EUROPEISKA KOMMISSIONEN

UNIONENS HÖGA REPRESENTANT FÖR UTRIKES FRÅGOR OCH SÄKERHETSPOLITIK

Bryssel den 6.4.2016
JOIN(2016) 18 final

GEMENSAMT MEDDELANDE TILL EUROPAPARLAMENTET OCH RÅDET

Gemensam ram för att motverka hybridhot

Europeiska unionens insatser

1. INLEDNING

Under de senaste åren har Europeiska unionens säkerhetsläge förändrats dramatiskt. Freden och stabiliteten i EU:s östra och södra grannskap är utsatt för stora utmaningar. Det visar på det fortsatta behovet av att anpassa och stärka unionens kapacitet att garantera säkerhet, med tydlig betoning på det nära sambandet mellan yttre och inre säkerhet. Många av dagens utmaningar när det gäller fred, säkerhet och välstånd härrör från instabilitet i EU:s omedelbara grannskap och från föränderliga hot. I sina politiska riktlinjer för 2014 framhöll Europeiska kommissionens ordförande Jean-Claude Juncker behovet av ”att arbeta för ett starkare Europa i frågor som rör säkerhet och försvar” och kombinera europeiska och nationella instrument på ett effektivare sätt än tidigare. Efter uppmaningen från rådet (utrikes frågor) av den 18 maj 2015 åtog sig den höga representanten i nära samarbete med kommissionens avdelningar och Europeiska försvarsbyrån (EDA), och i samråd med EU:s medlemsstater, att arbeta för att lägga fram en gemensam ram med genomförbara förslag som kan bidra till att motverka hybridhot och stärka resiliensen hos EU och medlemsstaterna, samt hos partnerländer[1]. I juni 2015 upprepade Europeiska rådet behovet av att mobilisera EU-instrument för att bidra till att bekämpa hybridhot[2].

Definitionen av hybridhot varierar och måste vara flexibel eftersom hotet hela tiden förändras. Begreppet syftar dock till att fånga upp den blandning av tvångsåtgärder och omstörtande verksamhet samt konventionella och okonventionella metoder (dvs. diplomatiska, militära, ekonomiska och tekniska) som statliga eller icke-statliga aktörer kan använda på ett samordnat sätt för att uppnå särskilda mål, samtidigt som de håller sig under tröskeln för en formell krigsförklaring. Tonvikten ligger vanligen på att utnyttja målets svagheter och skapa tvetydighet för att försvåra beslutsfattandet. Massiva desinformationskampanjer, där sociala medier används för att kontrollera den politiska beskrivningen eller radikalisera, rekrytera och leda proxyaktörer, kan fungera som verktyg för hybridhot.

I den mån motverkandet av hybridhot rör den nationella säkerheten och det nationella försvaret samt upprätthållandet av lag och ordning, ligger det främsta ansvaret hos medlemsstaterna, eftersom de nationella svagheterna fortsatt främst är landsspecifika. Många EU-medlemsstater står dock inför gemensamma hot, som också kan vara inriktade på gränsöverskridande nät eller infrastrukturer. Sådana hot kan hanteras mer effektivt genom samordnade insatser på EU-nivå, genom att EU:s politik och instrument används på grundval av europeisk solidaritet, ömsesidigt bistånd och ett utnyttjande av Lissabonfördragets fulla potential. EU:s politik och instrument kan spela en central roll när det gäller att bidra till att öka medvetenheten, och gör det redan i hög grad. Detta bidrar till att öka medlemsstaternas resiliens i fråga om att bemöta gemensamma hot. De yttre EU-åtgärder som föreslås i denna ram utgår från principerna i artikel 21 i fördraget om Europeiska unionen (EU-fördraget), bl.a. demokrati, rättsstaten, de mänskliga

[1] Rådets slutsatser om den gemensamma säkerhets- och försvarspolitiken (GSFP), maj 2015 [rådets dokument 8971/15].
[2] Europeiska rådets slutsatser, juni 2015 [EUCO 22/15].

rättigheternas universalitet och odelbarhet samt respekt för principerna i Förenta nationernas stadga och i folkrätten[3].

Detta gemensamma meddelande syftar till att underlätta en helhetssyn som syftar till att EU, i samordning med medlemsstaterna, specifikt ska kunna motverka hot som är hybrida till sin karaktär, genom att skapa synergier mellan alla relevanta instrument och främja nära samarbete mellan alla berörda aktörer[4]. Åtgärderna bygger på befintliga strategier och befintlig sektoriell politik som bidrar till att uppnå ökad säkerhet. Bland de verktyg som kan bidra till att motverka hybridhot kan särskilt nämnas den europeiska säkerhetsagendan[5], Europeiska unionens kommande strategi för utrikes- och säkerhetspolitik och den europeiska handlingsplanen på försvarsområdet[6], EU:s strategi för cybersäkerhet[7], den europeiska strategin för energitrygghet[8] och Europeiska unionens strategi för sjöfartsskydd[9].

Eftersom Nato också arbetar för att motverka hybridhot och rådet (utrikes frågor) föreslagit ett ökat samarbete och en ökad samordning på detta område, syftar vissa av förslagen till att förbättra samarbetet mellan EU och Nato när det gäller att motverka hybridhot.

De föreslagna insatserna är inriktade på att öka medvetenheten, bygga upp resiliensen, förebygga och reagera på kriser samt att återhämta sig efter kriser.

2. KÄNNA IGEN HYBRIDHOT

Hybridhot syftar till att utnyttja ett lands svagheter och avsikten är ofta att undergräva grundläggande demokratiska värden och friheter. Som ett första steg kommer den höga representanten och kommissionen att samarbeta med medlemsstaterna för att öka situationsmedvetenheten genom att övervaka och bedöma de risker som kan vara inriktade på EU:s svagheter. Kommissionen håller på att utarbeta metoder för säkerhetsriskanalys som ska bidra till att informera beslutsfattare och främja en riskbaserad utformning av politiken när det gäller allt ifrån flygsäkerhet till penningtvätt och finansiering av terrorism. En undersökning där medlemsstaterna identifierar de områden som är sårbara för hybridhot skulle också vara relevant. Syftet skulle vara att ta fram indikatorer för hybridhot, införliva dessa i system för tidig varning och de befintliga systemen för riskbedömning samt sprida dem på lämpligt sätt.

