Europaudvalget 2017
JOIN (2017) 0030
Offentligt

EUROPA-
KOMMISSIONEN

UNIONENS HØJTSTÅENDE
REPRÆSENTANT FOR
UDENRIGSANLIGGENDER
OG SIKKERHEDSPOLITIK

Bruxelles, den 19.7.2017
JOIN(2017) 30 final

FÆLLES RAPPORT TIL EUROPA-PARLAMENTET OG RÅDET

om gennemførelsen af den fælles ramme for imødegåelse af hybride trusler - Den Europæiske Unions indsats

1. INDLEDNING

EU står over for en af sine allerstørste sikkerhedsmæssige udfordringer nogensinde. Truslerne antager i tiltagende grad ikke-konventionelle former – nogle er rent fysiske trusler, såsom nye former for terrorisme, mens andre trusler er at finde i cyberspace i form af komplekse cyberangreb. Atter andre trusler er mere subtile i form af samfundsundergravende udøvelse af pression, bl.a. gennem misinformationskampagner og manipulering af medierne. Formålet hermed er at undergave europæiske kerneværdier, såsom menneskers værdighed, frihed og demokrati. Den seneste tids koordinerede cyberangreb verden over, som det er vanskeligt at placere ansvaret for, har vist os, hvor sårbare vores samfund og institutioner er.

Europa-Kommissionen og den højtstående repræsentant vedtog i april 2016 en fælles meddelelse om imødegåelse af hybride trusler[1] ("den fælles ramme"). I den fælles ramme anerkendes det, at hybride trusler er grænseoverskridende og komplekse, og det foreslås, at der anlægges en helhedsorienteret tilgang med inddragelse af hele statsapparatet ("whole-of-government approach") for derved at styrke den overordnede modstandsdygtighed i vores samfund. Rådet[2] udtrykte tilfredshed med initiativet og med de foreslåede foranstaltninger og opfordrede Kommissionen og den højtstående repræsentant til i juli 2017 at aflægge statusrapport. Selvom EU kan bistå medlemsstaterne i at opbygge modstandsdygtighed mod hybride trusler, er imødegåelse af hybride trusler først og fremmest medlemsstaternes ansvar, eftersom truslerne vedrører national sikkerhed og forsvar.

Den fælles ramme for imødegåelse af hybride trusler udgør en vigtig del af EU's samlede, integrerede tilgang til sikkerhed og forsvar. Den bidrager til at skabe et Europa, der yder beskyttelse, som Kommissionens formand, Jean-Claude Juncker, henstillede til i sin tale om Unionens tilstand i september 2016. I 2016 lagde EU også grundstenen til en stærkere europæisk forsvarspolitik som reaktion på borgernes forventninger om øget beskyttelse. I EU's globale strategi for udenrigs- og sikkerhedspolitik[3] uddybes behovet for en integreret tilgang for at kæde den interne modstandsdygtighed sammen med EU's optræden udadtil, og der opfordres til synergi mellem forsvarspolitikken og de politikker, der dækker det indre marked, erhvervslivet, de retshåndhævende myndigheder og efterretningstjenesterne. Efter vedtagelsen af den europæiske forsvarshandlingsplan i november 2016 har Kommissionen fremsat flere konkrete initiativer, der skal bidrage til at styrke EU's evne til at reagere på hybride trusler ved at opbygge modstandsdygtighed inden for forsvarsforsyningskæden og styrke det indre marked for forsvarsmateriel. Navnlig iværksatte Kommissionen den 7. juni 2017 Den Europæiske Forsvarsfond med en foreslået finansiering på 600 mio. EUR frem til 2020 og derefter 1,5 mia. EUR pr. år. I meddelelsen om sikkerhedsunionen[4] anerkendes behovet for at imødegå hybride trusler og vigtigheden af at sikre større sammenhæng mellem interne og eksterne foranstaltninger på sikkerhedsområdet.

[1] Fælles meddelelse til Europa-Parlamentet og Rådet: Fælles ramme for imødegåelse af hybride trusler - Den Europæiske Unions indsats (JOIN (2016) 18 final).
[2] Rådets konklusioner om imødegåelse af hybride trusler (pressemeddelelse 196/2016 af 19. april 2016).
[3] Forelagt for Det Europæiske Råd af den højtstående repræsentant den 28. juni 2016.
[4] COM(2016) 230 final af 20.4.2016.

