EUROPA-
KOMMISSIONEN

UNIONENS HØJTSTÅENDE
REPRÆSENTANT FOR
UDENRIGSANLIGGENDER
OG SIKKERHEDSPOLITIK

Bruxelles, den 6.4.2016
JOIN(2016) 18 final

FÆLLES MEDDELELSE TIL EUROPA-PARLAMENTET OG RÅDET

Fælles ramme for imødegåelse af hybride trusler

Den Europæiske Unions indsats

1. INDLEDNING

I de seneste år har Den Europæiske Unions sikkerhedspolitiske situation ændret sig dramatisk. Centrale udfordringer med hensyn til fred og stabilitet i EU's østlige og sydlige nabolande understreger fortsat behovet for, at EU foretager en tilpasning og øger sin kapacitet som garant for sikkerhed og stabilitet med resolut fokus på den tætte forbindelse mellem den eksterne og den interne sikkerhed. Mange af de aktuelle udfordringer med hensyn til fred, sikkerhed og velstand har rod i ustabilitet i EU's umiddelbare nærhed og i et trusselsbillede under forandring. I kommissionsformand Jean-Claude Junckers politiske retningslinjer fra 2014 understregede han, at der er behov for at "gøre Europa stærkere i sikkerheds- og forsvarsanliggender" og kombinere EU-instrumenter og nationale instrumenter mere effektivt end hidtil. I forlængelse heraf og af den opfordring, som Rådet for Udenrigsanliggender fremsatte på sit møde den 18. maj 2015, påbegyndte den højtstående repræsentant, i tæt samarbejde med Kommissionens tjenestegrene og Det Europæiske Forsvarsagentur (EDA) og i samråd med EU's medlemsstater, det arbejde, der nu munder ud i fremlæggelsen af en fælles ramme med praktisk omsættelige forslag, der kan bidrage til at imødegå hybride trusler og fremme EU's og dets medlemsstaters og partnernes modstandsdygtighed[1]. I juni 2015 mindede Det Europæiske Råd om behovet for at anvende EU's instrumenter til at bidrage til at imødegå hybride trusler[2].

Definitionen af hybride trusler kan variere og må nødvendigvis være fleksibel, fordi trusselsbilledet til stadighed ændrer sig. Begrebet dækker over en blanding af indgribende og undergravende virksomhed med konventionelle og ukonventionelle midler (dvs. diplomatiske, militære, økonomiske eller teknologiske), som statslige eller ikkestatslige aktører anvender på koordineret vis for at opnå specifikke mål uden at overskride tærsklen til formel krigsførelse. Der lægges som regel vægt på at udnytte målets svagheder og skabe en uklar situation, der vanskeliggør beslutningsprocesser. Massive misinformationskampagner ved hjælp af sociale medier til at kontrollere den politiske dagsorden eller radikalisere, rekruttere eller styre stedfortræderaktører, er et middel, der anvendes i forbindelse med hybride trusler.

Bekæmpelse af hybride trusler er først og fremmest medlemsstaternes ansvar, eftersom den vedrører national sikkerhed og forsvar og opretholdelse af lov og orden, og eftersom de fleste nationale svagheder er landespecifikke. Mange af EU's medlemsstater står dog over for fælles trusler, der også kan være rettet mod grænseoverskridende net eller infrastruktur. Sådanne trusler bekæmpes mere effektivt ved at anvende EU-politikker og -instrumenter som led i en koordineret indsats på EU-plan på grundlag af europæisk solidaritet, gensidig bistand og udnyttelse af Lissabontraktatens fulde potentiale. EU's politikker og instrumenter kan spille en central og nyttig oplysende rolle, og det gør de i vidt omfang grad allerede. Det bidrager til at styrke medlemsstaternes modstandsdygtighed, når de skal tackle fælles trusler. De udenrigspolitiske

[1] Rådets konklusioner om den fælles sikkerheds- og forsvarspolitik (FSFP) af maj 2015 [rådsdokument 8971/15].

[2] Det Europæiske Råds konklusioner af juni 2015 [EUCO 22/15].

foranstaltninger, som den fælles ramme indeholder, bygger på principperne i artikel 21 i traktaten om Den Europæiske Union (TEU), herunder demokrati, retsstatsprincippet, menneskerettighedernes og de grundlæggende frihedsrettigheders universalitet og udelelighed samt respekt for grundsætningerne i De Forenede Nationers pagt og folkeretten[3].

Denne fælles meddelelse tager sigte på at fremme en helhedsorienteret tilgang, som sætter EU i stand til i samarbejde med medlemsstaterne at tackle netop hybride trusler ved at skabe synergi mellem alle de relevante instrumenter og skabe et tæt samarbejde mellem alle de relevante aktører[4]. Foranstaltningerne bygger videre på de eksisterende strategier og sektorpolitikker, som bidrager til større sikkerhed. Særlig udgør den europæiske dagsorden om sikkerhed[5], Den Europæiske Unions kommende globale strategi for udenrigs- og sikkerhedspolitikken og den europæiske forsvarshandlingsplan[6], EU-strategien for cybersikkerhed[7], energisikkerhedsstrategien[8] og den europæiske strategi for maritim sikring[9] redskaber, som kan bidrage til bekæmpe hybride trusler.

Da også NATO arbejder på at imødegå hybride trusler, og da Rådet for Udenrigsanliggender har foreslået at intensivere samarbejdet og koordinationen på dette område, tager nogle af forslagene sigte på at øge samarbejdet mellem EU og NATO om at imødegå hybride trusler.

Den foreslåede indsats fokuserer på følgende elementer: oplysning, styrkelse af modstandsdygtighed, forebyggelse af og reaktion på krisesituationer samt tilbagevenden til en normal situation.

2. HVORDAN SES DET, AT EN TRUSSEL ER HYBRID?

Hybride trusler har til formål at udnytte et lands svagheder og sigter ofte mod at underminere grundlæggende demokratiske værdier og frihedsrettigheder. Som et første skridt vil den højtstående repræsentant og Kommissionen arbejde sammen med medlemsstaterne om at øge situationskendskabet ved at overvåge og vurdere risiciene i forbindelse med trusler rettet mod svagheder i EU. Kommissionen er i færd med at udvikle metoder til vurdering af sikkerhedsrisici med henblik på at bidrage til oplysning af beslutningstagerne og fremme en risikobaseret udformning af politik på områder fra luftfartssikkerhed til finansiering af terrorisme og hvidvaskning af penge. Desuden vil det være hensigtsmæssigt, at medlemsstaterne foretager en undersøgelse af, hvilke områder der er sårbare over for hybride trusler. Målet er at finde frem til indikatorer for hybride

[3] Den Europæiske Unions charter om grundlæggende rettigheder er bindende for EU's institutioner og for medlemsstaterne, når de gennemfører EU-retten.
[4] Eventuelle forslag til lovgivning skal opfylde Kommissionens krav om bedre regulering i overensstemmelse med Kommissionens retningslinjer for bedre regulering (SWD(2015) 111).
[5] COM(2015) 185 final.
[6] Fremlægges i 2016.
[7] Ramme for EU's cyberforsvarspolitik (rådsdokument 15585/14) og "EU-strategi for cybersikkerhed: Et åbent, sikkert og beskyttet cyberspace" (JOIN(2013) 1 af 7.2.2013).
[8] Joint Communication on 'European Energy Security Strategy', maj 2014 **(**SWD(2014) 330).
[9] Fælles meddelelse: "Et åbent og sikkert globalt maritimt område: elementer til en EU-strategi for maritim sikkerhed" (JOIN(2014) 9 final af 6.3.2014).

trusler og indarbejde dem i mekanismer for tidlig varsling og i de eksisterende mekanismer til risikovurdering og udveksle dem efter behov.