[3] Europeiska unionens stadga om de grundläggande rättigheterna är bindande för EU-institutionerna och för medlemsstaterna när de tillämpar unionsrätten.
[4] Eventuella lagförslag kommer att bli föremål för kommissionens krav på bättre lagstiftning, i linje med kommissionens riktlinjer för bättre lagstiftning, SWD(2015) 111.
[5] COM(2015) 185 final.
[6] Ska läggas fram under 2016.
[7] Ramen för EU:s politik för it-försvar [rådets dokument 15585/14] och det gemensamma meddelandet *EU:s strategi för cybersäkerhet: En öppen, säker och trygg cyberrymd*, från februari 2013 [JOIN(2013)1].
[8] Gemensamt meddelande om en europeisk strategi för energitrygghet, från maj 2014 **[**SWD(2014) 330].
[9] Det gemensamma meddelandet *För ett öppet och säkert globalt sjöbevakningsområde - inslag i en EU-strategi för sjöfartsskydd* – JOIN(2014) 9 final – av den 6 mars 2014.

<u>Åtgärd 1:</u> 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.

3. ORGANISERA EU:S INSATSER: ÖKA MEDVETENHETEN

3.1. EU:s gemensamma enhet för hybridhot

Det är av avgörande betydelse att EU, i samordning med medlemsstaterna, har en tillräcklig medvetenhet om situationen för att man ska kunna identifiera eventuella förändringar i säkerhetsläget i samband med hybridverksamhet som bedrivs av statliga och/eller icke-statliga aktörer. För att effektivt motverka hybridhot är det viktigt att förbättra informationsutbytet och främja utbyte av relevanta upplysningar mellan sektorer och mellan EU, dess medlemsstater och partnerländer.

EU:s gemensamma enhet för hybridhot kommer att kunna vara en central för analys av hybridhot, upprättad inom ramen för Europeiska unionens underrättelseanalyscentrum (EU Intcen) inom Europeiska utrikestjänsten. Enheten skulle ta emot, analysera och dela med sig av sekretessbelagd information och information från öppna källor som specifikt rör indikatorer och varningar avseende hybridhot från olika aktörer inom Europeiska utrikestjänsten (inklusive EU-delegationerna), kommissionen (med EU:s organ[10]) och medlemsstaterna. I samverkan med befintliga organ på EU-nivå[11] och nationell nivå skulle enheten analysera de externa aspekter av hybridhot som påverkar EU och dess grannskap, för att snabbt analysera incidenter och bidra med information till EU:s strategiska beslutsfattande, bl.a. genom att bidra till de säkerhetsriskbedömningar som utförs på EU-nivå. Resultaten av enhetens analyser skulle bearbetas och hanteras i enlighet med Europeiska unionens regler för sekretessbelagda uppgifter och skydd av dessa[12]. Enheten bör stå i förbindelse med befintliga organ på EU-nivå och nationell nivå. Medlemsstaterna bör inrätta nationella kontaktpunkter som står i kontakt med EU:s gemensamma enhet för hybridhot. Personal i och utanför EU (även de som utstationerats vid EU:s delegationer, insatser och uppdrag) och i medlemsstaterna bör också utbildas i att känna igen tidiga tecken på hybridhot.

<u>Åtgärd 2:</u> Inom ramen för den befintliga EU Intcen-strukturen inrätta EU:s gemensamma enhet för hybridhot som kan ta emot och analysera sekretessbelagd information och information från öppna källor om hybridhot. Medlemsstaterna uppmanas att upprätta nationella kontaktpunkter för hybridhot för att garantera samarbete och säker kommunikation med EU:s gemensamma enhet för hybridhot.

[10] I enlighet med deras mandat.
[11] T.ex. Europeiskt it-brottscentrum och Europeiskt centrum mot terrorism vid Europol, Frontex, EU:s incidenthanteringsorganisation (CERT-EU).
[12] Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995.

3.2. Strategisk kommunikation

De som ligger bakom hybridhot kan systematiskt sprida desinformation, bl.a. genom riktade kampanjer i sociala medier, i syfte att radikalisera personer, destabilisera samhället och kontrollera den politiska beskrivningen. Det är av avgörande betydelse att kunna bemöta hybridhot genom att använda en riktig strategi för **strategisk kommunikation**. Snabba reaktioner baserade på fakta och en höjning av den allmänna medvetenheten är viktiga faktorer för att öka samhällets resiliens.

I den strategiska kommunikationen bör de sociala medierna och de traditionella audiovisuella och internetbaserade medierna utnyttjas till fullo. Europeiska utrikestjänsten bör, med utgångspunkt i arbetsgrupperna East Stratcoms och Arab Stratcoms verksamhet, optimera användningen av lingvister som flytande behärskar relevanta icke-EU-språk och specialister på sociala medier som kan övervaka information från länder utanför EU och sörja för riktad kommunikation för att reagera på desinformation. Medlemsstaterna bör dessutom utarbeta samordnade mekanismer för strategisk kommunikation i syfte att stödja angivandet av källor och kampen mot desinformation i syfte att exponera hybridhot.

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.***

3.3. Kompetenscentrum för ”motverkande av hybridhot”

Utifrån erfarenheterna från vissa medlemsstater och partnerorganisationer[13] skulle ett multinationellt institut eller ett nätverk av sådana kunna fungera som ett kompetenscentrum för motverkande av hybridhot. Centrumet skulle kunna vara inriktat på att undersöka hur hybridstrategier har tillämpats, och uppmuntra utvecklingen av nya koncept och ny teknik inom den privata sektorn och näringslivet för att hjälpa medlemsstaterna att bygga upp sin resiliens. Undersökningarna skulle kunna bidra till att anpassa EU:s och medlemsstaternas strategier, doktriner och koncept till varandra, och till att garantera att beslutsfattandet också tar hänsyn till de svårigheter och tvetydigheter som hänger samman med hybridhot. Centrumet bör utarbeta program som syftar till att främja forskning och utveckla övningar som gör att man kan hitta praktiska lösningar på de utmaningar som hybridhoten innebär. Centrumet skulle förlita sig på den sakkunskap som utarbetats av dess medarbetare från olika länder och från den civila, militära, privata och akademiska sektorn.

Centrumet skulle kunna ha ett nära samarbete med EU:s[14] och Natos[15]befintliga kompetenscentrum för att kunna utnyttja den kunskap om hybridhot som vunnits genom

[13] Natos kompetenscentrum.
[14] T.ex. EU:s institut för säkerhetsstudier (EU ISS) och EU:s ämnesspecifika kompetenscentrum om CBRN-frågor.
[15] http://www.nato.int/cps/en/natohq/topics_68372.htm.

it-försvar, strategisk kommunikation, civil–militär samverkan, på energiområdet och i krishantering.