EU's ledere har gjort sikkerhed og forsvar til et hovedspørgsmål i debatten om Europas fremtid[5]. Dette blev anerkendt i Romerklæringen af 25. marts 2017, som indeholder en vision for en tryg og sikker Union, der er fast besluttet på at styrke sin fælles sikkerhed og sit fælles forsvar. Det Europæiske Råds formand, Europa-Kommissionens formand og NATO's generalsekretær underskrev den 8. juli 2016 i Warszawa en fælles erklæring med det formål at puste nyt liv i det strategiske partnerskab mellem EU og NATO og give det fornyet substans. I den fælles erklæring opstilles der syv konkrete områder, hvor samarbejdet mellem de to organisationer bør styrkes, heriblandt også imødegåelse af hybride trusler. Efterfølgende gav EU og NATO deres opbakning til et fælles sæt på 42 gennemførelsesforslag, og der blev udgivet en første rapport i juni 2017, hvori det fremgik, at der er gjort betydelige fremskridt[6].

I Kommissionens oplæg om fremtiden for Europas forsvar[7], som blev forelagt i juni 2017, opridser Kommissionen tre forskellige scenarier for, hvordan man håndterer de stigende sikkerheds- og forsvarstrusler, som Europa står over for, og styrker Europas egen forsvarskapacitet inden 2025. I alle disse tre scenarier betragtes sikkerhed og forsvar som en integreret del af det europæiske projekt med hensyn til at beskytte og fremme vores interesser såvel hjemme som ude i verden. Europa er nødt til at blive garant for sikkerheden og at sørge for sin egen sikkerhed i højere grad fremover. Der er ingen medlemsstat, der på egen hånd kan klare de kommende udfordringer – og dette gælder ikke mindst udfordringen med at imødegå hybride trusler. Samarbejde på forsvars- og sikkerhedsområdet er derfor ikke blot en valgmulighed, det er en nødvendighed for at sikre et Europa, der kan yde beskyttelse.

Denne rapport har til formål at gøre status over fremskridtene og beskrive de næste skridt til indførelse af foranstaltningerne inden for de fire områder, der foreslås i den fælles ramme: at forbedre situationsbevidstheden; at opbygge større modstandsdygtighed; at øge medlemsstaternes og EU's kapacitet til at forebygge og reagere på krisesituationer og på samordnet vis at vende tilbage til normaltilstand; samt at øge samarbejdet med NATO med henblik på at sikre, at EU's og NATO's foranstaltninger supplerer hinanden. Rapporten bør sammenholdes med de månedlige statusrapporter om indførelsen af en effektiv og ægte sikkerhedsunion.

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

Hybride aktiviteter forekommer stadigt hyppigere i Europas sikkerhedsmæssige "landskab". Disse aktiviteter tiltager i intensitet, og der er voksende bekymring over indblanding i valgafholdelse, misinformationskampagner og ondsindede cyberaktiviteter og for, at gerningsmændene bag hybride aktiviteter skal forsøge at radikalisere udsatte medlemmer af samfundet og udnytte dem som stedfortrædere. Sårbarheden over for hybride trusler begrænses ikke af landegrænser. De hybride trusler kræver en samordnet reaktion også fra EU's og NATO's side. Udviklingen siden april 2016 har vist, at selv om trusler fortsat ofte vurderes isoleret, er der i Unionen en voksende erkendelse og forståelse af, at nogle af

[5] Bratislavakøreplanen, som blev vedtaget af Det Europæiske Råd den 16. september 2016, samt Romerklæringen, som blev vedtaget af lederne af 27 medlemsstater og af Det Europæiske Råd, Europa-Parlamentet og Europa-Kommissionen den 25. marts 2017.

[6] http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-conclusions-eu-nato-cooperation

[7] Oplæg om fremtiden for det europæiske forsvar af 7.6.2017, https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_da.pdf

aktiviteterne er hybride, og at der er behov for en koordineret indsats. EU vil fortsætte sine bestræbelser på at forbedre situationsbevidstheden og øge samarbejdet.

Foranstaltning 1: 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.

Rådet har oprettet Gruppen af Formandskabets Venner bestående af eksperter fra medlemsstaterne, som skal udarbejde en generisk undersøgelse, der skal give dem bedre mulighed for at finde frem til de vigtigste indikatorer for hybride trusler, indarbejde disse indikatorer både i mekanismer for tidlig varsling og i de eksisterende mekanismer til risikovurdering og udveksle dem indbyrdes, efter behov. Kommissoriet er blevet aftalt, og arbejdet er allerede indledt. Den generiske undersøgelse forventes at være klar ved udgangen af 2017, hvorefter den vil blive iværksat. Beskyttelsen mod hybride trusler bør være gensidigt forstærkende for EU og NATO. Medlemsstaterne opfordres derfor til at udføre disse undersøgelser så hurtigt som muligt, da de vil give værdifulde oplysninger om omfanget af sårbarhed og beredskab i hele Europa.

