastruktur och EU:s gemensamma enhet för hybridhot och med Nato som observatör. Man enades om en gemensam färdplan och åtgärder för det framtida arbetet, på grundval av ett frågeformulär som sänts till de nationella myndigheterna i medlemsstaterna. Kommissionen kommer under hösten att fortsätta att rådgöra med berörda parter i syfte att komma överens om indikatorer före utgången av 2017.

Europeiska försvarsbyrån arbetar för att kartlägga gemensam kapacitet och forskningsbrister som uppstår mellan energiinfrastrukturer och försvarskapacitet. Europeiska försvarsbyrån kommer under hösten 2017 att utveckla ett idédokument samt pilotåtgärder för holistiska metoder.

[9] Finland, Frankrike, Tyskland, Lettland, Litauen, Polen, Sverige, Förenade kungariket, Estland och Spanien.
[10] Centrumet är öppet för andra EU-medlemsstater och Nato-allierade.

Trygga EU:s energiförsörjning

Åtgärd 6: Kommissionen kommer i samarbete med medlemsstaterna att stödja ansträngningar för att diversifiera energikällorna och främja säkerhets- och trygghetsnormer för att öka den kärntekniska infrastrukturens resiliens.

Kommissionen lade i december 2016 och i april 2017 fram konkreta förslag i paketet för trygg energiförsörjning och rådet och Europaparlamentet kom överens om den nya förordningen om tryggad gasförsörjning som syftar till att förhindra kriser i gasförsörjningen. De nya bestämmelserna kommer att säkerställa ett regionalt samordnat och gemensamt tillvägagångssätt från medlemsstaterna vad gäller åtgärder för försörjningstrygghet. Detta kommer att ge EU bättre möjligheter att förbereda sig för och hantera gasbrister i händelse av en kris eller en hybridattack. För första gången kommer solidaritetsprincipen att komma till användning. Medlemsstater kommer att kunna hjälpa sina grannländer i händelse av en allvarlig kris eller attack så att europeiska hushåll och företag inte drabbas av avbrott i försörjningen.

EU har också gjort framsteg med att utveckla viktiga projekt för att diversifiera sina försörjningsvägar och energikällor i linje med den strategiska ramen för energiunionen och den europeiska strategin för energitrygghet. När det till exempel gäller den södra gaskorridoren pågår konkreta byggnadsarbeten på alla stora projekt: utbyggnaden av den sydkaukasiska ledningen, de transanatoliska och transadriatiska gasledningarna, Shah Deniz II samt utvidgningen av den södra gaskorridoren till Centralasien, framför allt Turkmenistan. Importen av flytande naturgas till Europa ökar och kommer från nya källor, som Förenta staterna. Exemplet med terminalen i Litauen visar hur diversifieringsprojekt kan minska beroendet av en enda leverantör. En förstärkning av energiansträngningarna och en bättre användning av inhemska, framför allt förnybara, energikällor bidrar också till diversifieringen av försörjningsvägar och energikällor.

När det gäller kärnsäkerhet stöder kommissionen aktivt, särskilt genom workshoppar med nationella myndigheter och tillsynsmyndigheter, ett konsekvent och effektivt genomförande av de två direktiven om kärnsäkerhet och grundläggande säkerhetsnormer, som medlemsstaterna är skyldiga att införliva till slutet av 2017 respektive 2018. Dessutom bidrar Euratoms forsknings- och utbildningsprogram till att förbättra kärnsäkerheten.

Transportsäkerhet och säkerhet i försörjningskedjan

Åtgärd 7: Kommissionen kommer att övervaka framväxande hot i hela transportsektorn och kommer att uppdatera lagstiftning där så är lämpligt. Vid genomförandet av EU:s strategi för sjöfartsskydd samt EU:s strategi och handlingsplaner för riskhantering på tullområdet kommer kommissionen och den höga representanten (inom ramen för sina respektive befogenheter), i samordning med medlemsstaterna, att undersöka hur hybridhot ska bemötas, särskilt när det gäller hot mot kritisk transportinfrastruktur.

I enlighet med meddelandet om säkerhetsunionen underlättar kommissionen bedömningar av säkerhetsrisker på EU-nivå med medlemsstaterna, EU:s underrättelseanalyscentrum och relevanta organ för att identifiera hot mot transportsäkerheten och stödja utvecklingen av effektiva och proportionerliga riskreducerande åtgärder. Nedskjutningen av Malaysia Airlines flyg MH17 över östra Ukraina 2014 visade på riskerna med att flyga över konfliktområden. I

linje med rekommendationerna från den europeiska högnivågruppen för konfliktområden[11] har kommissionen med stöd av nationella experter på luftfart och säkerhet och Europeiska utrikestjänsten utvecklat en metod för EU-gemensam riskbedömning som möjliggör utbyte av säkerhetsskyddklassade uppgifter och definitionen av en gemensam hotbild. I mars 2017 utfärdade Europeiska byrån för luftfartssäkerhet (Easa) en första *Conflict Zones Information Bulletin*[12] baserad på resultaten av denna EU-gemensamma riskbedömning. Kommissionen överväger att utvidga de åtgärder för riskbedömning som genomförts på luftfartsområdet till andra transportslag (t.ex. järnväg, sjöfart) och förslag kommer att läggas fram under 2018. I juni 2017 inledde kommissionen, utrikestjänsten och medlemsstaterna en riskbedömning av järnvägssäkerheten för att kartlägga brister och möjliga åtgärder för att reducera dessa.