<u>Åtgärd 4:</u> Medlemsstaterna uppmanas att överväga att inrätta ett kompetenscentrum för att "motverka hybridhot".

4. ORGANISERA EU:S INSATSER: ÖKA RESILIENSEN

Resiliens är förmågan att stå emot stress och återhämta sig, stärkt av utmaningen. För att effektivt motverka hybridhot måste man åtgärda den centrala infrastrukturens, försörjningskedjornas och samhällets potentiella svagheter. Genom att utnyttja EU:s instrument och politik kan man öka resiliensen hos infrastruktur på EU-nivå.

4.1. Skydd av kritisk infrastruktur

Det är viktigt att skydda kritisk infrastruktur (t.ex. energiförsörjningskedjor, transport), eftersom en okonventionell attack mot "mjuka mål" från dem som ligger bakom hybridhot kan leda till allvarliga ekonomiska eller samhälleliga störningar. För att säkerställa skyddet av kritisk infrastruktur innehåller det europeiska programmet för skydd av kritisk infrastruktur[16] en systematisk sektorsöverskridande metod för alla typer av risker, inriktad på ömsesidiga beroenden, som bygger på genomförandet av verksamhet inom ramen för flödena för förebyggande och reaktivt arbete samt beredskapsarbete. I direktivet om europeisk kritisk infrastruktur[17] fastställs ett förfarande för identifiering och klassificering av europeisk kritisk infrastruktur och en gemensam metod för bedömning av behovet att stärka skyddet av denna. I synnerhet bör arbetet inom ramen för direktivet återupptas för att stärka resiliensen hos kritisk infrastruktur med anknytning till transport (t.ex. EU:s viktigaste flygplatser och handelshamnar). Kommissionen kommer att bedöma om gemensamma verktyg, bl.a. indikatorer, bör utarbetas för att öka den kritiska infrastrukturens resiliens mot hybridhot inom alla berörda sektorer.

<u>Åtgärd 5:</u> 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.

4.1.1. Energinät

Störningsfri produktion och distribution av energi är av avgörande betydelse för EU och omfattande strömavbrott kan orsaka skada. Centralt för att motverka hybridhot är en ytterligare diversifiering av EU:s energikällor, leverantörer och tillförselvägar i syfte att få en säkrare energiförsörjning med större resiliens. Kommissionen håller också på att utföra risk- och säkerhetsbedömningar (s.k. stresstest) av EU:s kraftstationer. För att få

[16] *Meddelande från kommissionen om ett europeiskt program för skydd av kritisk infrastruktur*, 12.12.2006, KOM(2006) 786 slutlig.

[17] Rådets direktiv 2008/114/EG av den 8 december 2008 om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna, EUT L 345, 23.12.2008.

till stånd en diversifiering av energikällorna håller arbetet inom strategin för energiunionen på att intensifieras. Exempelvis kan den södra gaskorridoren göra det möjligt för gas från området kring Kaspiska havet att nå Europa, medan det i norra Europa inrättas gasmarknadsplatser med flera leverantörer. Dessa exempel bör följas i Central- och Östeuropa samt i Medelhavsområdet, där en knutpunkt för gasleveranser håller på att utvecklas.[18] Den framväxande marknaden för flytande naturgas kommer också att bidra till uppnåendet av detta mål.

Kommissionen stöder utarbetandet och antagandet av strängast möjliga säkerhetsnormer för kärnmaterial och kärnanläggningar, vilket skulle öka resiliensen. Kommissionen uppmuntrar ett konsekvent införlivande och genomförande av direktivet om kärnsäkerhet[19], som innehåller bestämmelser om förebyggande av olyckor och begränsning av olyckornas följder, och av bestämmelserna i direktivet om grundläggande säkerhetsnormer[20] när det gäller internationellt samarbete om beredskap och åtgärder vid nödsituationer, särskilt mellan angränsande medlemsstater och med angränsande länder.

***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.**

4.1.2 Transportsäkerhet och säkerhet i försörjningskedjan

Transport är av avgörande betydelse för unionen. Hybridattacker på transportinfrastruktur (t.ex. flygplatser, vägar, hamnar och järnvägar) kan få allvarliga konsekvenser, och störa resor och leveranskedjor. Vid genomförandet av lagstiftning om luft- och sjöfartssäkerhet[21] utför kommissionen regelbundna kontroller[22] och avser att ta itu med framväxande hybridhot genom sitt arbete med landtransportsäkerhet. I detta sammanhang diskuteras en EU-ram inom den reviderade förordningen om luftfartssäkerhet[23], som ett led i luftfartsstrategin för Europa[24]. Dessutom behandlas hoten

[18] Vad gäller de framsteg som gjorts hittills, se *Tillståndet i energiunionen 2015* (COM(2015) 572 final.

[19] Rådets direktiv 2009/71/Euratom av den 25 juni 2009 om upprättande av ett gemenskapsramverk för kärnsäkerhet vid kärntekniska anläggningar, ändrat genom rådets direktiv 2014/87/Euratom av den 8 juli 2014.

[20] Rådets direktiv 2013/59/Euratom av den 5 december 2013 om fastställande av grundläggande säkerhetsnormer för skydd mot de faror som uppstår till följd av exponering för joniserande strålning, och om upphävande av direktiven 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom och 2003/122/Euratom.

[21] Europaparlamentets och rådets förordning (EG) nr 300/2008 av den 11 mars 2008 om gemensamma skyddsregler för den civila luftfarten och om upphävande av förordning (EG) nr 2320/2002; Kommissionens genomförandeförordning (EU) 2015/1998 av den 5 november 2015 om detaljerade bestämmelser för genomförande av de gemensamma grundläggande standarderna avseende luftfartsskydd; Europaparlamentets och rådets direktiv 2005/65/EG av den 26 oktober 2005 om ökat hamnskydd; Europaparlamentets och rådets förordning (EG) nr 725/2004 om förbättrat sjöfartsskydd på fartyg och i hamnanläggningar.

[22] Enligt EU:s lagstiftning ska kommissionen utföra inspektioner för att kontrollera att medlemsstaterna följer kraven i fråga om luft- och sjöfartssäkerhet. Detta inbegriper inspektioner av den behöriga myndigheten i medlemsstaten, samt inspektioner av flygplatser, hamnar, lufttrafikföretag och fartyg samt av enheter med ansvar för säkerhetsåtgärder. Kommissionens inspektioner syftar till att säkerställa att medlemsstaterna genomför EU-lagstiftningen fullt ut.