<u>Foranstaltning 1</u>*: *Medlemsstaterne opfordres til, eventuelt med støtte fra Kommissionen og den højtstående repræsentant, at iværksætte en undersøgelse af hybride risici for at finde frem til centrale svagheder, herunder specifikke indikatorer for potentielle hybride trusler mod nationale og fælleseuropæiske strukturer og net.

3. TILRETTELÆGGELSE AF EU'S INDSATS: OPLYSNING

3.1. Central EU-enhed for analyse og udveksling af oplysninger om hybride trusler

Det har stor betydning, at EU i samarbejde med medlemsstaterne har et tilstrækkeligt situationskendskab til at konstatere alle ændringer i den sikkerhedsmæssige situation, som har forbindelse til hybride aktiviteter fra statslige eller ikkestatslige aktørers side. Det er vigtigt at forbedre udvekslingen af oplysninger og fremme relevant udveksling af efterretninger på tværs af sektorer og mellem Den Europæiske Union, dens medlemsstater og partnere for at kunne bekæmpe hybride trusler effektivt.

En central EU-enhed for analyse og udveksling af oplysninger om hybride trusler vil kunne samle analysen af hybride trusler på ét sted inden for EU-Udenrigstjenestens Efterretningsanalysecenter (EU INTCEN). Fra de forskellige aktører i EU-Udenrigstjenesten (herunder EU-delegationerne), Kommissionen (herunder EU-agenturer[10]) og medlemsstaterne vil enheden kunne modtage klassificerede og offentligt tilgængelige oplysninger, særlig vedrørende indikatorer for hybride trusler, som den vil kunne analysere og udveksle. I tæt samarbejde med tilsvarende organer på EU-plan[11] og nationalt plan vil enheden kunne analysere de eksterne aspekter af hybride trusler mod EU og EU's nærområde med henblik på hurtigt at analysere relevante hændelser og kvalificere EU's strategiske beslutningsprocesser, herunder komme med input til EU's sikkerhedsrisikovurderinger. Enhedens analyseresultater vil blive behandlet og håndteret i overensstemmelse med Den Europæiske Unions bestemmelser om klassificeret information og databeskyttelse[12]. Enheden skal fungere som forbindelsesled til de eksisterende organer på EU-plan og nationalt plan. Medlemsstaterne bør oprette nationale kontaktpunkter, der varetager kontakten til EU-enheden. Personalet i og uden for EU (herunder de, der indsættes i EU-delegationer, -operationer og -missioner) og i medlemsstaterne bør uddannes i at genkende tidlige tegn på hybride trusler.

<u>Foranstaltning 2</u>*: *Oprettelse af en central EU-enhed for analyse og udveksling af oplysninger om hybride trusler i EU's eksisterende Efterretningsanalysecenter. Det skal kunne modtage og analysere klassificerede og offentligt tilgængelige oplysninger

[10] I overensstemmelse med deres mandat.
[11] F.eks. Europols Europæiske Center til Bekæmpelse af IT-Kriminalitet og europæisk center for terrorbekæmpelse, Frontex og EU's IT-beredskabsenheder (CERT-EU).
[12] Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995.

om hybride trusler. Medlemsstaterne opfordres til at oprette nationale kontaktpunkter for hybride trusler for at sikre samarbejde og sikker kommunikation med EU-enheden.

3.2. Strategisk kommunikation

De, der står bag de hybride trusler, kan systematisk udsprede misinformation, herunder gennem målrettede kampagner på sociale medier. Derved forsøger de at radikalisere enkeltpersoner, destabilisere samfundet og kontrollere den politiske dagsorden. Det er af stor betydning at anvende en **strategisk kommunikation**sstrategi i forbindelse med hybride trusler. For at opbygge samfundets modstandsdygtighed er det vigtigt hurtigt at give saglige svar og oplyse offentligheden om hybride trusler.

I den strategiske kommunikation bør der gøres fuld brug af både sociale medier og de traditionelle audiovisuelle og internetbaserede medier. EU-Udenrigstjenesten bør bygge videre på East StratCom-taskforcens og Arab StratCom-taskforcens indsats og optimere anvendelsen af sprogfolk, der taler de relevante ikke-EU-sprog flydende, og eksperter i sociale medier, som kan overvåge de oplysninger, der stammer fra lande uden for EU, og imødegå misinformation. Desuden bør medlemsstaterne udvikle mekanismer til strategisk kommunikation, der støtter angivelse af kilder og bekæmper misinformation med henblik på at henlede opmærksomheden på hybride trusler.

Foranstaltning 3*: *Den højtstående repræsentant vil sammen med medlemsstaterne undersøge, hvordan kapaciteten til proaktiv strategisk kommunikation kan ajourføres og samordnes, og anvendelsen af medier og sprogeksperter optimeres.

3.3. Ekspertisecenter for imødegåelse af hybride trusler

Et flernationalt institut eller et netværk af sådanne kunne fungere som ekspertisecenter for imødegåelse af hybride trusler og bygge videre på de erfaringer, som visse medlemsstater og partnerorganisationer[13] har gjort. Centret kunne fokusere på forskning i, hvordan hybride strategier er blevet anvendt, og tilskynde til udvikling af nye begreber og teknologier i den private sektor og erhvervslivet med henblik på at bistå medlemsstaterne med at opbygge modstandsdygtighed. Forskningen kunne bidrage til at tilpasse EU's og medlemsstaternes politikker, doktriner og begreber og til at sikre, at der i forbindelse med beslutningsprocessen tages højde for den kompleksitet og uklarhed, der er forbundet med hybride trusler. Centret vil skulle udarbejde programmer, der bringer forskningen videre, og øvelser, der fører til praktiske løsninger på de udfordringer, som de hybride trusler skaber. Et stærkt center bygger på ekspertisen hos de multinationale og tværsektorielle aktører fra de civile, militære, private og akademiske sektorer, der deltager i dets arbejde.

Et sådant center kunne arbejde tæt sammen med eksisterende EU-[14] og NATO-[15]ekspertisecentre, så det kan drage fordel af den viden om hybride trusler, som er

[13] NATO's ekspertisecentre.
[14] F.eks. EU's Institut for Sikkerhedsstudier (EUISS) og ekspertisecentre på CBRN-området.
[15] http://www.nato.int/cps/en/natohq/topics_68372.htm.

opbygget i forbindelse med cyberforsvar, strategisk kommunikation, energi og kriserespons.

Foranstaltning 4*: *Medlemsstaterne opfordres til at overveje at oprette et ekspertisecenter for imødegåelse af hybride trusler.

4. TILRETTELÆGGELSE AF EU'S INDSATS: STYRKELSE AF MODSTANDSDYGTIGHEDEN

Modstandsdygtighed er evnen til at modstå belastninger og komme styrket ud af udfordringer. Hvis de hybride trusler skal bekæmpes effektivt, må der tages hånd om de potentielle svagheder i central infrastruktur, forsyningskæder og samfundet. Infrastrukturen på EU-plan kan gøres mere modstandsdygtig ved at trække på en række EU-instrumenter og -politikker.