Avsevärda ansträngningar för luftfartsskydd och flygledningstjänst har också gjorts i säkerhetsforskningsprojekt inom det sjunde ramprogrammet och Horisont 2020. På det civila luftfartsområdet utvecklar kommissionen, tillsammans med Easa och berörda parter, två nya initiativ för att förbättra it-säkerheten, och även hantera hybridhot: inrättandet av en it-incidenthanteringsorganisation för luftfart och en arbetsgrupp om it-säkerhet inom det gemensamma företaget för forskningsprojektet om flygledningstjänster i det gemensamma europeiska luftrummet (Sesar). Europeiska försvarsbyrån ska tillhandahålla militär expertis när det gäller it för luftfart till det gemensamma företaget Sesar, samt till Easa, genom den så kallade europeiska strategiska samordningsplattformen för it-säkerhet, som på begäran av medlemsstaterna och näringslivet kommer att bidra till samordning på EU-nivå av all verksamhet inom luftfarten. I linje med färdplanen om it-säkerhet för luftfarten genomförde Easa under 2016 analyser av luckor i befintliga bestämmelser och särskilt i utformningen och inrättandet av det europeiska centrumet för it-säkerhet inom luftfart. Centrumet är nu i drift och samarbetar med it-incidenthanteringsorganisationen för EU:s institutioner och byråer (Cert-EU (ett samförståndsavtal undertecknades i februari 2017) om hotbildsanalyser för luftfarten och med Eurocontrol (en färdplan för samarbetet har antagits), och en webbplats för spridning av analyser av öppna källor har utvecklats. Under hösten 2017 kommer ett standardiseringsprogram och ett säkert informationsutbyte att antas.

Riskhantering på tullområdet

På tullområdet inriktar sig kommissionen på en betydande uppgradering av systemet för förhandsinformation om gods och riskhantering. Systemet täcker hela skalan av tullrelaterade risker, bland annat i samband med hot mot säkerheten och integriteten i internationella leverantörskedjor och relevant kritisk infrastruktur (t.ex. direkta hot mot hamnanläggningar, flygplatser eller landgränser som orsakas av import). Uppgraderingen syftar till att säkerställa att tullen i EU får all nödvändig information från näringsidkare när det gäller rörlighet för varor, att de kan sprida denna information på ett mer effektivt sätt mellan medlemsstaterna, att de tillämpar gemensamma samt medlemsstatsspecifika riskbestämmelser, och att de mer effektivt kan identifiera sändningar med hög riskfaktor genom att samarbeta mer intensivt med andra myndigheter, bl.a. andra brottsbekämpande organ och säkerhetsorgan. Den it-utveckling som behövs för att kommissionen ska genomföra denna uppgradering är för närvarande i sin inledningsfas och relevanta investeringar på central nivå kommer att inledas under de närmaste månaderna.

[11] https://www.easa.europa.eu/system/files/dfu/208599_EASA_CONFLICT_ZONE_CHAIRMAN_REPORT_no_B_update.pdf
[12] https://ad.easa.europa.eu/czib-docs/page-1

Rymden

Åtgärd 8: Inom ramen för rymdstrategin och den europeiska handlingsplanen på försvarsområdet kommer kommissionen att föreslå att rymdinfrastrukturens förmåga att stå emot hybridhot ska stärkas, särskilt genom att eventuellt utvidga tillämpningsområdet för rymdövervakning och spårning till att även omfatta hybridhot, genom att utarbeta nästa generation av statlig satellitkommunikation på EU-nivå och genom att införa Galileo inom kritisk infrastruktur som är beroende av tidssynkronisering.

Kommissionen kommer vid utarbetandet av regelverket om statlig satellitkommunikation, rymdövervakning och spårning under 2018 att integrera resiliens mot hybridhot i sin bedömning. Vid förberedelserna för utvecklingen av Galileo och Copernicus kommer kommissionen i linje med rymdstrategin att bedöma om dessa tjänster kan bidra till att reducera sårbarheten hos kritisk infrastruktur. Utvärderingsrapporten bör vara klar under hösten 2017 och förslaget om nästa generation av Copernicus och Galileo under 2018. Europeiska försvarsbyrån arbetar med samarbetsprojekt för kapacitetsutveckling på områdena rymdbaserade kommunikationer, militär positionsbestämning, navigering och tidsbestämning och jordobservation. Samtliga projekt kommer att inriktas på krav för resiliens mot bakgrund av nuvarande och framväxande hybridhot.

Försvarskapacitet

Åtgärd 9: Den höga representanten, vid behov med stöd av medlemsstaterna, kommer i samverkan med kommissionen att lägga fram förslag till projekt om anpassning av försvarskapaciteten och om utveckling på kapacitet av betydelse för EU, specifikt för att motverka hybridhot mot en eller flera medlemsstater.

Under 2016 och 2017 genomförde Europeiska försvarsbyrån tillsammans med kommissionen, Europeiska utrikestjänsten och experter från medlemsstaterna tre skrivbordsövningar med hybridhotsscenarier. Erfarenheterna från dessa kommer att beaktas vid översynen av kapacitetsutvecklingsplanen, så att den resulterande utvecklingen av nyckelkapacitet som krävs för att motverka hybridhot kommer att ingå i EU:s nya prioriteringar för kapacitetsutveckling. Arbetet med översynen av behovskatalogen 2005 kommer att beakta hybridhotsaspekten. I april 2017 slutförde Europeiska försvarsbyrån en rapport om de militära konsekvenserna av hybridattacker riktade mot kritisk hamninfrastruktur som kommer att diskuteras i en workshop med experter i oktober 2017. En annan särskild analys av militärens roll vid bekämpandet av minidrönare planeras till 2018. Dessutom kan kapacitetsprioriteringar för att stärka resiliensen mot de hybridhot som medlemsstaterna identifierat också vara berättigade till stöd från Europeiska försvarsfonden från och med 2019. Kommissionen uppmanar medlagstiftarna att säkerställa ett snabbt antagande och medlemsstaterna att lägga fram förslag till kapacitetsprojekt för att stärka EU:s resiliens mot hybridhot.

Åtgärd 10: Kommissionen kommer i samarbete med medlemsstaterna att öka medvetenheten om och resiliensen mot hybridhot inom befintliga beredskaps- och samordningsmekanismer, särskilt hälsosäkerhetskommittén.