[23] Kommissionens förordning (EU) nr 2016/4 av den 5 januari 2016 om ändring av förordning (EG) nr 216/2008 vad gäller väsentliga miljöskyddskrav. Förordning (EG) nr 216/2008 av den 20 februari 2008

mot säkerheten till sjöss i Europeiska unionens strategi för sjöfartsskydd och dess handlingsplan[25]. Detta gör det möjligt för EU och dess medlemsstater att på ett heltäckande sätt ta itu med utmaningar på sjöfartsskyddsområdet, däribland hybridhot, genom ett sektorsövergripande samarbete mellan civila och militära aktörer där syftet är att skydda kritisk sjöfartsinfrastruktur, den globala leverantörskedjan, sjöfartshandeln samt marina natur- och energiresurser. Säkerheten i den internationella försörjningskedjan behandlas också i Europeiska unionens strategi och handlingsplan för riskhantering på tullområdet[26].

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 handlingsplan 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.***

4.1.3 Rymden

Hybridhot kan riktas mot rymdinfrastruktur med sektorsövergripande följder. EU har utformat stödramen för rymdövervakning och spårning[27] för att koppla samman sådana tillgångar som ägs av medlemsstaterna i syfte att tillhandahålla rymdövervaknings- och spårningstjänster[28] till identifierade användare (medlemsstater, EU-institutioner, ägare och operatörer av rymdfarkoster och civilskyddsmyndigheter). I samband med den kommande rymdstrategin för Europa kommer kommissionen att undersöka möjligheten att vidareutveckla denna ram i syfte att övervaka hybridhot mot rymdinfrastruktur.

Satellitkommunikation är en viktig tillgång för krishantering, katastrofinsatser, polis, gränsbevakning och kustbevakning. De utgör ryggraden i storskalig infrastruktur som transporter, rymdfart eller fjärrstyrda luftfartygssystem. I enlighet med Europeiska rådets uppmaning om att utarbeta nästa generation av statlig satellitkommunikation håller kommissionen, i samarbete med Europeiska försvarsbyrån, på att utvärdera olika sätt att samla efterfrågan, mot bakgrund av den kommande rymdstrategin och europeiska handlingsplanen på försvarsområdet.

---

om fastställande av gemensamma bestämmelser på det civila luftfartsområdet och inrättande av en europeisk byrå för luftfartssäkerhet.

[24] Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén och Regionkommittén *En luftfartsstrategi för Europa*, COM(2015)0598 final, 7.12.2015.

[25] I december 2014 antog rådet en handlingsplan för att genomföra EU:s strategi för sjöfartsskydd; http://ec.europa.eu/maritimeaffairs/policy/maritime-security/doc/20141216-action-plan_en.pdf

[26] Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén och Regionkommittén om *EU:s strategi och handlingsplan för riskhantering på tullområdet: Hantera risker, stärka säkerheten i leveranskedjan och underlätta handeln*, COM (2014) 527 final.

[27] Se Europaparlamentets och rådets beslut 541/2014/EU.

[28] T.ex. varningar för att undvika kollisioner i omloppsbana, för att rymdföremål ska falla sönder eller kollidera, samt för riskfyllda återinträden av rymdföremål i jordens atmosfär.

Många kritiska infrastrukturer är beroende av exakta tidsuppgifter för att synkronisera sina nät (t.ex. energi- och telekommunikationsinfrastruktur) eller tidsstämplingstransaktioner (t.ex. finansmarknader). Beroendet av en enda tidssynkroniseringssignal från det globala systemet för satellitnavigering innebär att den resiliens som krävs för att motverka hybridhot saknas. Det europeiska globala systemet för satellitnavigering (Galileo) skulle erbjuda en andra tillförlitlig källa för tidsbestämning.

Åtgärd 8: ***Inom ramen för den kommande rymdstrategin och 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***.

4.2. Försvarskapacitet

Försvarskapaciteten behöver stärkas för att öka EU:s resiliens mot hybridhot. Det är viktigt att identifiera de centrala kapacitetsområdena, t.ex. övervaknings- och spaningskapacitet. Europeiska försvarsbyrån skulle kunna vara en katalysator för militär kapacitetsutveckling, t.ex. genom att förkorta utvecklingscykler för försvarskapacitet, investera i teknik, system och prototyper och öppna upp försvarsföretag för innovativ kommersiell teknik med anknytning till hybridhot. Möjliga åtgärder skulle kunna granskas inom ramen för den kommande handlingsplanen på försvarsområdet.

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.***

4.3. Skydd av folkhälsan och livsmedelstrygghet

Manipulation av överförbara sjukdomar eller kontaminering av föda, mark, luft eller dricksvatten med kemiska, biologiska, radiologiska eller nukleära ämnen (CBRN) skulle kunna äventyra befolkningens hälsa. Dessutom kan avsiktlig spridning av djur- eller växtsjukdomar få allvarliga följder för livsmedelstryggheten i EU och stora ekonomiska och sociala effekter på viktiga områden i EU:s livsmedelskedja. EU:s befintliga strukturer för hälsosäkerhet, miljöskydd och livsmedelstrygghet kan användas för att reagera på hybridhot med användning av dessa metoder.

Inom ramen för EU:s lagstiftning om gränsöverskridande hot mot hälsan[29] samordnas beredskapen inför allvarliga gränsöverskridande hot mot hälsan genom befintliga

[29] Europaparlamentets och rådets beslut nr 1082/2013/EU av den 22 oktober 2013 om allvarliga gränsöverskridande hot mot människors hälsa och om upphävande av beslut nr 2119/98/EG, EUT L 293, 5.11.2013, s. 1.

mekanismer, där medlemsstater, EU-organ och vetenskapliga kommittéer[30] kopplas samman genom systemet för tidig varning och reaktion. Hälsosäkerhetskommittén, som samordnar medlemsstaternas insatser vid hot, kan sätta fokus på svagheter när det gäller folkhälsa[31] samt se till att riktlinjerna för kommunikation vid kriser och de krissimuleringsövningar med medlemsstaterna som syftar till att bygga upp kapaciteten även omfattar hybridhot (särskilt bioterrorism). När det gäller livsmedelstrygghet utbyter de behöriga myndigheterna information för riskanalys genom systemet för snabb varning för livsmedel och foder (RASFF) och det gemensamma riskhanteringssystemet (CRMS) på tullområdet i syfte att övervaka de hälsorisker som kontaminerade livsmedel innebär. I fråga om djurhälsa kommer översynen av EU:s rättsliga ram[32] att tillföra nya element till den befintliga ”verktygslådan” [33] för att öka beredskapen även inför hybridhot.