4.1. Beskyttelse af kritisk infrastruktur

Det er vigtigt at beskytte kritisk infrastruktur (f.eks. energiforsyningskæder og transport). Et angreb med ukonventionelle midler på "bløde mål" kan have alvorlige økonomiske eller samfundsmæssige følgevirkninger. Med henblik på sikring af kritisk infrastruktur indeholder det europæiske program for beskyttelse af kritisk infrastruktur[16] (EPCIP) en strategi til bekæmpelse af alle former for trusler mod tværsektorielle systemer med fokus på gensidig afhængighed. Den bygger på gennemførelsen af aktiviteter inden for rammerne af arbejdet med forebyggelse, beredskab og respons. Direktivet om europæisk kritisk infrastruktur[17] fastsætter en procedure for indkredsning og udpegning af europæisk kritisk infrastruktur og en fælles fremgangsmåde til vurdering af behovet for at forbedre beskyttelsen af den. Særlig bør arbejdet med at styrke modstandsdygtigheden for kritisk transportrelateret infrastruktur (f.eks. EU's vigtigste lufthavne og handelshavne) genoptages inden for rammerne af direktivet. Kommissionen vil også foretage en vurdering af, om der skal udvikles fælles redskaber (herunder indikatorer), der forbedrer den kritiske infrastrukturs modstandsdygtighed mod hybride trusler i alle relevante sektorer.

Foranstaltning 5*: *Kommissionen vil i samarbejde med medlemsstater og aktører finde frem til fælles redskaber, herunder indikatorer, med henblik på at forbedre beskyttelsen af den kritiske infrastruktur mod hybride trusler i de relevante sektorer og øge dens modstandsdygtighed mod truslerne.

4.1.1. Energinet

Elproduktion og -distribution uden afbrydelser er af vital betydning for EU, og større strømafbrydelser kan have ødelæggende virkning. En yderligere diversificering af EU's energikilder, -leverandører og -ruter er et vigtigt element i bekæmpelsen af hybride trusler og tilvejebringelsen af en mere sikker og modstandsdygtig energiforsyning.

[16] Meddelelse fra Kommissionen om et europæisk program for beskyttelse af kritisk infrastruktur, 12.12.2006, KOM(2006) 786 endelig.
[17] Rådets direktiv 2008/114/EF af 8. december 2008 om indkredsning og udpegning af europæisk kritisk infrastruktur og vurdering af behovet for at beskytte den bedre, EUT L 345 af 23.12.2008.

Kommissionen foretager også risiko- og sikkerhedsvurderinger ("stresstests") af kraftværkerne i EU. Arbejdet inden for rammerne af strategien for energiunionen intensiveres med det formål at sørge for en diversificering af energiforsyningen. Eksempelvis kan den sydlige gaskorridor skabe mulighed for, at gas fra den kaspiske region kan nå Europa, og i Nordeuropa kan der etableres gasbørser, hvor flere forskellige leverandører kan afsætte flydende gas. Dette eksempel bør følges i Central- og Østeuropa og i Middelhavsområdet, hvor en gasbørs p.t. er ved at blive udviklet[18]. Udviklingen af et marked for flydende naturgas vil også bidrage til at nå dette mål.

For så vidt angår nukleare materialer og anlæg støtter Kommissionen udviklingen og vedtagelsen af de højeste standarder for sikkerhed, hvilket styrker modstandsdygtigheden. Kommissionen opfordrer til konsekvent gennemførelse af direktivet om nuklear sikkerhed[19], hvori der er fastsat regler vedrørende forebyggelse af ulykker og afbødning af følgerne af ulykker, og af direktivet om grundlæggende sikkerhedsnormer[20], der vedrører internationalt samarbejde om beredskabet og indsatsen i nødsituationer, særlig mellem nabomedlemsstater og med nabolande.

<u>Foranstaltning 6</u>: Kommissionen vil i samarbejde med medlemsstaterne støtte bestræbelserne på at diversificere energikilderne og fremme sikkerheden og sikkerhedsstandarderne, således at den nukleare infrastrukturs modstandsdygtighed øges.

4.1.2 Transportsikkerhed og sikkerhed i forsyningskæden

Transport er afgørende for, at EU kan fungere. Hybride angreb på transportinfrastrukturen (f.eks. lufthavne, vejinfrastruktur, havne og jernbaner) kan få alvorlige konsekvenser og føre til forstyrrelser af trafik og forsyningskæder. I forbindelse med gennemførelsen af lovgivningen om luftfartssikkerhed[21] og maritim sikkerhed[22] udfører Kommissionen regelmæssige inspektioner og søger gennem sit arbejde vedrørende landtransportsikkerhed at tage hånd om de hybride trusler, der viser sig. I den sammenhæng er en EU-ramme under drøftelse inden for rammerne af forordningen om

---

[18] Med hensyn til de fremskridt, der er gjort indtil nu, se "Status over energiunionen 2015" (COM(2015) 572 final).

[19] Rådets direktiv 2009/71/Euratom af 25. juni 2009 om EF-rammebestemmelser for nukleare anlægs nukleare sikkerhed, som ændret ved Rådets direktiv 2014/87/Euratom af 8. juli 2014.

[20] Rådets direktiv 2013/59/Euratom af 5. december 2013 om fastlæggelse af grundlæggende sikkerhedsnormer til beskyttelse mod de farer, som er forbundet med udsættelse for ioniserende stråling og om ophævelse af direktiv 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom og 2003/122/Euratom.

[21] Europa-Parlamentets og Rådets forordning (EF) nr. 300/2008 af 11. marts 2008 om fælles bestemmelser om sikkerhed inden for civil luftfart og om ophævelse af forordning (EF) nr. 2320/2002, Kommissionens gennemførelsesforordning (EU) 2015/1998 af 5. november 2015 om detaljerede foranstaltninger til gennemførelse af de fælles grundlæggende normer for luftfartssikkerhed, Europa-Parlamentets og Rådets direktiv 2005/65/EF af 26. oktober 2005 om bedre havnesikring og Europa-Parlamentets og Rådets forordning (EF) nr. 725/2004 af 31. marts 2004 om bedre sikring af skibe og havnefaciliteter.

[22] I henhold til EU-retten skal Kommissionen udføre inspektioner for at sikre, at kravene til luftfartssikkerhed og maritim sikkerhed gennemføres korrekt af medlemsstaterne. Det omfatter inspektioner af den kompetente myndighed i medlemsstaterne og inspektioner i lufthavne, i havne, hos luftfartsselskaber, på skibe og i enheder, der gennemfører sikkerhedsforanstaltninger. Kommissionens inspektioner har til formål at sikre, at medlemsstaterne gennemfører EU's standarder fuldt ud.

civil luftfartssikkerhed[23] som led i luftfartsstrategien for Europa[24]. Desuden tages der hånd om truslerne mod den maritime sikkerhed i Den Europæiske Unions strategi for maritim sikkerhed[25]. Sidstnævnte sætter EU og medlemsstaterne i stand til på samlet vis at tackle maritime sikkerhedsudfordringer, herunder bekæmpe hybride trusler, gennem tværsektorielt samarbejde mellem civile og militære aktører om at beskytte kritisk maritim infrastruktur, den globale forsyningskæde, maritim handel samt maritime ressourcer, naturressourcer og energiressourcer. Der tages også hånd om sikkerheden i den internationale forsyningskæde i EU's strategi og handlingsplan for toldrisikostyring[26].

Foranstaltning 7*: *Kommissionen vil overvåge de trusler, der måtte vise sig, i hele transportsektoren og om nødvendigt ajourføre lovgivningen. I forbindelse med gennemførelsen af EU's maritime sikkerhedsstrategi og EU's strategi og handlingsplan for toldrisikostyring vil Kommissionen og den højtstående repræsentant (inden for deres respektive kompetenceområde) i samarbejde med medlemsstaterne undersøge, hvordan der skal reageres på hybride trusler, særlig trusler mod kritisk transportinfrastruktur.