I syfte att stärka beredskapen och resiliensen mot hybridhot, inbegripet uppbyggnad av kapacitet inom hälso- och sjukvårdssystemen och livsmedelssektorn, stöder kommissionen medlemsstaterna genom utbildning, simuleringsövningar och genom att underlätta utbytet av erfarenheter och riktlinjer och genom finansiering av gemensamma åtgärder. Detta sker framför allt inom EU:s hälsosäkerhetsram för allvarliga gränsöverskridande hot mot

människors hälsa och inom folkhälsoprogrammet som genomför det internationella hälsoreglementet, som är en bindande lagstiftning för 196 länder, inklusive medlemsstaterna, och som syftar till att förebygga och reagera på akuta, gränsöverskridande hälsorisker i hela världen. För att pröva den sektorsövergripande beredskapen och reaktionen inom hälso- och sjukvårdssektorn kommer kommissionen att genomföra en övning för komplexa och flerdimensionella hybridhot under hösten 2017. Kommissionen och medlemsstaterna förbereder en gemensam åtgärd under 2018–20 om vaccinering, inklusive tillgången på vaccin, efterfrågeprognoser och forskning om innovativa vaccintillverkningsprocesser i syfte att öka tillgången på vaccin och förbättra hälsosäkerheten på EU-nivå. Kommissionen samarbetar även med Europeiska myndigheten för livsmedelssäkerhet och Europeiska centrumet för förebyggande och kontroll av sjukdomar för att anpassa sig till avancerade vetenskapliga utredningsmetoder, för att mer exakt identifiera och fastkälla källan till hot mot hälsan och en åtföljande snabb hantering av livsmedelssäkerhetsincidenter. Kommissionen har inrättat ett nätverk av forskningsfinansiärer, Globalt forskningssamarbete om smittskydd, för en samordnad forskningsinsats inom 48 timmar efter varje betydande utbrott.

***Åtgärd 11*: Kommissionen uppmuntrar medlemsstaterna att inrätta och fullt ut utnyttja ett nätverk mellan de 28 it-incidentcentrumen och EU:s incidenthanteringsorganisation, även som en ram för strategiskt samarbete, och att göra detta till en prioriterad fråga. Kommissionen bör, i samordning med medlemsstaterna, se till att sektorsvisa initiativ mot it-hot (t.ex. på luftfarts-, energi- eller sjöfartsområdet) överensstämmer med den sektorsövergripande kapacitet som omfattas av it-säkerhetsdirektivet i syfte att sammanföra information, sakkunskap och snabba insatser.**

Den senaste tidens globala it-attacker som med hjälp av ransomware och sabotageprogram slagit ut tusentals datasystem har återigen understrukit det akuta behovet av att öka it-systemens resiliens och säkerhetsåtgärderna inom EU. Som meddelades i halvtidsöversynen av strategin för den digitala inre marknaden håller kommissionen och den höga representanten nu på att se över 2013 års EU-strategi för cybersäkerhet, särskilt genom antagandet av ett lagstiftningspaket som planeras till september 2017. Målet är att tillhandahålla ett effektivare och sektorsövergripande svar på dessa hot och öka förtroendet för det digitala samhället och ekonomin. Man kommer även att se över mandatet för Europeiska unionens byrå för nät- och informationssäkerhet (Enisa) för att definiera dess roll i det förändrade it-säkerhetslandskapet. Europeiska rådet[13] välkomnade kommissionens avsikt att se över EU:s strategi för cybersäkerhet.

Antagandet av direktivet om nätverks- och informationstjänster[14] i juli 2016 var ett viktigt steg mot uppbyggnaden av it-säkerhetsresiliens på europeisk nivå. Genom direktivet fastställs de första EU-omfattande reglerna om it-säkerhet, förbättras it-säkerhetskapaciteten och förstärks samarbetet mellan medlemsstaterna. Direktivet kräver också att företag inom kritiska sektorer vidtar lämpliga säkerhetsåtgärder och anmäler allvarliga it-incidenter till berörd nationell myndighet. Bland dessa sektorer återfinns energi, transporter, vatten, hälso- och sjukvård, bankväsende och finansmarknadens infrastruktur. Onlinemarknadsplatser, molntjänster och sökmotorer kommer att behöva vidta liknande åtgärder. En konsekvent tillämpning mellan olika sektorer samt över gränserna kommer att säkerställas genom den samarbetsgrupp för nätverks- och informationstjänster som kommissionen inrättade 2016 och som har till uppgift att undvika fragmentering av marknaden. I detta sammanhang anses

[13] Slutsatser från Europeiska rådets möte den 22-23 juni 2017.
[14] 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 (EUT L 194, 19.7.2016, s. 1).

direktivet om nätverks- och informationstjänster vara referensramen för alla sektorsspecifika initiativ på it-säkerhetsområdet. Genom direktivet skapas också ett nätverk av it-incidentcentrum som samlar alla berörda aktörer. Kommissionen och Cert-EU övervakar parallellt och aktivt utvecklingen av it-hot och utbyter information med nationella myndigheter för att se till att EU-institutionernas it-system är säkra och resilienta mot it-attacker. WannaCry-ransomwareincidenten i maj 2017 gav nätverket en första möjlighet att operativt utbyta information och samarbeta genom rådgivning. EU:s incidenthanteringsorganisation stod i nära kontakt med det europeiska it-brottscentrumet vid Europol, de drabbade ländernas it-incidentcentrum, enheter för it-brottslighet samt viktiga partner inom branschen för att reducera hotet och bistå offren. Utbytet av nationella lägesrapporter skapade en gemensam situationsmedvetenhet i hela EU. Erfarenheten gjorde det möjligt för nätverket att vara bättre förberett vid de kommande tillbuden (t.ex. NonPetya). Flera problem identifierades också och håller på att åtgärdas.