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

4.4. It-säkerhet

Det sammankopplade och digitaliserade samhället är till stor nytta för EU. It-angrepp kan störa digitala tjänster i hela EU och sådana attacker skulle kunna användas av dem som ligger bakom hybridhot. Det är viktigt att öka resiliensen i kommunikations- och informationssystemen i Europa för att stödja den digitala inre marknaden. EU:s strategi för cybersäkerhet och den europeiska säkerhetsagendan ger den övergripande strategiska ramen för EU:s initiativ om it-säkerhet och it-brottslighet. EU har haft en aktiv roll när det gäller att utveckla medvetenhet, samarbetsmekanismer och insatser inom ramen för strategin för cybersäkerhet. I det föreslagna it-säkerhetsdirektivet[34] behandlas it-säkerhetsriskerna för en lång rad väsentliga tjänsteleverantörer på områdena energi, transport, finanser och hälso- och sjukvård. Dessa leverantörer, samt leverantörer av viktiga digitala tjänster (t.ex. datormoln), bör vidta lämpliga säkerhetsåtgärder och rapportera allvarliga incidenter till de nationella myndigheterna, och notera om det kan röra sig om hybridhot. När direktivet har antagits av medlagstiftarna skulle ett effektivt införlivande och genomförande av detta främja it-säkerhetskapaciteten i medlemsstaterna och stärka deras samarbete kring it-säkerhet genom utbyte av information och bästa

[30] Kommissionens beslut C(2015) 5383 av den 7 augusti 2015 om inrättande av vetenskapliga kommittéer på området för folkhälsa, konsumentsäkerhet och miljö.
[31] I enlighet med Europaparlamentets och rådets beslut nr 1082/2013/EU av den 22 oktober 2013 om allvarliga gränsöverskridande hot mot människors hälsa och om upphävande av beslut nr 2119/98/EG, EUT L 293, s. 1.
[32] Europaparlamentets och rådets förordning (EU) 2016/429 av den 9 mars 2016 om överförbara djursjukdomar och om ändring och upphävande av vissa akter med avseende på djurhälsa (”djurhälsolag”), EUT L 84, 31.3.2016. När det gäller Europaparlamentets och rådets förordning om skyddsåtgärder mot växtskadegörare nådde Europaparlamentet och rådet en politisk överenskommelse om texten den 16 december 2015.
[33] T.ex. EU:s vaccinbanker, sofistikerade elektroniska system för information om djursjukdomar, ökade krav på åtgärder av laboratorier och andra organisationer som sysslar med patogener.
[34] Kommissionens förslag till Europaparlamentets och rådets direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen, COM(2013) 48 final, 7.2.2013. Rådet och Europaparlamentet har nått politisk enighet om det föreslagna direktivet och direktivet borde antas formellt inom kort.

praxis när det gäller att motverka hybridhot. I direktivet föreskrivs inrättandet av ett nätverk av 28 nationella it-incidentcentrum (CSIRT) och av en incidenthanteringsorganisation (Cert-EU)[35] som ska fortsätta det operativa samarbetet på frivillig basis.

För att uppmuntra offentlig-privat samarbete och EU-omfattande strategier för it-säkerhet har kommissionen inrättat plattformen för nät- och informationssäkerhet, som utfärdar riktlinjer med bästa praxis för riskhantering. Medan medlemsstaterna fastställer säkerhetskrav och förfaranden för att anmäla nationella incidenter, uppmuntrar kommissionen en hög konvergens i fråga om riskhanteringsstrategier, särskilt med stöd av Europeiska unionens byrå för nät- och informationssäkerhet (Enisa).

<u>Åtgärd 11:</u> Kommissionen uppmuntrar medlemsstaterna att inrätta och fullt ut utnyttja ett nätverk mellan de 28 it-incidentcentrumen och Cert-EU, 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.

4.4.1. Industrin

Ökad användning av molntjänster och stordata har ökat sårbarheten inför hybridhot. Strategin för den digitala inre marknaden föreskriver ett avtalsbaserat offentligt-privat partnerskap för it-säkerhet[36] som ska inriktas på forskning och innovation, och hjälpa unionen att upprätthålla en hög teknisk kapacitet inom detta område. Det avtalsbaserade offentlig-privata partnerskapet kommer att bygga upp förtroende hos olika marknadsaktörer och utveckla synergier mellan tillgångs- och efterfrågesidan. Även om det avtalsbaserade offentlig-privata partnerskapet och de kompletterande åtgärderna främst kommer att inriktas på civila produkter och tjänster för it-säkerhet, bör resultatet av dessa initiativ göra det möjligt för teknikanvändare att skydda sig bättre mot hybridhot.

<u>Åtgärd 12:</u> 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.

4.4.2. Energi

Uppkomsten av smarta hem och apparater och utvecklingen av smarta nät samt den ökande digitaliseringen av energisystemen leder också till en ökad sårbarhet för it-

[35] EU-institutionernas incidenthanteringsorganisation (Cert-EU).
[36] Ska inledas i mitten av 2016.

attacker. Den europeiska strategin för energitrygghet[37] och strategin för energiunionen[38] stöder en strategi som tar hänsyn till alla risker, med resiliens mot hybridhot som en naturlig del. Det tematiska nätverket för skydd av kritisk energiinfrastruktur främjar samarbete mellan aktörer inom energisektorn (olja, gas och el). Kommissionen har lanserat en webbaserad plattform för att analysera och utbyta information om hot och incidenter[39]. Tillsammans med de berörda parterna[40] är den också i färd med att utarbeta en övergripande strategi för energisektorn när det gäller it-säkerhet i driften av smarta nät, i syfte att minska sårbarheten. Även om elmarknaderna blir allt mer integrerade är reglerna och förfarandena för hur man ska hantera krissituationer fortfarande nationella. Vi måste se till att myndigheterna samarbetar för att förbereda sig inför och förebygga och begränsa risker, och att alla berörda aktörer agerar utifrån gemensamma regler.