4.1.3 Rummet

Ruminfrastruktur kan blive mål for hybride trusler, og det kan få konsekvenser i flere forskellige sektorer. EU har udformet en støtteramme for overvågning og sporing i rummet[27] for at samle aktiver ejet af medlemsstater i netværk med henblik på at levere rumovervågnings- og sporingstjenester[28] til kendte brugere (medlemsstater, EU-institutioner, ejere og operatører af rumfartøjer og civilbeskyttelsesmyndigheder). I forbindelse med den kommende rumstrategi for Europa vil Kommissionen undersøge, hvordan den kan udvikles yderligere, så de hybride trusler mod ruminfrastruktur overvåges.

Satellitkommunikation er et nøgleaktiv i krisestyring, katastrofeberedskab, politi, grænseovervågning og kystovervågning. Satellitkommunikation er rygraden i større infrastrukturer, f.eks. transportinfrastruktur, ruminfrastruktur eller fjernstyrede luftfartøjssystemer. I overensstemmelse med Det Europæiske Råds opfordring til at forberede den næste generation af statslig satellitkommunikation (GOVSATCOM) er Kommissionen i samarbejde med Det Europæiske Forsvarsagentur i færd med at vurdere,

[23] Kommissionens forordning (EU) 2016/4 af 5. januar 2016 om ændring af Europa-Parlamentets og Rådets forordning (EF) nr. 216/2008 for så vidt angår væsentlige miljøbeskyttelseskrav. Forordning (EF) nr. 216/2008 af 20.2.2008 om fælles regler for civil luftfart og om oprettelse af et europæisk luftfartssikkerhedsagentur.

[24] Meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget af 7.12.2015: En luftfartsstrategi for Europa (COM(2015) 598 final).

[25] I december 2014 vedtog Rådet en handlingsplan for gennemførelsen af EU-strategien for maritim sikkerhed http://ec.europa.eu/maritimeaffairs/policy/maritime-security/doc/20141216-action-plan_en.pdf.

[26] Meddelelse fra Kommissionen til Europa-Parlamentet, Rådet og Det Europæiske Økonomiske og Sociale Udvalg: EU's strategi og handlingsplan for toldrisikostyring: Håndtering af risici, styrkelse af sikkerhed i forsyningskæden og lettelse af handel (COM (2014) 527 final).

[27] Se Europa-Parlamentets og Rådets afgørelse nr. 541/2014/EU.

[28] F.eks. varsling, der forebygger kollision af rumfartøjer i kredsløb.

hvordan efterspørgslen kan samles, i forbindelse med den kommende rumstrategi og den europæiske forsvarshandlingsplan.

Megen kritisk infrastruktur er afhængig af præcise oplysninger om tid for at synkronisere deres net (f.eks. energi og telekommunikation) eller tidsstemple transaktioner (f.eks. finansielle markeder). Afhængigheden af et enkelt tidssynkroniseringssignal fra det globale satellitbaserede navigationssystem giver ikke mulighed for den modstandsdygtighed, der kræves for at bekæmpe hybride trusler. Galileo, det europæiske globale satellitbaserede navigationssystem, ville udgøre en alternativ pålidelig kilde til oplysninger om tid.

Foranstaltning 8*: *Inden for rammerne af den kommende rumstrategi og den europæiske forsvarshandlingsplan vil Kommissionen foreslå at øge ruminfrastrukturens modstandsdygtighed mod hybride trusler, særlig gennem en mulig udvidelse af anvendelsesområdet for overvågning og sporing i rummet til hybride trusler, forberedelsen af næste generation af GOVSATCOM på europæisk plan og ibrugtagning af Galileo i kritisk infrastruktur, der er afhængig af tidssynkronisering.

4.2. Forsvarskapacitet

Der er behov for at øge forsvarskapaciteten for at styrke EU's modstandsdygtighed mod hybride trusler. Det er vigtigt at indkredse de vigtigste kapacitetsområder, f.eks. overvågningskapacitet og rekognosceringskapacitet. Det Europæiske Forsvarsagentur kunne være katalysator for udvikling af militær kapacitet vedrørende hybride trusler (f.eks. ved at afkorte udviklingscyklusserne for militær kapacitet, investere i teknologi, systemer og prototyper og åbne forsvarsindustrien for innovative kommercielle teknologier). Mulige foranstaltninger kunne undersøges inden for rammerne af den kommende europæiske forsvarshandlingsplan.

Foranstaltning 9*: *Den højtstående repræsentant vil, eventuelt med støtte fra medlemsstaterne, fremlægge forslag til projekter om, hvordan forsvarskapaciteten skal udvikles, og om hvordan EU skal gøres mere relevant, med særligt henblik på at imødegå hybride trusler mod en eller flere medlemsstater.

4.3. Beskyttelse af folkesundheden og fødevaresikkerheden

Folkesundheden kan bringes i fare ved manipulation med overførbare sygdomme eller forurening af fødevarer, jord, luft og drikkevand med kemiske, biologiske, radiologiske og nukleare (CBRN) agenser. I EU kan forsætlig spredning af dyre- eller plantesygdomme desuden få alvorlige følger for fødevaresikkerheden og store økonomiske og sociale konsekvenser for fødevarekæden. De eksisterende EU-strukturer inden for sundhedssikkerhed, miljøbeskyttelse og fødevaresikkerhed kan bruges til at tackle de hybride trusler, hvor ovennævnte midler anvendes.

I henhold til EU-retten vedrørende grænseoverskridende sundhedstrusler[29] koordineres beredskabet ved alvorlige grænseoverskridende trusler mod sundheden ved hjælp af de eksisterende mekanismer i et samarbejde mellem medlemsstater, EU-agenturer og videnskabelige komitéer[30], gennem systemet for tidlig varsling og reaktion. Udvalget for Sundhedssikkerhed, som koordinerer medlemsstaternes indsats i forbindelse med trusler, kan fungere som kontaktpunkt vedrørende svagheder på folkesundhedsområdet[31] med henblik på, at de hybride trusler (særlig bioterrorisme) indgår i retningslinjerne for krisekommunikation og i øvelserne i (krisesimulations)kapacitetsopbygning sammen med medlemsstaterne. På området fødevaresikkerhed udveksler de kompetente myndigheder gennem det hurtige varslingssystem for fødevarer og foder (RASFF) og toldrisikoforvaltningssystemet (CRMS) oplysninger om risikoanalyser for at overvåge de sundhedsrisici, som forurenede fødevarer udgør. For så vidt angår dyrs og planters sundhed vil revisionen af de eksisterende EU-lovrammer[32] føje nye elementer til den eksisterende "værktøjskasse"[33] med henblik på at være bedre forberedt, også på hybride trusler.

<u>Foranstaltning 10</u>: Kommissionen vil i samarbejde med medlemsstaterne øge bevidstheden om og modstandsdygtigheden mod hybride trusler inden for de eksisterende beredskabs- og koordineringsmekanismer, særlig Udvalget for Sundhedssikkerhed.

4.4. IT-sikkerhed

EU nyder i høj grad godt af at have et indbyrdes forbundet og digitaliseret samfund. Cyberangreb kunne få de digitale tjenester til at bryde sammen i hele EU, og sådanne angreb kunne anvendes af dem, der står bag hybride trusler. Af hensyn til det digitale indre marked er det vigtigt at forbedre kommunikations- og informationssystemernes modstandsdygtighed. EU-strategien for cybersikkerhed og den europæiske dagsorden om sikkerhed udstikker en samlet strategisk ramme for EU's initiativer vedrørende IT-sikkerhed og IT-kriminalitet. EU har arbejdet aktivt med bevidstgørelse, samarbejdsmekanismer og respons som et af resultaterne af strategien for cybersikkerhed. Særlig omhandler direktivet om net- og informationssikkerhed[34] IT-

[29] Europa-Parlamentets og Rådets afgørelse nr. 1082/2013/EU af 22. oktober 2013 om alvorlige grænseoverskridende sundhedstrusler og om ophævelse af beslutning nr. 2119/98/EF(EUT L 293 af 5.11.2013, s. 1).