***Åtgärd 12*: Kommissionen kommer, i samordning med medlemsstaterna, att samarbeta med industrin inom ramen för ett avtalsbaserat offentlig-privat partnerskap för it-säkerhet i syfte att utveckla och testa teknik för att bättre skydda användare och infrastrukturer mot de it-relaterade aspekterna av hybridhot.**

I juli 2016 undertecknade kommissionen, i samordning med medlemsstaterna, och **industrin** ett avtalsbaserat offentlig-privat partnerskap för it-säkerhet om investeringar upp till 450 miljoner euro inom ramen för EU:s forsknings- och innovationsprogram Horisont 2020 i syfte att utveckla och testa teknik för att bättre skydda användare och infrastrukturer mot it-hot och hybridhot. Partnerskapet ledde till den första alleuropeiska strategiska forskningsagendan som särskilt inriktas på att öka resiliensen hos kritisk infrastruktur och hos medborgare mot it-attacker. Partnerskapet ökade samordningen mellan de berörda parterna vilket leder till ökad effektivitet och ändamålsenlighet i it-säkerhetsfinansieringen inom Horisont 2020. Partnerskapet arbetar parallellt med frågor som rör it-säkerhetscertifiering av informations- och kommunikationsteknik samt frågor om hur den akuta bristen på it-säkerhetsutbildad arbetskraft ska hanteras. Med tanke på de mycket stora behoven av civil forskning och den höga resiliens som krävs på försvarsområdet bidrar Europeiska försvarsbyråns arbetsgrupp om forskning och teknik på it-området till forskning på områden som identifieras av den europeiska cybersäkerhetsorganisationen i deras strategiska forsknings- och innovationsagenda.

***Åtgärd 13*: Kommissionen kommer att utfärda riktlinjer för att ägare av tillgångar inom smarta nät ska kunna förbättra it-säkerheten i sina anläggningar. Inom ramen för initiativet om elmarknadens utformning kommer kommissionen att överväga att lägga fram förslag om ”riskberedskapsplaner” och regler för informationsutbyte och säkerställande av solidaritet mellan medlemsstaterna i kristider, bl.a. regler om hur man ska förebygga och begränsa it-attacker.**

Inom **energisektorn** håller kommissionen på att utarbeta en sektorsspecifik strategi för it-säkerhet med inrättandet av en it-säkerhetsplattform för expertis på energiområdet för att stärka genomförandet av direktivet om nät- och informationssäkerhet. En undersökning från februari 2017 kartlagde bästa tillgängliga teknik för att öka it-säkerheten i system med smarta mätare, till stöd för denna plattform. Kommissionen inrättade också en nätplattform för informationsutbyte inom EU om incidenter och hot som analyserar och sprider uppgifter om it-hot och incidenter inom energisektorn.

Stärka den finansiella sektorns motståndskraft mot hybridhot

Åtgärd 14: I samarbete med Enisa[15], medlemsstaterna samt berörda internationella, europeiska och nationella myndigheter och finansinstitut kommer kommissionen att främja och underlätta upprättandet av plattformar och nätverk för utbyte av information om hot och ta itu med faktorer som hindrar utbytet av sådan information.

I vetskap om att it-hot är bland de allvarligaste riskerna för den finansiella stabiliteten har kommissionen utfört en översyn av regelverket för betaltjänster inom EU, som nu ska genomföras. Det reviderade betaltjänstdirektivet[16] inför nya bestämmelser för att förbättra säkerheten för betalningsinstrument och stark kundautentisering, i syfte att minska bedrägerier, särskilt när det gäller internetbetalningar. Den nya lagstiftningsramen kommer att gälla från januari 2018. För att göra betalningstransaktioner säkra utvecklar för närvarande kommissionen, med hjälp av Europeiska bankmyndigheten och i samråd med berörda parter, bestämmelser om tekniska standarder om stark kundautentisering och om gemensam och säker kommunikation som förväntas offentliggöras i slutet av 2017. Kommissionen har också haft ett nära internationellt samarbete med G7-partnerna som resulterat i G7:s grundläggande principer för it-säkerhet inom finanssektorn, som godkändes i oktober 2016 av G7-ländernas finansministrar och centralbankschefer. Dessa principer är utformade för enheter inom den finansiella sektorn (privata och offentliga) och bidrar till en samordnad strategi för it-säkerhet inom den finansiella sektorn för att gemensamt ta itu med it-hot, inbegripet ökade och mer sofistikerade it-hot.

Transporter

Åtgärd 15: Kommissionen och den höga representanten kommer (inom sina respektive behörighetsområden), i samarbete med medlemsstaterna, att undersöka hur hybridhot ska bemötas, särskilt när det gäller it-angrepp inom transportsektorn.

Genomförandet av handlingsplanen för EU:s strategi för sjöfartsskydd[17] kommer att bidra till att bryta silomentaliteten mellan civila och militära myndigheter vad gäller informationsutbyte och gemensam användning av tillgångar. Ett myndighetsövergripande tillvägagångssätt har lett till ett ökat samarbete mellan olika aktörer. Kommissionen och utrikestjänsten avser att slutföra en gemensam civil-militär strategisk forskningsagenda till slutet av 2017 med en avslutande workshop om skydd av kritisk sjöfartsinfrastruktur. Arbetet kan framöver utvidgas till att omfatta framväxande hot av störningar mot undervattensledningar, energiöverföring, fiberoptiska och traditionella kommunikationskablar utanför nationella vatten.