***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.*

4.4.3. Säkerställande av sunda finansiella system

För att EU:s ekonomi ska fungera krävs ett säkert finansiellt system och betalningssystem. Det är mycket viktigt att det finansiella systemet och dess infrastruktur skyddas mot it-attacker, oavsett vem som ligger bakom attacken och vilket motivet är. För att bekämpa hybridhot mot EU:s finansiella tjänster måste branschen förstå hotet, ha testat sina försvarssystem och ha den teknik som krävs för att skydda branschen mot angrepp. Det är därför av avgörande betydelse att aktörerna på finansmarknaden, relevanta myndigheter och viktiga leverantörer eller kunder utbyter information om hot, men utbytet måste vara säkert och uppfylla kraven på skydd av personuppgifter. I linje med arbetet i internationella forum, bl.a. G7:s arbete inom denna sektor, kommer kommissionen att försöka identifiera vilka faktorer som hindrar ett lämpligt utbyte av information om hot och föreslå lösningar. Det är viktigt att sörja för en regelbunden testning och finjustering av protokollen för skydd av företag och relevant infrastruktur, vilket inbegriper en kontinuerlig uppgradering av teknik som ökar säkerheten.

***Åtgärd 14:** I samarbete med Enisa[41], 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.*

[37] Meddelande från kommissionen till Europaparlamentet och rådet: *Europeisk strategi för energitrygghet* – COM(2014)0330 final.
[38] Meddelandet En ramstrategi för en motståndskraftig energiunion med en framåtblickande klimatpolitik, COM(2015)080 final.
[39] Incident and Threat Information Sharing EU Centre – ITIS.
[40] Inom ramen för Energy Expert CyberSecurity Platform (EECSP).
[41] Europeiska unionens byrå för nät- och informationssäkerhet.

4.4.4. Transporter

Moderna transportsystem (järnväg, väg, flyg, sjöfart) är beroende av informationssystem som är sårbara för it-attacker. Med tanke på den gränsöverskridande dimensionen har EU en särskild roll. Kommissionen kommer tillsammans med medlemsstaterna att fortsätta att analysera it-hot och risker i samband med olagliga störningar av transportsystem. Kommissionen håller på att utveckla en färdplan om it-säkerhet för luftfarten i samarbete med Europeiska byrån för luftfartssäkerhet (Easa)[42]. It-hot mot säkerheten till sjöss behandlas också i Europeiska unionens strategi för sjöfartsskydd och dess handlingsplan.

<u>Åtgärd 15:</u> 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.

4.5. Åtgärder mot finansiering av hybridhot

De som ligger bakom hybridhot behöver finansiering för att kunna fortsätta med sin verksamhet. Finansieringen kan användas för att stödja terroristgrupper eller mer subtila former av destabiliserande verksamhet, t.ex. att stödja påtryckningsgrupper och extrema politiska partier. EU har stärkt sina insatser mot brottslighet och finansiering av terrorism, i enlighet med den europeiska säkerhetsagendan, särskilt handlingsplanen[43]. Den reviderade Europeiska ramen mot penningtvätt stärker kampen mot finansiering av terrorism och penningtvätt, underlättar de nationella finansunderrättelseenheternas (FIU) arbete med att identifiera och spåra misstänkta penningöverföringar och informationsutbyten, och säkerställer samtidigt möjligheten att spåra överföringar av medel i Europeiska unionen. Den kan därför också bidra till att motverka hybridhot. När det gäller Gusp-instrumenten skulle man kunna undersöka möjligheten att använda skräddarsydda och verkningsfulla restriktiva åtgärder för att motverka hybridhot.

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

4.6. Stärkt resiliens mot radikalisering och våldsbejakande extremism

Även om terrorism och våldsbejakande extremism inte i sig är av hybrid karaktär kan de som ligger bakom hybridhot inrikta sig på och rekrytera sårbara samhällsmedlemmar och radikalisera med hjälp av moderna kommunikationskanaler (bl.a. sociala medier på internet och proxygrupper) och propaganda.

---

[42] Den nya Easa-förordningen är för närvarande föremål för en diskussion mellan Europaparlamentet och rådet på grundval av kommissionens förslag från december 2015. Förslag till Europaparlamentets och rådets förordning om fastställande av gemensamma bestämmelser på det civila luftfartsområdet och inrättande av Europeiska unionens byrå för luftfartssäkerhet, och om upphävande av Europaparlamentets och rådets förordning (EG) nr 216/2008, COM(2015) 613 final, 2015/0277 (COD).

[43] Meddelande från kommissionen till Europaparlamentet och rådet om *en handlingsplan för att stärka kampen mot finansiering av terrorism* – COM(2016) 50 final.

I syfte att ta itu med extremistiskt innehåll på internet är kommissionen – inom ramen för strategin för den digitala inre marknaden – i färd med att analysera det potentiella behovet av nya åtgärder, med hänsyn till deras inverkan på den grundläggande rätten till yttrandefrihet och informationsfrihet. Detta skulle kunna inbegripa strikta förfaranden för att ta bort olagligt innehåll, samtidigt som man undviker att avlägsna lagligt innehåll (”anmälning och åtgärder”), samt att mellanhänder får ett större ansvar och måste utöva tillbörlig aktsamhet vid hanteringen av sina nät och system. Detta skulle komplettera den befintliga frivilliga modellen, där internetföretag och företag inom sociala medier (särskilt inom ramen för EU:s internetforum), i samarbete med Europols EU-enhet för anmälan av innehåll på internet, snabbt avlägsnar terroristpropaganda.

Inom ramen för den europeiska säkerhetsagendan motarbetas radikalisering genom utbyte av erfarenheter och utarbetande av bästa praxis, vilket inbegriper samarbete i tredjeländer. Syftet med den rådgivande gruppen för strategisk kommunikation om Syrien är att stärka utvecklingen och spridningen av alternativa budskap för att motverka terroristpropaganda. EU:s nätverk för kunskapsspridning om radikalisering stöder medlemsstater och rättstillämpare som måste kunna interagera med radikaliserade personer (bl.a. utländska terroriststridande) eller med personer som bedöms vara känsliga för radikalisering. Nätverket för kunskapsspridning om radikalisering tillhandahåller utbildning och rådgivning och kommer att stödja prioriterade tredjeländer, som är villiga att engagera sig. Kommissionen håller också på att främja ett rättsligt samarbete mellan olika straffrättsliga aktörer, bl.a. Eurojust, för att bekämpa terrorism och radikalisering i medlemsstaterna, vilket inbegriper hantering av utländska terroriststridande och återvändande.

Som ett komplement till ovannämnda strategier bidrar EU i sina **yttre åtgärder** till att motverka våldsbejakande extremism, bl.a. genom externt engagemang och deltagande, genom förebyggande åtgärder (motverkande av radikalisering och terroristfinansiering) och genom åtgärder för att ta itu med de bakomliggande ekonomiska, politiska och samhälleliga faktorer som skapar en grogrund för terroristgrupper.