[30] Commission Decision C(2015) 5383 of 7.8.2015 on establishing Scientific Committees in the field of public health, consumer safety and the environment.

[31] I overensstemmelse med Europa-Parlamentets og Rådets afgørelse nr. 1082/2013/EU af 22. oktober 2013 om alvorlige grænseoverskridende sundhedstrusler og om ophævelse af beslutning nr. 2119/98/EF (EUT L 293 af 5.11.2013, s. 1).

[32] Europa-Parlamentets og Rådets forordning (EU) 2016/429 om overførbare dyresygdomme og om ændring og ophævelse af visse retsakter på området for dyresundhed ("dyresundhedsloven") (EUT L 84 af 31.3.2016, s. 1). For så vidt angår Europa-Parlamentets og Rådets forordning om beskyttelsesforanstaltninger mod skadegørere på planter blev der opnået en politisk enighed mellem Europa-Parlamentet og Rådet om teksten den 16.12.2015.

[33] F.eks. EU-vaccinebanker, et avanceret elektronisk system til information om dyresygdomme og øgede forpligtelser for laboratorier og andre enheder, der arbejder med smitstoffer, til at træffe de fornødne foranstaltninger.

[34] Kommissionens forslag til Europa-Parlamentets og Rådets direktiv af 7.2.2013 om foranstaltninger, der skal sikre et højt fælles niveau for net- og informationssikkerhed i hele EU (COM(2013) 48 final). Der er

sikkerhedsrisici for en bred vifte af udbydere af grundlæggende tjenester på områderne energi, transport, finans og sundhed. Disse udbydere bør i lighed med udbydere af vigtige digitale tjenester (f.eks. cloudcomputing) træffe passende sikkerhedsforanstaltninger og indberette alvorlige hændelser til de nationale myndigheder, herunder gøre opmærksom på eventuelle tegn på hybride trusler. Når Rådet og Europa-Parlamentet har vedtaget direktivet, vil en effektiv gennemførelse af det øge IT-sikkerhedskapaciteten i medlemsstaterne og styrke samarbejdet om IT-sikkerhed gennem udveksling af oplysninger og god praksis om imødegåelse af hybride trusler. Særlig skal der i henhold til direktivet oprettes et net af de 28 nationale CSIRT'er (enheder, der håndterer IT-sikkerhedshændelser) og CERT-EU[35], der viderefører det operationelle samarbejde på frivilligt grundlag.

For at tilskynde til offentligt-privat samarbejde og en EU-omspændende tilgang til IT-sikkerhed har Kommissionen oprettet platformen for net- og informationssikkerhed, som vejleder om god praksis og risikostyring. Medlemsstaterne fastlægger sikkerhedskravene og de nærmere bestemmelser om, hvordan der skal gives meddelelse om nationale hændelser. Kommissionen tilskynder til en høj grad af konvergens i tilgangen til risikostyring og trækker i den forbindelse særlig på Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA).

<u>Foranstaltning 11</u>: Kommissionen opfordrer medlemsstaterne til at give det høj prioritet at oprette et net af de 28 nationale CSIRT'er og CERT-EU og en ramme for strategisk samarbejde, og til at gøre fuld brug af begge. Kommissionen bør i samarbejde med medlemsstaterne sikre, at sektorinitiativer vedrørende cybertrusler (f.eks. inden for luftfart, energi og det maritime område) er i overensstemmelse med de tværsektorielle kapaciteter, der er omfattet af direktivet om net- og informationssikkerhed med henblik på at samle oplysninger, ekspertise og hurtige reaktioner.

4.4.1. Erhvervslivet

Den øgede afhængighed af cloudcomputing og massedata har øget sårbarheden over for hybride trusler. Strategien for et digitalt indre marked i EU indeholder et kontraktligt offentlig-privat partnerskab om IT-sikkerhed[36], som vil fokusere på forskning og innovation og hjælpe EU med at fastholde en stor teknologisk kapacitet på dette område. Det kontraktlige offentlig-private partnerskab vil skabe tillid hos markedsaktørerne og synergier mellem efterspørgsels- og udbudssiden. Det kontraktlige offentlig-private partnerskab og ledsageforanstaltningerne vil primært fokusere på civile IT-sikkerhedsprodukter og -tjenester, men som et resultat af disse initiativer skulle teknologibrugerne gerne blive bedre beskyttet også mod hybride trusler.

---

opnået politisk enighed mellem Rådet og Europa-Parlamentet om det foreslåede direktiv, som forventes formelt vedtaget inden længe.

[35] EU's IT-beredskabsenheder for EU-institutionerne.

[36] Iværksættes medio 2016.

<u>Foranstaltning 12</u>: Kommissionen vil i samarbejde med medlemsstaterne arbejde sammen med erhvervslivet om inden for rammerne af et kontraktligt offentlig-privat partnerskab om IT-sikkerhed at udvikle og teste teknologier, der yder brugerne og infrastrukturen bedre beskyttelse mod IT-aspekterne af hybride trusler.

4.4.2. Energi

Fremkomsten af intelligente bygninger og apparater, udviklingen af intelligente net og øget digitalisering af energisystemet medfører også øget sårbarhed over for cyberangreb. Den europæiske energisikkerhedsstrategi[37] og strategien for energiunionen[38] understøtter en tilgang, der bekæmper alle trusler, og hvori modstandsdygtighed mod hybride trusler er indarbejdet. Det tematiske net vedrørende beskyttelse af kritisk energiinfrastruktur fremmer samarbejdet mellem aktører i energisektoren (olie, gas og el). Kommissionen har lanceret en webbaseret platform med henblik på at analysere og udveksle oplysninger om trusler og hændelser[39]. Desuden er den sammen med aktørerne[40] ved at udvikle en samlet IT-sikkerhedsstrategi vedrørende drift af intelligente net for energisektoren med henblik på at mindske sårbarheden. Skønt elmarkederne bliver stadig mere integrerede, er reglerne og procedurerne for, hvordan krisesituationer håndteres, fortsat nationale. Vi må sørge for, at regeringerne samarbejder med hinanden om at forberede sig på, forebygge og begrænse risiciene, og at alle involverede aktører handler ud fra et fælles regelsæt.

<u>Foranstaltning 13</u>: Kommissionen vil udstede retningslinjer, så ejerne af intelligente net kan forbedre IT-sikkerheden i deres anlæg. I forbindelse med forslaget om en ny udformning af elmarkedet vil Kommissionen overveje at foreslå "risikoberedskabsplaner" og procedureregler for udveksling af oplysninger og sikring af solidaritet mellem medlemsstaterne i krisesituationer, herunder regler om, hvordan cyberangreb kan forebygges og afbødes.