En nyligen genomförd undersökning[18] utvärderar kapaciteten för riskbedömning hos de nationella myndigheter som utför kustbevakningsuppgifter. Undersökningen identifierar de viktigaste hindren för samarbete och rekommenderar praktiska sätt att förbättra samarbetet

[15] Europeiska unionens byrå för nät- och informationssäkerhet.
[16] Europaparlamentets och rådets direktiv (EU) 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden (EUT L 337, 23.12.2015, s. 35).
[17] https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdfoch den andra rapporten om genomförandet av handlingsplanen för EU:s strategi för sjöfartsskydd som presenterades för medlemsstaterna den 21 juni 2017.
[18] *Evaluation of risk assessment capacity at the level of Member States' authorities performing coast guard functions*, 2017, https://ec.europa.eu/maritimeaffairs/documentation/studies

mellan sjöfartsmyndigheter på EU-nivå och nationell nivå på detta område. Riskbedömning är nödvändig för att motverka maritima hot och ännu mer avgörande för utvärdering och förebyggande av hybridhot, eftersom dessa kräver ytterligare och mer komplexa överväganden. Resultaten av undersökningen kommer att presenteras i olika kustbevakningsrelaterade forum så att de föreslagna rekommendationerna kan bedömas och genomföras för att öka samarbetet på detta område med beredskap och reaktion på hybridhot som huvudmål.

Kampen mot finansiering av terrorism

Åtgärd 16: Kommissionen kommer att använda genomförandet av handlingsplanen mot finansiering av terrorism som ett sätt att bidra till motverkandet av hybridhot.

Förövare av hybridhot och deras anhängare behöver finansiella medel för att verkställa sina planer. EU:s insatser mot brottslighet och finansiering av terrorism inom ramen för den europeiska säkerhetsagendan och handlingsplanen mot finansiering av terrorism kan också bidra till att motverka hybridhot. I december 2016 lade kommissionen fram tre lagstiftningsförslag, bland annat om straffrättsliga påföljder för penningtvätt och olagliga utbetalningar samt frysning och förverkande av tillgångar[19].
Samtliga medlemsstater måste senast den 26 juni 2017 ha införlivat det fjärde direktivet mot penningtvätt[20] och i juli 2016 lade kommissionen fram ett lagstiftningsförslag för att komplettera och förstärka direktivet med ytterligare åtgärder[21].

Den 26 juni 2017 utfärdade kommissionen den överstatliga riskbedömningen som föreskrivs i det fjärde direktivet mot penningtvätt. Kommissionen lade dessutom fram ett förslag till förordning för att förhindra import och lagring av kulturföremål i EU som olagligen exporteras från tredjeländer[22]. Senare i år kommer kommissionen att rapportera om sin pågående bedömning av behovet av eventuella ytterligare åtgärder för att spåra finansiering av terrorism i EU. Kommissionen ser också över lagstiftningen om bekämpning av bedrägeri och förfalskning som rör andra betalningsmedel än kontanter[23].

Den åttonde rapporten om **framsteg i riktning mot en effektiv och verklig säkerhetsunion** innehåller mer detaljer vad gäller genomförandet av handlingsplanen mot finansiering av terrorism.

Främja EU:s gemensamma värderingar och ett inkluderande, öppet och resilient samhälle

Stärkt resiliens mot radikalisering och våldsbejakande extremism

[19] Den tredje rapporten om framsteg i riktning mot en effektiv och verklig säkerhetsunion (COM(2016) 831 final).
[20] Europaparlaments och rådets direktiv (EU) 2015/849 av den 20 maj 2015 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism, om ändring av Europaparlaments och rådets förordning (EU) nr 648/2012 och om upphävande av Europaparlamentets och rådets direktiv 2005/60/EG och kommissionens direktiv 2006/70/EG (EUT L 141, 5.6.2015, s. 73).
[21] För närmare upplysningar se den tredje rapporten om framsteg i riktning mot en effektiv och verklig säkerhetsunion (COM(2016) 831 final) och den åttonde rapporten om framsteg i riktning mot en effektiv och verklig säkerhetsunion (COM(2017) 354 final).
[22] COM(2017) 26.6.2017, COM(2017) 340 final, SWD(2017) 275 final.
[23] Den åttonde rapporten om framsteg i riktning mot en effektiv och verklig säkerhetsunion (COM(2017) 354 final).

Religiös och ideologisk radikalisering, etniska konflikter och minoritetskonflikter kan underblåsas av externa aktörer genom stöd till vissa grupper eller genom ansträngningar för att skapa konflikter mellan olika grupper. Ytterligare utmaningar har dykt upp, exempelvis hot från ensamma aktörer, nya vägar till radikalisering, eventuellt även i samband med migrationskrisen samt framväxten av högerextremism (inklusive våld mot migranter) och risk för polarisering. Medan arbetet mot radikalisering framskrider inom säkerhetsunionen, kan det också vara indirekt relevant ur en hybridhotssynvinkel eftersom personer mottagliga för radikalisering kan manipuleras av förövare av hybridhot.

Åtgärd 17: ***Kommissionen genomför för närvarande de åtgärder mot radikalisering som anges i den europeiska säkerhetsagendan och analyserar behovet av att stärka förfarandena för att ta bort olagligt innehåll, och uppmanar mellanhänder att utöva tillbörlig aktsamhet vid hanteringen av nät och system.***

Förebygga radikalisering

Kommissionen fortsätter att genomföra många olika åtgärder som svar på radikalisering, i enlighet med meddelandet från juni 2016 om att stödja det förebyggande arbetet mot radikalisering som leder till våldsbejakande extremism[24], t.ex. främjande av en inkluderande utbildning och gemensamma värden, åtgärder för att motverka extremistisk propaganda på nätet och radikalisering i fängelser, ett stärkt samarbete med tredjeländer och mer forskning för att bättre förstå radikaliseringens utvecklingen och skapa bättre underlag för åtgärder. Nätverket för kunskapsspridning om radikalisering har haft en ledande roll i kommissionens arbete för att stödja medlemsstaterna på detta område och har samarbetat med aktörer på lokal nivå. Mer detaljer ges i den åttonde rapporten om framsteg i riktning mot en effektiv och verklig säkerhetsunion[25].