a. FORBEDRING AF SITUATIONSBEVIDSTHEDEN

Udveksling af efterretningsanalyser og vurderingsarbejde er et vigtigt redskab til at mindske usikkerheden og styrke situationsbevidstheden. Der er gjort betydelige fremskridt i det forløbne år. EU's analyseenhed for hybride trusler (EU Hybrid Fusion Cell) er blevet oprettet og er nu fuldt operationel, den østlige taskforce for strategisk kommunikation (East StratCom) er etableret og Finland har iværksat det europæiske center til imødegåelse af hybride trusler. En stor del af indsatsen har være fokuseret på at analysere, hvilke redskaber og hjælpemidler der benyttes til propaganda eller misinformation, med et godt samarbejde mellem EU's østlige taskforce for strategisk kommunikation, EU's analyseenhed for hybride trusler og NATO. Dette udgør et solidt grundlag for at fortsætte opbygningen af en mere velforankret kultur, hvor trusler mod vores indre og ydre sikkerhed analyseres og vurderes som værende hybride trusler.

EU's analyseenhed for hybride trusler

Foranstaltning 2: Oprettelse af en analyseenhed for hybride trusler inden for EU's eksisterende Efterretningsanalysecenter (EU INTCEN), der kan modtage og analysere klassificerede og offentligt tilgængelige oplysninger om hybride trusler. Medlemsstaterne opfordres til at oprette nationale kontaktpunkter for hybride trusler for at sikre samarbejde og sikker kommunikation med EU's analyseenhed for hybride trusler.

EU's analyseenhed for hybride trusler blev oprettet inden for EU's Efterretningsanalysecenter med det formål at modtage og analysere klassificerede og offentligt tilgængelige oplysninger fra forskellige interessenter vedrørende hybride trusler. Analyserne udveksles derefter internt i EU og blandt medlemsstaterne og tjener som vidensgrundlag for EU's beslutningsprocesser, herunder som input til risikovurderinger på EU-plan. Efterretningsafdelingen under EU's Militærstab (EUMS INT) bidrager med militære analyser til det arbejde, EU's analyseenhed for hybride trusler udfører. Der er hidtil udarbejdet over 50 vurderinger og briefinger vedrørende hybride trusler. Enheden har siden januar 2017 udgivet tidsskriftet "Hybrid

Bulletin", som indeholder analyser af aktuelle trusler, heriblandt også hybride trusler, og som rundsendes internt i EU's institutioner og organer samt til nationale kontaktpunkter[8]. Analyseenheden nåede som planlagt fuld operativ kapacitet i maj 2017. Og endelig pågår der samvirke på medarbejderniveau med NATO's nyoprettede afdeling for analyse af hybride trusler ("Hybrid Analysis Branch"), som omfatter dels udveksling af de erfaringer, der er indhøstet i forbindelse med opbygningen af EU's analyseenhed for hybride trusler, dels udveksling af oplysninger (dog under behørig iagttagelse af EU's regler om klassificerede oplysninger). EU's analyseenhed for hybride trusler arbejder p.t. på at formulere yderligere initiativer til at øge samarbejdet fremover, og den vil spille en nøglerolle i de parallelt løbende øvelser, som EU og NATO planlægger at afholde i efteråret 2017, og hvor enhedens reaktionsevne vil blive testet og de indhøstede erfaringer vil blive indarbejdet.

Strategisk kommunikation

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

I løbet af de seneste måneder er der gjort øget brug af misinformationskampagner og systematisk spredning af falske nyheder på sociale medier som metoder til at underminere modstandere. Ved brug af sociale medier som foretrukken platform kan påstande, der umiddelbart virker pålidelige og sandfærdige, ændre folkeopinionen til fordel for bestemte personer, organisationer eller myndigheder. Disse hybride taktikker har et bredere mål om at skabe forvirring i vores samfund og miskreditere demokratiske regeringer og vores strukturer, institutioner og valgafholdelse. Falske nyheder bliver typisk spredt via onlineplatforme (jf. tillige foranstaltning 17). Kommissionen og den højtstående repræsentant bifalder de seneste skridt fra onlineplatformes og nyhedsmediers side til bekæmpelse af misinformation. Kommissionen vil fortsat tilskynde til sådanne frivillige foranstaltninger.

Den højtstående repræsentant har oprettet den østlige taskforce for strategisk kommunikation, som forudser og reagerer på misinformationsepisoder og -kampagner. Dette har forbedret kommunikationen om Unionens politik i de østlige nabolande væsentligt og har samtidig styrket mediernes vilkår i disse lande. Taskforcen har i løbet af de seneste to år afsløret over 3 000 tilfælde af misinformation på 18 forskellige sprog. Den kommende lancering af et nyt websted, "#EUvsdisinformation", med en online søgefunktion vil give væsentligt bedre brugeradgang. Men undersøgelser og analyser har vist, at antallet af misinformationskanaler og -budskaber pr. døgn er betydeligt højere. EU-STRAT-projektet, som finansieres under Horisont 2020, analyserer politikker og medier i de lande, der indgår i Det Østlige Partnerskab.