4.4.3. Sunde finansielle systemer

For at fungere har økonomien i EU behov for et sikrere finansielt system og betalingssystem. Det er vigtigt at beskytte det finansielle system og dets infrastruktur mod cyberangreb, uanset hvilke motiver de, der angriber det, har. For at kunne håndtere hybride trusler mod finansielle tjenesteydelser i EU må sektoren forstå truslen, afprøve sine forsvarsmekanismer og råde over den teknologi, der er nødvendig for at beskytte sig mod angreb. Tilsvarende er det afgørende at udveksle oplysninger mellem finansielle markedsaktører og med de relevante myndigheder og centrale leverandører af tjenesteydelser eller kunder, men informationsudvekslingen skal være sikker og opfylde databeskyttelseskravene. I overensstemmelse med arbejdet i internationale fora, herunder G7's arbejde vedrørende sektoren, vil Kommissionen søge at finde frem til faktorer, som vanskeliggør en hensigtsmæssig udveksling af oplysninger om trusler, og foreslå løsninger. Det er vigtigt at sikre løbende afprøvning og finjustering af protokoller for at

[37] Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet: Europæisk energisikkerhedsstrategi – COM(2014) 330 final.
[38] Meddelelsen "En rammestrategi for en modstandsdygtig energiunion med en fremadskuende klimapolitik", COM(2015) 80 final.
[39] EU-Center for Udveksling af Oplysninger om Hændelser og Trusler.
[40] I form af Energiekspert-IT-sikkerhedsplatformen.

beskytte erhvervslivet og den relevante infrastruktur og herunder løbende opgradere den sikkerhedsfremmende teknologi.

<u>Foranstaltning 14</u>: Kommissionen vil i samarbejde med ENISA[41], medlemsstaterne og relevante internationale, europæiske og nationale myndigheder og finansielle institutioner fremme og støtte platforme og netværk til udveksling af oplysninger om trusler og afhjælpe faktorer, som vanskeliggør udveksling af oplysninger.

4.4.4. Transport

Moderne transportsystemer (jernbane-, vej-, luft- og sø-) er afhængige af informationssystemer, der er sårbare over for cyberangreb. I betragtning af den grænseoverskridende dimension har EU en særlig rolle. Kommissionen vil i samarbejde med medlemsstaterne fortsat analysere cybertrusler og risici forbundet med ulovlige handlinger rettet mod transportsystemer. Kommissionen er i samarbejde med Det Europæiske Luftfartssikkerhedsagentur (EASA) ved at udarbejde en køreplan for IT-sikkerhed inden for luftfart[42]. Desuden tages der hånd om cybertruslerne mod den maritime sikkerhed i Den Europæiske Unions strategi for maritim sikkerhed og den tilhørende handlingsplan.

<u>Foranstaltning 15</u>: Kommissionen og den højtstående repræsentant undersøger (inden for deres respektive kompetenceområde) i samarbejde med medlemsstaterne, hvordan der skal reageres på hybride trusler, særlig dem, der vedrører cyberangreb i transportsektoren

4.5. En målrettet indsats mod finansiering af hybride trusler

De, der står bag hybride trusler, har brug for pengemidler for at kunne fortsætte deres aktiviteter. Pengemidlerne anvendes til at støtte terrorgrupper eller mere spidsfindige former for destabilisering, f.eks. i form af støtte til pressionsgrupper og yderligtgående politiske partier. EU har intensiveret bestræbelserne på at bekæmpe kriminalitet og finansiering af terrorisme, som fastsat i den europæiske dagsorden om sikkerhed, særlig gennem handlingsplanen[43]. I denne forbindelse styrker den reviderede ramme for bekæmpelse af hvidvaskning af penge bekæmpelsen af terrorfinansiering og hvidvaskning af penge og letter de finansielle efterretningsenheders (FIU) arbejde med at indkredse og følge op på mistænkelige pengeoverførsler og udvekslinger af oplysninger, samtidig med at det sikres, at overførsler af midler i Den Europæiske Union kan spores.

[41] Den Europæiske Unions Agentur for Net- og Informationssikkerhed.

[42] Kommissionen fremlagde i december 2015 sit forslag til ny forordning om Det Europæiske Luftfartssikkerhedsagentur, som det i øjeblikket drøftes af Europa-Parlamentet og Rådet. Forslag til Europa-Parlamentets og Rådets forordning om fælles regler for civil luftfart og oprettelse af Den Europæiske Unions Luftfartssikkerhedsagentur og om ophævelse af Europa-Parlamentets og Rådets forordning (EF) nr. 216/2008, COM(2015) 613 final, 2015/277 (COD).

[43] Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om en handlingsplan med henblik på at styrke bekæmpelsen af finansiering af terrorisme, COM(2016)50 final.

Derfor kunne rammen også bidrage til at imødegå hybride trusler. For så vidt angår FUSP-instrumenter kunne det undersøges, om der skal anvendes skræddersyede og effektive restriktive foranstaltninger til at imødegå hybride trusler.

<u>Foranstaltning 16:</u> Kommissionen vil anvende gennemførelsen af handlingsplanen for bekæmpelse af finansiering af terrorisme til også at bekæmpe hybride trusler.

4.6. Større modstandsdygtighed over for radikalisering og voldelig ekstremisme

Selv om terrorhandlinger og voldelig ekstremisme i sig selv ikke udgør hybride trusler, kan de, der står bag hybride trusler, søge at rekruttere sårbare borgere i samfundet og radikalisere dem via moderne kommunikationskanaler (herunder sociale medier på internettet og proxygrupper) og propaganda.

For at bekæmpe ekstremistisk indhold på internettet er Kommissionen - inden for rammerne af strategien for et digitalt indre marked i EU - ved at analysere behovet for potentielt nye foranstaltninger under behørig hensyntagen til virkningerne heraf for de grundlæggende rettigheder såsom ytrings- og informationsfriheden. Dette kan omfatte strenge procedurer for fjernelse af ulovligt indhold, uden at der samtidig fjernes lovligt indhold ("varsel og handling"), og at formidlerne ved forvaltningen af deres net og systemer udviser større ansvarlighed og rettidig omhu. Sådanne foranstaltninger vil supplere den aktuelle frivillige tilgang, hvor internetvirksomheder og virksomhederne bag sociale medier (navnlig under EU's internetforum) i samarbejde med Europols europæiske enhed for indberetning af internetindhold hurtigt fjerner terroristpropaganda.

Inden for rammerne af den europæiske dagsorden om sikkerhed bekæmpes radikalisering ved udveksling af erfaringer og udvikling af bedste praksis, herunder samarbejde med tredjelande. Rådgivningsholdet for strategisk kommunikation om Syrien sigter mod i højere grad at udvikle og formidler alternative budskaber for at bekæmpe terroristpropaganda. Netværket til bevidstgørelse om radikalisering støtter medlemsstaterne og fagfolk, som skal interagere med radikaliserede personer (herunder udenlandske krigere) eller med personer, der skønnes at være nemme ofre for radikalisering. Netværket til bevidstgørelse om radikalisering tilrettelægger uddannelsesaktiviteter og yder rådgivning foruden at tilbyde støtte til prioriterede tredjelande, der er villige til at samarbejde. Derudover er Kommissionen ved at fremme et retligt samarbejde mellem aktører på det strafferetlige område, herunder Eurojust, med henblik på at bekæmpe terrorisme og radikalisering på tværs af medlemsstaterne, herunder håndtering af udenlandske krigere og hjemvendte.

Ved at supplere ovennævnte tiltag i forbindelse med sin **udenrigspolitik** bidrager EU til at bekæmpe voldelig ekstremisme, bl.a. gennem engagement udadtil og outreachaktiviteter, forebyggelse (bekæmpelse af radikalisering og finansiering af terrorisme) samt gennem foranstaltninger for at tackle de bagved liggende økonomiske, politiske og samfundsmæssige faktorer, som giver terroristgrupper mulighed for at blomstre.

<u>Foranstaltning 17:</u> Kommissionen er ved at gennemføre en række foranstaltninger til bekæmpelse af radikalisering, der er fastsat i den europæiske dagsorden om sikkerhed, og at analysere behovet for at styrke procedurerne for fjernelse af ulovligt indhold, idet formidlerne ved forvaltningen af deres net og systemer opfordres til at udvise rettidig omhu.