Radikalisering och hatpropaganda på nätet

I linje med den europeiska säkerhetsagendan[26] har kommissionen vidtagit åtgärder för att minska tillgången till olagligt innehåll på nätet, särskilt genom EU-enheten för anmälan av innehåll på internet vid Europol och EU:s internetforum[27]. Betydande framsteg har också gjorts inom ramen för uppförandekoden för att motverka olaglig hatpropaganda på nätet[28]. Mer detaljer ges i den åttonde rapporten om framsteg i riktning mot en effektiv och verklig säkerhetsunion[29]. Dessa åtgärder kommer att förstärkas, bland annat på grundval av slutsatserna från Europeiska rådet[30], G7-toppmötet[31] och G20-toppmötet i Hamburg[32].

[24] http://ec.europa.eu/dgs/education_culture/repository/education/library/publications/2016/communication-preventing-radicalisation_en.pdf
[25] COM(2017) 354 final
[26] För närmare upplysningar se den åttonde rapporten om framsteg i riktning mot en effektiv och verklig säkerhetsunion, COM(2017) 354 final.
[27] För närmare upplysningar se den åttonde rapporten om framsteg i riktning mot en effektiv och verklig säkerhetsunion, COM(2017) 354 final.
[28] Uppförandekod om olaglig hatpropaganda på nätet, 31 maj 2016, http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf
[29] För närmare upplysningar se den åttonde rapporten om framsteg i riktning mot en effektiv och verklig säkerhetsunion, COM(2017) 354 final.
[30] Slutsatser från Europeiska rådets möte den 22-23 juni 2017.
[31] G7-toppmötet i Taormina, Italien, 26–27 maj 2017.
[32] G20-toppmötet i Hamburg, Tyskland, 7-8 juli 2017.

Nätplattformar har en nyckelroll när det gäller att motverka olagligt eller skadligt innehåll. Såsom anges i halvtidsöversynen av strategin för den digitala inre marknaden[33] kommer kommissionen att säkerställa bättre samordning av plattformsdialogerna om mekanismer och tekniska lösningar för avlägsnande av olagligt innehåll. Där så är möjligt bör målet vara att basera dessa mekanismer på riktlinjer för olika aspekter, såsom anmälan och avlägsnande av olagligt innehåll. Kommissionen kommer också att tillhandahålla riktlinjer om ansvarsbestämmelser.

Ökat samarbete med tredjeländer

Åtgärd 18: ***Den höga representanten kommer, i samordning med kommissionen, att inleda en undersökning om hybridrisker i grannregionerna. Den höga representanten, kommissionen och medlemsstaterna kommer att använda de instrument som står till deras förfogande för att bygga upp partnerländernas kapacitet och öka deras resiliens mot hybridhot. GSFP-uppdrag, som antingen är oberoende eller kompletterar EU-instrument, skulle kunna utstationeras för att hjälpa partnerländerna att stärka sin kapacitet.***

EU har stärkt sitt fokus på att bygga upp kapacitet och resiliens i partnerländerna inom säkerhetssektorn, bl.a. genom att utgå från sambandet mellan säkerhet och utveckling, genom att utveckla säkerhetsdimensionen i den reviderade europeiska grannskapspolitiken och inleda dialoger om säkerhet och bekämpning av terrorism med länderna runt Medelhavet. I detta syfte inleddes en riskundersökning som ett pilotprojekt i samarbete med Republiken Moldavien. Dess syfte är att hjälpa till att fastställa landets viktigaste sårbara punkter och se till att EU:s stöd är särskilt inriktat på dessa områden. Resultaten av pilotprojektet visade att undersökningen i sig var användbar. Med utgångspunkt i de erfarenheter som gjorts kommer kommissionen och Europeiska utrikestjänsten att utfärda rekommendationer om att prioritera åtgärder för att bygga upp effektivitet, strategiska kommunikationer, skydd av kritisk infrastruktur och it-säkerhet.

Med utgångspunkt i denna första erfarenhet kan framöver ytterligare grannländer dra nytta av undersökningen, med anpassningar till olika nationella och lokala situationer och specifika hot och med undvikande av överlappning med pågående dialoger om säkerhet och terrorismbekämpning. Mer allmänt antog kommissionen och den höga representanten den 7 juni 2017 det gemensamma meddelandet En strategi för resiliens i EU:s yttre åtgärder[34]. Syftet är att stödja partnerländerna att bli mer resilienta mot dagens globala utmaningar. Meddelandet lyfter fram behovet av att övergå från krishantering till en mer strukturell, långsiktig strategi för att hantera sårbara punkter, med betoning på förutseende, förebyggande och beredskap.

Resiliens mot it-angrepp för utveckling

EU stöder länder utanför Europa i syfte att stärka resiliensen i deras informationsnät. Den ständigt ökande digitaliseringen har en inneboende säkerhetsaspekt som skapar särskilda globala utmaningar för resiliensen i informationsnätverk eftersom it-attacker är

[33]Se meddelandet från kommissionen, COM(2017) 228 final.
[34]Gemensamt meddelande till Europaparlamentet och rådet: En strategi för resiliens i EU:s yttre åtgärder, JOIN(2017) 21 final.

gränsöverskridande. EU stöder tredjeländer med att bygga upp deras förmåga att förebygga och reagera på oförutsedda fel och it-attacker. Efter ett pilotprojekt om it-säkerhet i f.d. jugoslaviska republiken Makedonien, Kosovo[35] samt Moldavien som slutfördes 2016, kommer kommissionen att lansera ett nytt program för perioden 2017–20 för att förbättra it-resiliensen i tredjeländer, främst i Afrika och Asien, men också i Ukraina. Syftet är att öka säkerheten och beredskapen hos kritisk infrastruktur och informationsnät i tredjeländer på grundval av ett myndighetsövergripande tillvägagångssätt, samtidigt som överensstämmelsen med de mänskliga rättigheterna och rättsstatsprincipen säkerställs.