<u>Åtgärd 17:</u> 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.

4.7. Ökat samarbete med tredjeländer

Såsom betonas i den europeiska säkerhetsagendan har EU stärkt sitt fokus på kapacitetsuppbyggnad i **partnerländer** inom säkerhetssektorn, bl.a. genom att bygga på kopplingen mellan säkerhet och utveckling och genom att utveckla säkerhetsdimensionen

i den reviderade europeiska grannskapspolitiken[44]. Dessa åtgärder kan också främja partnernas förmåga att stå emot hybridverksamhet.

Kommissionen avser att ytterligare intensifiera utbytet av operativ och strategisk information med utvidgningsländerna och inom det östliga partnerskapet och södra grannskapet, i syfte att bidra till kampen mot organiserad brottslighet, terrorism, irreguljär migration och smuggling av handeldvapen. När det gäller terrorismbekämpning håller EU på att intensifiera samarbetet med tredjeländer genom att uppgradera säkerhetsdialogerna och handlingsplanerna.

EU:s externa finansieringsinstrument syftar till att bygga upp fungerande och ansvariga institutioner i tredjeländer[45], vilket är en förutsättning för en effektiv bekämpning av säkerhetshot och stärkning av resiliensen. Viktiga verktyg i detta sammanhang är reform av säkerhetssektorn och kapacitetsuppbyggnad till stöd för säkerhet och utveckling[46]. Inom ramen för instrumentet som bidrar till stabilitet och fred[47] har kommissionen tagit fram insatser för att stärka resiliensen mot it-hot och partnernas förmåga att upptäcka och vidta åtgärder mot it-angrepp och it-brottslighet. Dessa insatser kan motverka hybridhot i tredjeländer. EU finansierar kapacitetsuppbyggnad i partnerländer för att minska säkerhetsriskerna i samband med kemiska, biologiska, radiologiska och nukleära frågor[48].

I linje med den övergripande strategin för krishantering skulle medlemsstaterna kunna använda instrument och uppdrag inom den gemensamma säkerhets- och försvarspolitiken (GSFP), som antingen är oberoende eller kompletterar redan utnyttjade EU-instrument, för att hjälpa partnerländerna att stärka sin kapacitet. De åtgärder som skulle kunna övervägas är i) stöd till strategisk kommunikation, ii) rådgivning till centrala ministerier som är utsatta för hybridhot och iii) kompletterande stöd till gränsförvaltning i nödsituationer. Man skulle kunna undersöka möjligheterna till ytterligare synergier mellan GSFP-instrument och aktörer på säkerhets- och tullområdet samt på det rättsliga

[44] Gemensamt meddelande till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén – *Översyn av den europeiska grannskapspolitiken*, 18.11.2015, JOIN(2015) 50 final.

[45] Se föregående. Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén – *EU:s utvidgningsstrategi*, 10.11.2015, COM(2015) 611 final. Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén – *Att göra EU:s utvecklingspolitik mer effektiv: en agenda för förändring*, 13.10.2011, COM(2011) 637 final.

[46] Gemensamt meddelande till Europaparlamentet och rådet – *Kapacitetsuppbyggnad till stöd för säkerhet och utveckling – möjliggöra för partnerländerna att förebygga och hantera kriser* (JOIN(2015)17 final).

[47] Europaparlamentets och rådets förordning (EU) nr 230/2014 av den 11 mars 2014 om inrättande av ett instrument som bidrar till stabilitet och fred, EUT L 77, 15.3.2014, s. 1.

[48] Till de berörda områdena hör gränsövervakning, krishantering, omedelbara insatser, olaglig handel, exportkontroll av produkter med dubbla användningsområden, övervakning och kontroll av sjukdomar, nukleär kriminalteknik, återhämtning efter incidenter och skydd av högriskanläggningar. Tredjeländer kan få del av bästa praxis som härrör från redskap som utvecklats inom ramen för EU:s CBRN-handlingsplan, t.ex. det europeiska utbildningscentrumet för kärnsäkerhet och EU:s deltagande i den internationella arbetsgruppen för gränsövervakning.

området, bl.a. berörda EU-organ[49], Interpol och Europeiska gendarmeristyrkan, i enlighet med deras mandat.

<u>Åtgärd 18:</u> 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 resiliensen mot hybridhot. GSFP-uppdrag, som antingen är oberoende eller kompletterar EU-instrument, skulle kunna utstationeras för att hjälpa partnerländerna att stärka sin kapacitet.

5. FÖREBYGGANDE AV OCH ÅTGÄRDER VID KRISER SAMT ÅTERHÄMTNING

I enlighet med avsnitt 3.1 är syftet med den föreslagna gemensamma enheten för hybridhot att analysera indikatorer för att förebygga och vidta åtgärder mot hybridhot och informera EU:s beslutsfattare. Även om svagheter kan åtgärdas 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. I detta avseende kan de insatser som Europeiska centrumet för samordning av katastrofberedskap[50] gör för att underlätta nationella civilskyddsåtgärder och stärka den nationella civilskyddskapaciteten vara en effektiv mekanism för att bemöta hybridhot som kräver civilskyddsinsatser. Detta skulle kunna ske i samverkan med andra EU-mekanismer och system för tidig varning, särskilt med Europeiska utrikestjänstens lägescentral när det gäller externa säkerhetsdimensioner och Centrumet för strategisk analys och insatskapacitet när det gäller den inre säkerheten.

Solidaritetsklausulen (artikel 222 i EUF-fördraget) gör det möjligt för unionen att vidta åtgärder, och möjliggör även åtgärder mellan medlemsstaterna, om en medlemsstat utsätts för en terroristattack eller drabbas av en naturkatastrof eller en katastrof som orsakas av människor. Unionens insatser för att bistå medlemsstaten genomförs genom tillämpning av rådets beslut 2014/415/EU[51]. Samordningsåtgärder inom rådet bör bygga på EU-arrangemangen för integrerad politisk krishantering[52]. Inom ramen för dessa arrangemang identifierar kommissionen och den höga representanten (inom sina respektive behörighetsområden) relevanta unionsinstrument och lägger fram förslag till rådet om beslut om undantagsåtgärder.