4.7. Øget samarbejde med tredjelande

Som understreget i den europæiske dagsorden om sikkerhed har EU sat øget fokus på at opbygge kapacitet i ***partnerlande*** inden for sikkerhedssektoren, bl.a. ved at udnytte forbindelsen mellem sikkerhed og udvikling og styrke den sikkerhedsmæssige dimension i EU's reviderede naboskabspolitik[44]. Disse foranstaltninger kan også forbedre partnernes modstandsdygtighed over for hybridaktiviteter.

Kommissionen har til hensigt yderligere at intensivere udvekslingen af operationelle og strategiske oplysninger med kandidatlandene og inden for det østlige partnerskab og det sydlige naboskab, når det er relevant, for at hjælpe med til at bekæmpe organiseret kriminalitet, terrorisme, irregulær migration og ulovlig handel med håndvåben. Hvad angår terrorbekæmpelse, optrapper EU samarbejdet med tredjelande ved at indlede bedre dialoger om sikkerhedsspørgsmål og handlingsplaner.

EU's eksterne finansieringsinstrumenter har til formål at opbygge velfungerende og ansvarlige institutioner i tredjelande[45], hvilket er en forudsætning for effektivt at reagere på sikkerhedstrusler og øge modstandsdygtigheden. I den forbindelse udgør reform af sikkerhedssektoren og kapacitetsopbygning til støtte for sikkerhed og udvikling[46] vigtige redskaber. Inden for rammerne af instrumentet, der bidrager til stabilitet og fred[47], har Kommissionen udformet en række foranstaltninger for at øge cyberrobustheden og partnernes kapacitet til at opdage og reagere på IT-angreb og IT-kriminalitet, hvilket kan være med til at bekæmpe hybride trusler i tredjelande. EU finansierer kapacitetsopbyggende aktiviteter i partnerlande for at mindske de sikkerhedsmæssige risici i forbindelse med spørgsmål vedrørende CBRN[48].

---

[44] Fælles meddelelse til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget - Revision af den europæiske naboskabspolitik (JOIN(2015) 50 final af 18.11.2015).

[45] Som ovenfor. Meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget — EU Enlargement Strategy (COM(2015) 611 final af 10.11.2015). Meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget - Forbedring af virkningen af EU's udviklingspolitik: En dagsorden for forandring (KOM(2011) 637 endelig af 13.10.2011).

[46] Fælles meddelelse - Kapacitetsopbygning til støtte for sikkerhed og udvikling - Hvordan partnere kan sættes i stand til at forebygge og styre kriser (JOIN(2015) 17 final).

[47] Europa-Parlamentets og Rådets forordning (EU) nr. 230/2014 af 11. marts 2014 om oprettelse af et instrument, der bidrager til stabilitet og fred (EUT L 77 af 15.3.2014, s. 1).

[48] Blandt de områder, der er omfattet, er grænseovervågning, første reaktion, ulovlig handel og udførsel af produkter og teknologi med dobbelt anvendelse, sygdomsovervågning og -kontrol, nuklear eftersporing, genopretning efter hændelse og beskyttelse af højrisikofaciliteter. Bedste praksis fra redskaber udviklet inden for rammerne af EU's CBRN-handlingsplan såsom det europæiske center for uddannelse i nuklear sikkerhed og EU's deltagelse i International Border Monitoring Working Group kan deles med tredjelande.

Endelig kan medlemsstaterne på baggrund af den omfattende tilgang til krisestyring anvende de redskaber og missioner, den fælles sikkerheds- og forsvarspolitik (FSFP) giver, uafhængigt af eller som supplement til de anvendte EU-instrumenter for derved at bistå partnere med at øge deres kapacitet. Følgende foranstaltninger kunne overvejes: i) støtte til strategisk kommunikation, ii) rådgivende støtte til vigtige ministerier, der udsættes for hybride trusler, iii) supplerende støtte til grænseforvaltning i tilfælde af en nødsituation. Andre synergier mellem FSFP-instrumenter og sikkerhed, told- og retsmyndigheder, herunder de relevante EU-agenturer[49], Interpol og den europæiske gendarmeristyrke, kan udnyttes i overensstemmelse med disses mandater.

<u>Foranstaltning 18:</u> Den højtstående repræsentant vil i samarbejde med Kommissionen iværksætte en undersøgelse af hybride risici i naboregioner.

Den højtstående repræsentant, Kommissionen og medlemsstaterne vil anvende de instrumenter, de har til rådighed, til at opbygge partnernes kapacitet og øge deres modstandsdygtighed over for hybride trusler. Der kan uafhængigt af eller som supplement til EU-instrumenter anvendes FSFP-missioner til at bistå partnere med at øge deres kapacitet.

5. FOREBYGGELSE AF OG REAKTION PÅ KRISESITUATIONER SAMT TILBAGEVENDEN TIL EN NORMAL SITUATION

Som skitseret i afsnit 3.1 har den foreslåede EU-enhed for analyse og udveksling af oplysninger om hybride trusler til formål at analysere relevante indikatorer for at forebygge og reagere på hybride trusler og informere EU's beslutningstagere. Selv om svagheder kan afhjælpes gennem langsigtede politikker på nationalt plan og EU-plan, er det på kort sigt fortsat vigtigt at øge medlemsstaternes og EU's kapacitet til hurtigt og på samordnet vis at forebygge hybride trusler, reagere på dem og vende tilbage til en normal situation.

Det er vigtigt hurtigt at kunne reagere på hændelser, der skyldes hybride trusler. I den forbindelse kan en styrkelse af Det Europæiske Katastrofeberedskabs-koordineringscenters nationale civilbeskyttelsesforanstaltninger og kapacitet[50] udgøre en måde til effektivt at reagere på forskellige aspekter af hybride trusler, som kræver en civilbeskyttelsesindsats. Dette kan ske samordnet med andre EU-reaktionsmekanismer og systemer for tidlig varsling, navnlig med EU-Udenrigstjenestens situationsrum, når det drejer sig om den eksterne sikkerhed, og det strategiske analyse- og beredskabscenter, hvad angår den interne sikkerhed.

Solidaritetsbestemmelsen (artikel 222 i TEUF) muliggør en EU-indsats og en indsats mellem medlemsstaterne, hvis en medlemsstat udsættes for et terrorangreb eller er offer for en naturkatastrofe eller en menneskeskabt katastrofe. EU's indsats for at bistå medlemsstaterne gennemføres på grundlag af Rådets afgørelse 2014/415/EU[51].

[49] Europol, Frontex, Cepol, Eurojust.
[50] http://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en.
[51] Rådets afgørelse 2014/415/EU om ordninger til Unionens gennemførelse af solidaritetsbestemmelsen (EUT L 192 af 1.7.2014, s. 53).

Ordninger for at sikre koordineringen internt i Rådet skal tage udgangspunkt i EU's integrerede ordninger for politisk kriserespons[52]. I medfør af disse ordninger indkredser Kommissionen og den højtstående repræsentant (hver på deres respektive kompetenceområde) de relevante EU-instrumenter og fremlægger forslag til afgørelser for Rådet om ekstraordinære foranstaltninger.

Artikel 222 i TEUF vedrører også situationer, der involverer en eller flere medlemsstaters direkte bistand til en medlemsstat, som udsættes for et terrorangreb eller er offer for en naturkatastrofe eller en menneskeskabt katastrofe. I den henseende finder Rådets afgørelse 2014/415/EU ikke anvendelse. I lyset af uklarhederne i forbindelse med hybride aktiviteter er det Kommissionen og den højtstående repræsentant (inden for deres respektive kompetenceområder), der skal vurdere, om solidaritetsbestemmelsen skal tages i anvendelse som sidste udvej, hvis en EU-medlemsstat er udsat for betydelige hybride trusler.