Luftfartsskydd

Den civila luftfarten är fortfarande ett viktigt och symboliskt mål för terrorister och kan också bli mål för hybridhot. Medan EU har utvecklat ett robust luftfartsskydd kan flygningar från tredjeländer vara mer sårbara. I linje med FN:s säkerhetsråds resolution 2309 (2016) ökar kommissionen sina ansträngningar att bygga upp kapacitet i tredjeländer. I januari 2017 inledde kommissionen en ny integrerad riskbedömning för att prioritera och samordna insatser för kapacitetsuppbyggnad som genomförs på EU-nivå och i medlemsstaterna, samt med internationella partner. Kommissionen inledde 2016 ett fyraårigt projekt om civilt luftfartsskydd i Afrika och på Arabiska halvön i syfte att motverka terroristhotet mot den civila luftfarten. Projektet är inriktat på utbyte av sakkunskap mellan partnerstaterna och experter från medlemsstaterna i Europeiska civila luftfartskonferensen, mentorprogram, utbildning och handledning. Verksamheten kommer att utökas ytterligare under 2017.

c. FÖREBYGGANDE AV OCH ÅTGÄRDER VID KRISER SAMT ÅTERHÄMTNING

Även om konsekvenserna kan reduceras genom långsiktiga strategier på nationell nivå och EU-nivå är det av avgörande betydelse att på kort sikt förstärka medlemsstaternas och unionens förmåga att förebygga, vidta åtgärder mot och återhämta sig från hybridhot på ett snabbt och samordnat sätt. Det är av avgörande betydelse att vidta snabba åtgärder vid händelser som utlösts av hybridhot. Stora framsteg har gjorts på detta område under det senaste året, och ett operativt protokoll har nu införts i EU för krishantering vid en eventuell hybridattack. Regelbunden övervakning och övning kommer att äga rum framöver.

Åtgärd 19: Den höga representanten och kommissionen kommer, i samarbete med medlemsstaterna, att upprätta ett gemensamt operativt protokoll och genomföra regelbundna övningar för att förbättra kapaciteten för strategiskt beslutsfattande som svar på komplexa hybridhot på grundval av förfaranden för integrerad politisk krishantering.

I den gemensamma ramen rekommenderas inrättandet av mekanismer för snabba åtgärder vid händelser som utlösts av hybridhot för att samordna mellan EU:s responsmekanismer[36] och system för tidig varning. I detta syfte har kommissionen och Europeiska utrikestjänsten

[35] Denna beteckning påverkar inte ståndpunkter om Kosovos status och är i överensstämmelse med FN:s säkerhetsråds resolution 1244/99 och med Internationella domstolens utlåtande om Kosovos självständighetsförklaring.

[36] Rådets EU-arrangemang för integrerad politisk krishantering, kommissionens Argus-system och Europeiska utrikestjänstens krishantering.

utvecklat ett operativt protokoll för att motverka hybridhot (EU Playbook)[37] som beskriver formerna för samordning, informationsinsamling och analys, utarbetande av underlag till beslutsprocesser, övningar och utbildning samt samarbete med partnerorganisationer, särskilt Nato, vid hybridhot. På samma sätt har Nato utarbetat ett protokoll för ökad samverkan mellan EU och Nato för att förebygga och motverka hybridhot på områdena it-försvar, strategisk kommunikation, situationsmedvetenhet och krishantering. EU Playbook kommer att testas genom en övning under hösten 2017 som en del av Europeiska unionens parallella och samordnade övning, vilket inbegriper samverkan med Nato.

Åtgärd 20: Kommissionen och den höga representanten kommer, inom sina respektive behörighetsområden, att undersöka tillämpligheten och de praktiska konsekvenserna av artikel 222 i EUF-fördraget och artikel 42.7 i EU-fördraget om det inträffar en omfattande och allvarlig hybridattack.

Artikel 42.7 i EU-fördraget hänvisar till väpnat angrepp på en medlemsstats territorium, medan artikel 222 i EUF-fördraget (solidaritetsklausulen) hänvisar till terroristattacker eller naturkatastrofer eller katastrofer på en medlemsstats territorium. Det är mer sannolikt att den senare kommer till användning vid hybridattacker, som utgör en blandning av brottslig och samhällsundergrävande verksamhet. Åberopandet av solidaritetsklausulen utlöser en samordning på rådsnivå (EU:s arrangemang för integrerad politisk krishantering) och att relevanta EU-institutioner och organ, samt EU-program och mekanismer, involveras. Rådets beslut 2014/415/EU innehåller bestämmelser för unionens genomförande av solidaritetsklausulen. Dessa tillämpningsföreskrifter är fortfarande giltiga och det finns inte något behov av att se över rådets beslut. Om en hybridattack omfattar ett väpnat angrepp kan artikel 42.7 också åberopas. I ett sådant fall ska stödet och biståndet ges av såväl medlemsstaterna som EU. Kommissionen och den höga representanten kommer att fortsätta att utvärdera de mest effektiva sätten att bekämpa sådana attacker.

Antagandet av EU:s operativa protokoll, som nämns ovan, stöder direkt denna bedömning och kommer att ingå i Europeiska unionens parallella och samordnade övning i oktober 2017. Denna övning kommer att testa EU:s olika mekanismer och förmåga att interagera, med målet att påskynda beslutsfattandet när den förvirring som ett hybridhot utlöst leder till svårbedömda situationer.

Åtgärd 21: Den höga representanten kommer, i samordning med medlemsstaterna, att integrera, utnyttja och samordna den militära insatskapaciteten när det gäller att motverka hybridhot inom ramen för den gemensamma säkerhets- och försvarspolitiken.

Som ett resultat av arbetet med att integrera militär kapacitet till stöd för Gusp/GSFP, och efter ett seminarium med militära experter i december 2016 och vägledning av Europeiska unionens militära kommitténs arbetsgrupp i maj 2017, slutfördes riktlinjerna om EU:s militära bidrag till att motverka hybridhot inom ramen för den gemensamma säkerhets- och försvarspolitiken i juli 2017, och arbetet kommer att fortsätta genom programmet för genomförande av konceptutveckling.