Artikel 222 i EUF-fördraget berör också situationer som inbegriper direkt stöd från en eller flera medlemsstater till en medlemsstat som har utsatts för en terroristattack eller en

[49] Europol, Frontex, Cepol, Eurojust.
[50] http://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en.
[51] Rådets beslut 2014/415/EU om närmare bestämmelser för unionens genomförande av solidaritetsklausulen (EUT L 192, 1.7.2014, s. 53).
[52] http://www.consilium.europa.eu/en/documents-publications/publications/2014/eu-ipcr/.

katastrof. Rådets beslut 2014/415/EU är inte tillämpligt i detta avseende. Med tanke på den tvetydighet som är associerad med hybridverksamhet bör kommissionen och den höga representanten (inom sina respektive behörighetsområden) bedöma om solidaritetsklausulen ska tillämpas som en sista utväg, om en EU-medlemsstat utsätts omfattande hybridhot.

Om flera allvarliga hybridhot utgör ett väpnat angrepp mot en EU-medlemsstat skulle artikel 42.7 i EU-fördraget, snarare än artikel 222 i EUF-fördraget, kunna åberopas för att lämpliga åtgärder ska kunna vidtas i tid. Omfattande och allvarliga hybridhot kan också kräva ökat samarbete och ökad samordning med Nato.

När de förbereder sina stridskrafter uppmanas medlemsstaterna att ta hänsyn till potentiella hybridhot. För att snabbt och effektivt kunna fatta beslut vid hybridangrepp måste medlemsstaterna genomföra regelbundna övningar, på operativ och politisk nivå, för att testa den nationella och multinationella beslutsförmågan. Målet skulle vara att medlemsstaterna, kommissionen och den höga representanten upprättar ett gemensamt operativt protokoll, med en beskrivning av effektiva förfaranden som ska tillämpas vid hybridhot, från den ursprungliga identifieringsfasen till den slutliga angreppsfasen, och en kartläggning av rollen för varje institution och aktör i processen.

En viktig del av GSFP-åtgärderna skulle kunna vara att tillhandahålla a) civil och militär utbildning, b) mentorskaps- och rådgivningsuppdrag som syftar till att förbättra säkerhets- och försvarskapaciteten hos en stat som utsätts för hot, c) beredskapsplanering för att identifiera tecken på hybridhot och stärka resurserna för tidig varning, d) stöd till förvaltningen av gränskontroller i nödfall, och e) stöd inom specialområden, t.ex. begränsning av CBRN-risker och icke-militär evakuering.

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.***

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.***

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.***

6. ÖKAT SAMARBETE MED NATO

Hybridhot utgör en utmaning inte bara för EU utan också för andra viktiga partnerorganisationer som Förenta nationerna (FN), Organisationen för säkerhet och

samarbete i Europa (OSSE) och i synnerhet Nato. Effektiva insatser kräver dialog och samordning på både politisk och operativ nivå mellan organisationerna. En närmare samverkan mellan EU och Nato skulle förbättra båda organisationernas förmåga att förbereda sig inför och vidta åtgärder mot hybridhot på ett effektivt, kompletterande och ömsesidigt stödjande sätt på grundval av principen om delaktighet, samtidigt som varje organisations beslutsautonomi och regler om uppgiftsskydd respekteras.

De båda organisationerna har gemensamma värderingar och står inför liknande problem. EU:s medlemsstater och de allierade i Nato förväntar sig att deras respektive organisation ska stödja dem och agera snabbt, beslutsamt och samordnat vid kriser, eller helst hindra kriser från att inträffa. Ett antal områden för närmare samarbete och samordning mellan EU och Nato har identifierats, bl.a. situationsmedvetenhet, strategisk kommunikation, it-säkerhet samt krisförebyggande och krisåtgärder. Den pågående informella dialogen mellan EU och Nato om hybridhot bör stärkas för att synkronisera de två organisationernas verksamhet på detta område.

För att EU:s och Natos insatser ska komplettera varandra är det viktigt att de båda organisationerna har samma bild av läget före och under kriser. Detta skulle kunna åstadkommas genom ett regelbundet utbyte av analyser och erfarenheter, men också genom direkta kontakter mellan EU:s gemensamma enhet för hybridhot och Natos motsvarande enhet. Lika viktigt är att bygga upp en ömsesidig förståelse av organisationernas respektive krishanteringsförfaranden för att sörja för snabba och effektiva insatser. Resiliensen skulle kunna förstärkas genom att man sörjer för komplementaritet vid fastställandet av riktmärken för kritiska delar av organisationernas infrastruktur, och genom ett nära samarbete om strategisk kommunikation och it-försvar. Gemensamma övningar på både politisk och teknisk nivå som är helt öppna för båda organisationer skulle kunna effektivisera beslutsfattandet i båda organisationer. Genom att undersöka ytterligare utbildningsmöjligheter skulle man bidra till att utveckla en jämförbar kompetensnivå på kritiska områden.

<u>Åtgärd 22:</u> 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.

7. SLUTSATSER

I detta gemensamma meddelande beskrivs åtgärder som syftar till att motverka hybridhot och stärka resiliensen på EU-nivå och nationell nivå, samt för EU:s partner. Eftersom fokus ligger på att **öka medvetenheten**, föreslås det att man inrättar särskilda mekanismer för informationsutbyte med medlemsstaterna och att man samordnar EU:s kapacitet att tillhandahålla strategisk kommunikation. Åtgärder har utarbetats 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. På vart och ett av dessa områden kommer ett viktigt första steg att vara att EU och medlemsstaterna genomför de strategier som beslutats, och att medlemsstaternas fullt ut genomför befintlig lagstiftning, medan en del mer konkreta insatser har förslagits för att ytterligare intensifiera dessa ansträngningar.

När det gäller **förebyggande av, åtgärder mot och återhämtning efter hybridhot**, föreslås att man undersöker möjligheterna att tillämpa solidaritetsklausulen i artikel 222 i EUF-fördraget (i enlighet med relevant beslut) och artikel 42.7 i EU-fördraget vid omfattande och allvarliga hybridhot. Förmågan att fatta strategiska beslut skulle kunna stärkas genom inrättandet av ett gemensamt operativt protokoll.

Slutligen föreslås en **utökning av samarbetet och samordningen mellan EU och Nato** i gemensamma insatser för att motverka hybridhot.

Vid genomförandet av denna gemensamma ram åtar sig den höga representanten och kommissionen att utnyttja de relevanta EU-instrument som står till deras förfogande. Det är viktigt att EU, tillsammans med medlemsstaterna, arbetar för att minska riskerna i samband med exponering för potentiella hybridhot från statliga och icke-statliga aktörer.