Hvis flere alvorlige hybride trusler udgør et væbnet angreb på en EU-medlemsstat, er det artikel 42, stk. 7, i TEU snarere end artikel 222 i TEUF, der skal anvendes for at sikre en hensigtsmæssig og rettidig reaktion. I tilfælde af omfattende og alvorlige hybride trusler kan et øget samarbejde og en øget koordinering med NATO være påkrævet.

Når medlemsstaterne forbereder deres styrker, opfordres de til at tage hensyn til potentielle hybride trusler. For at medlemsstaterne kan være forberedt på hurtigt og effektivt at træffe afgørelser i tilfælde af hybridangreb, er det nødvendigt, at de regelmæssigt gennemfører øvelser på operationelt og politisk plan for at afprøve beslutningsevnen på nationalt og multinationalt plan. Målet er at have en fælles operationel protokol mellem medlemsstaterne, Kommissionen og den højtstående repræsentant, hvori der skitseres effektive procedurer, der skal følges i tilfælde af en hybrid trussel, lige fra den fase, hvor truslen først indkredses, til den afsluttende angrebsfase, og hvori hver EU-institutions og aktørs rolle kortlægges.

Som en vigtig del af FSFP-engagementet kunne den omfatte a) civil og militær uddannelse, b) mentor- og rådgivningsmissioner for at forbedre en truet stats sikkerhed og forsvarskapacitet, c) beredskabsplanlægning for at indkredse tegn på hybride trusler og styrkelse af kapaciteten til tidlig varsling, d) støtte til forvaltning af grænsekontrollen og e) støtte på specialiserede områder såsom mindskelse af CBRN-risici og evakuering af civile.

<u>Foranstaltning 19:</u> Den højtstående repræsentant og Kommissionen vil i samarbejde med medlemsstaterne udforme en fælles operationel protokol og gennemføre regelmæssige øvelser for at forbedre den strategiske beslutningsevne som reaktion på hybride trusler på grundlag af krisestyringsprocedurer og integrerede ordninger for politisk kriserespons.

[52] http://www.consilium.europa.eu/da/documents-publications/publications/2014/eu-ipcr/

<u>Foranstaltning 20:</u> Kommissionen og den højtstående repræsentant vil på deres respektive kompetenceområder undersøge, hvordan artikel 222 i TEUF og artikel 42, stk. 7, i TEU finder anvendelse i tilfælde af omfattende og alvorlige hybridangreb og de praktiske virkninger heraf.

<u>Foranstaltning 21:</u> Den højtstående repræsentant vil i samarbejde med medlemsstaterne integrere, udnytte og koordinere den militære indsatskapacitet for at bekæmpe hybride trusler inden for rammerne af den fælles sikkerheds- og forsvarspolitik.

6. ØGET SAMARBEJDE MED NATO

Hybride trusler udgør en udfordring ikke bare for EU, men også for andre større partnerorganisationer, bl.a. De Forenede Nationer (FN), Organisationen for Sikkerhed og Samarbejde i Europa (OECD) og navnlig NATO. For at sikre en effektiv reaktion kræves der dialog og koordinering på både politisk og operationelt plan mellem organisationer. Et tættere samarbejde mellem EU og NATO ville sætte begge organisationer i stand til bedre at forberede sig på og reagere effektivt på hybride trusler på en måde, hvor de supplerer og gensidigt støtter hinanden på grundlag af princippet om deltagelse, samtidig med at der tages hensyn til hver organisations selvstændige beslutningstagning og databeskyttelsesregler.

De to organisationer har fælles værdier og står over for lignende udfordringer. Både EU-medlemsstaterne og NATO's allierede forventer af deres respektive organisationer, at de støtter dem, handler hurtigt, beslutsomt og på samordnet vis i tilfælde af en krise eller ideelt helt undgår, at der opstår en krise. Der er blevet indkredset en række områder med mulighed for et tættere samarbejde mellem EU og NATO, herunder situationsbevidsthed, strategisk kommunikation, IT-sikkerhed, kriseforebyggelse og kriseforanstaltninger. Den igangværende uformelle dialog mellem EU og NATO om hybride trusler skal styrkes for at synkronisere de to organisationers aktiviteter på dette område.

For at sikre, at EU's og NATO's reaktioner supplerer hinanden, er det vigtigt, at begge deler samme situationsbillede før og under krisen. Det kan ske gennem en regelmæssig udveksling af analyser og erfaringer, men også gennem direkte forbindelser mellem EU's enhed for analyse og udveksling af oplysninger om hybride trusler og NATO's enhed vedrørende hybride trusler. Det er ligeledes vigtigt at opbygge et gensidigt kendskab til hinandens respektive krisestyringsprocedurer for at sikre hurtige og effektive reaktioner. Det er muligt at øge modstandsdygtigheden ved at sikre komplementaritet ved fastsættelsen af benchmarks for kritiske dele af deres infrastruktur og et tæt samarbejde i forbindelse med strategisk kommunikation og cyberforsvar. Fælles øvelser på både politisk og teknisk plan vil gøre de to organisationers respektive beslutningsevne mere effektiv. Ved at undersøge mulighederne for andre uddannelsesaktiviteter vil der kunne opnås et sammenligneligt ekspertiseniveau på kritiske områder.

<u>Foranstaltning 22:</u> Den højtstående repræsentant vil i samarbejde med Kommissionen fortsætte den uformelle dialog og øge samarbejdet og koordineringen med NATO om situationsbevidsthed, strategisk kommunikation, IT-sikkerhed, kriseforebyggelse og

kriseforanstaltninger for at bekæmpe hybride trusler, samtidig med at principperne om ensartet deltagelse og hver organisations selvstændige beslutningstagning respekteres.

7. KONKLUSIONER

I denne fælles meddelelse skitseres en række foranstaltninger med henblik på at bekæmpe hybride trusler og øge modstandsdygtigheden på EU-plan og nationalt plan samt som partnere. Da der er fokus på at forbedre **situationskendskabet**, foreslås det at oprette en særlig mekanisme til udveksling af oplysninger med medlemsstaterne og koordinering af EU's kapacitet, hvad angår strategisk kommunikation. Der er redegjort for en række foranstaltninger for at **opbygge modstandsdygtighed** på områder såsom IT-sikkerhed, kritisk infrastruktur, beskyttelse af de finansielle systemer mod misbrug og bestræbelser for at bekæmpe voldelig ekstremisme og radikalisering. På hvert af disse områder vil første skridt være at gennemføre de strategier, som EU og medlemsstaterne er enedes om, samt medlemsstaternes fuldstændige gennemførelse af gældende lovgivning. Der foreslås ligeledes en række konkrete foranstaltninger i forlængelse af denne indsats.

Hvad angår indsatsen for at **forebygge krisesituationer, reagere på dem og komme på fode igen**, foreslås det at undersøge muligheden for at anvende solidaritetsbestemmelsen i artikel 222 i TEUF (som præciseret i den relevante afgørelse) og artikel 42, stk. 7, i tilfælde af omfattende og alvorlige hybridangreb. Kapaciteten til at træffe strategiske afgørelser skal øges ved at udforme en fælles operationel protokol.

Endelige foreslås det at **optrappe samarbejdet og koordineringen mellem EU og NATO** for i fællesskab at bekæmpe hybride trusler.

Ved gennemførelsen af denne fælles ramme vil den højtstående repræsentant og Kommissionen mobilisere de relevante EU-instrumenter, de hver især har til rådighed. Det er vigtigt for EU sammen med medlemsstaterne at arbejde for at mindske risiciene i forbindelse med potentielle hybride trusler fra statslige og ikkestatslige aktører.