[37] Arbetsdokument från kommissionens avdelningar SWD(2016) 227, som antogs den 7 juli 2016.

d. SAMARBETET MELLAN EU OCH NATO

***Åtgärd 22*: Den höga representanten kommer, i samordning med kommissionen, att fortsätta sin informella dialog och stärka samarbetet och samordningen med Nato i fråga om situationsmedvetenhet, strategisk kommunikation, it-säkerhet och ”krisförebyggande och krisåtgärder” i syfte att motverka hybridhot, samtidigt som principerna om delaktighet och varje organisations självständiga beslutsfattande respekteras.**

På grundval av den gemensamma förklaring som undertecknades av ordförandena för Europeiska rådet och Europeiska kommissionen, tillsammans med Natos generalsekreterare i Warszawa den 8 juli 2016, har EU och Nato utvecklat en gemensam uppsättning med 42 förslag att genomföra, som sedan godkändes i separata och parallella processer den 6 december 2016 av både EU och Nato[38]. I juni 2017 offentliggjorde den höga representanten och Natos generalsekreterare en rapport om hur arbetet med de 42 åtgärderna i den gemensamma förklaringen fortskrider. Att motverka hybridhot är ett av de sju samarbetsområden som anges i den gemensamma förklaringen och står för tio av de 42 åtgärderna. Rapporten visar att de gemensamma insatser som gjorts under det gångna året har lett till betydande resultat. Många av de specifika åtgärderna som syftar till att motverka hybridhot har redan nämnts, inbegripet det europeiska kompetenscentrumet för motverkande av hybridhot, bättre situationsmedvetenhet, inrättandet av EU:s gemensamma enhet för hybridhot och dess samspel med Natos nya sektion för hybridanalys och samarbetet mellan enheter för strategisk kommunikation. För första gången kommer personal från Nato och EU att tillsammans öva reaktioner på ett hybridscenario. Övningen förväntas att testa genomförandet av mer än en tredjedel av de gemensamma förslagen. EU kommer i år att genomföra sina egna parallella och samordnade övning och förbereder sig för att ta en ledande roll under 2018.

När det gäller resiliens har både EU och Nato engagerat sig i ömsesidiga briefingar, bland annat om EU:s mekanism för integrerad politisk krishantering. Regelbundna kontakter mellan Natos och EU:s personal, bland annat genom workshoppar, Nato eller deltagande i Europeiska försvarsbyråns styrelse har möjliggjort ett utbyte av information om Natos grundläggande krav på nationell resiliens. Ytterligare utbyten mellan kommissionen och Nato om främjande av resiliens planeras till hösten. Nästa lägesrapport om samarbetet mellan EU och Nato kommer att föreslå möjligheter till utökat samarbete mellan de båda organisationerna.

3. SLUTSATS

I den gemensamma ramen beskrivs åtgärder som syftar till att motverka hybridhot och stärka resiliensen på EU-nivå och nationell nivå samt för EU:s partner. Samtidigt som kommissionens och den höga representantens arbete i nära samarbete med medlemsstaterna och partner leder till resultat på alla områden är det viktigt att arbetet fortskrider för att möta pågående och ständigt föränderliga hybridhot. Medlemsstaterna har det primära ansvaret för att motverka hybridhot som rör nationell säkerhet och upprätthållande av lag och ordning. Den nationella resiliensen och kollektiva insatser för att skydda mot hybridhot måste ses som ömsesidigt förstärkande delar av samma övergripande arbete. Medlemsstaterna uppmanas därför att utföra undersökningar av hybridhot snarast möjligt eftersom de kommer att ge värdefull information om sårbarheten och beredskapen i hela EU. På grundval av de

[38] http://www.consilium.europa.eu/en/press/press-releases/2016/12/06-eu-nato-joint-declaration/

betydande framstegen med att öka medvetenheten bör potentialen hos EU:s gemensamma enhet för hybridhot maximeras. Den höga representanten uppmanar medlemsstaterna att stödja det arbete som utförs av Stratcom-arbetsgrupperna i syfte att på ett effektivare sätt motverka framväxten av hybridhot. EU kommer att stödja det finskledda Europeiska centrumet för motverkande av hybridhot fullt ut.

Den unika styrkan i EU:s insatser ligger i att bistå medlemsstater och partner med att bygga upp deras resiliens med hjälp av ett brett spektrum av befintliga instrument och program. Betydande framsteg har gjorts med åtgärder för att stärka resiliensen på områden som transport, energi, it-säkerhet, kritisk infrastruktur, skydd mot olaglig användning av det finansiella systemet och insatser för att motverka våldsbejakande extremism och radikalisering. EU:s insatser i arbetet med att bygga upp resiliens kommer att fortsätta eftersom hybridhotens karaktär utvecklas. EU kommer i synnerhet att utveckla indikatorer för att stärka den kritiska infrastrukturens skydd och resiliens mot hybridhot inom berörda sektorer.

Europeiska försvarsfonden får tillsammans med medlemsstaterna medfinansiera kapacitetsprioriteringar för att stärka resiliensen mot hybridhot. Det kommande lagstiftningspaketet för it-säkerhet samt sektorsövergripande åtgärder som syftar till att genomföra direktivet om nätverks- och informationstjänster kommer att tillhandahålla nya plattformar för att motverka hybridhot i hela EU.

Kommissionen och den höga representanten uppmanar medlemsstaterna och berörda parter att när så krävs snabbt komma överens om och säkerställa ett snabbt och effektivt genomförande av de många åtgärder som syftar till att stärka resiliensen som beskrivs i detta meddelande. EU kommer att bygga vidare på och fördjupa sitt givande samarbete med Nato.

Unionen är alltjämt fast besluten att mobilisera alla relevanta EU-instrument för att hantera komplexa hybridhot. Att stödja medlemsstaternas ansträngningar förblir en prioritering för unionen som agerar som en starkare och mer lyhörd säkerhetsgarant, i samarbete med sina viktiga partner.