Den højtstående repræsentant opfordrer medlemsstaterne til at støtte det arbejde, der udføres af taskforcerne for strategisk kommunikation, med henblik på at imødegå stigningen i hybride trusler mere effektivt. Dette vil hjælpe den sydlige taskforce for strategisk kommunikation (South StratCom) til at forbedre sin kommunikation med og sine henvendelser til den arabiske verden (bl.a. på arabisk), aflive myter samt udbrede kendskabet til Den Europæiske Union og dens politikker. Samspillet med lokale journalister vil være med til at sikre, at det journalistiske produkt bliver kulturelt tilpasset. De to taskforcer har til formål, med hjælp fra

[8] Hidtil har 21 medlemsstater udpeget nationale kontaktpunkter. Disse kontaktpunkter er personer i medlemsstaternes hovedstæder, der arbejder med politik og modstandsdygtighed.

EU's analyseenhed for hybride trusler, at støtte og supplere medlemsstaternes bestræbelser på dette område. Endvidere samfinansierer Kommissionen det europæiske strategiske kommunikationsnet (ESCN), som er et samarbejdsnetværk bestående af 26 medlemsstater, som udveksler analyser, gode praksisser og idéer vedrørende anvendelsen af strategisk kommunikation til bekæmpelse af voldelig ekstremisme samt vedrørende misinformation.

Ekspertisecenter for imødegåelse af hybride trusler

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

Som reaktion på opfordringen til at oprette et ekspertisecenter iværksatte Finland i april 2017 det europæiske center til imødegåelse af hybride trusler. Centrets medlemmer er ti af EU's medlemsstater[9] plus Norge og USA, og såvel EU som NATO er blevet opfordret til at støtte styringskomitéen[10]. Centrets mission er at fremme strategisk dialog og i samarbejde med interessegrupper at bedrive forskning og foretage analyser med henblik på at opbygge større modstandsdygtighed og evne til at reagere og således at bidrage til at imødegå hybride trusler. Centret forventes desuden at tjene som skueplads for kommende øvelser knyttet til hybride trusler. Centret har allerede etableret tæt kontakt med EU's analyseenhed for hybride trusler, og de to organisationers arbejde bør supplere hinanden. EU vurderer for øjeblikket, hvordan den kan yde konkret støtte til centret.

b. OPBYGNING AF MODSTANDSDYGTIGHED

Den fælles ramme bringer spørgsmålet om modstandsdygtighed (såsom trusler imod infrastruktur for transport, kommunikation, energiforsyning, finansverdenen eller regional sikkerhed) i centrum for EU's foranstaltninger med henblik på at modvirke propaganda- og misinformationskampagner, forsøg på at undergrave erhvervsmæssige, samfundsmæssige og økonomiske strømme samt angreb på IT- og internetbaseret infrastruktur. Udgangspunktet herfor er, at en styrkelse af modstandsdygtigheden udgør en forebyggende og afskrækkende foranstaltning med henblik på at befæste samfundene og undgå optrapning af krisesituationer både i og uden for EU. EU's merværdi ligger i at bistå medlemsstaterne og partnere med at opbygge deres modstandsdygtighed ved brug af en bred vifte af eksisterende instrumenter og programmer. Der er gjort betydelige fremskridt i foranstaltningerne for at opbygge modstandsdygtighed på områder såsom cybersikkerhed, kritisk infrastruktur, beskyttelse af de finansielle systemer mod misbrug og bestræbelser på at bekæmpe voldelig ekstremisme og radikalisering.

Beskyttelse af kritisk infrastruktur

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

Inden for rammerne af det europæiske program for beskyttelse af kritisk infrastruktur (EPCIP) har Kommissionen videreført arbejdet med at finde frem til fælles redskaber, herunder

[9] Det Forenede Kongerige, Estland, Finland, Frankrig, Letland, Litauen, Polen, Spanien, Sverige og Tyskland.
[10] Centret er åbent for deltagelse af andre EU-medlemsstater og NATO-allierede.

sårbarhedsindikatorer, med henblik på at øge den kritiske infrastrukturs modstandsdygtighed mod hybride trusler i relevante sektorer. Kommissionen afholdt i maj 2017 en workshop om hybride trusler mod kritisk infrastruktur med deltagelse af næsten alle medlemsstater, operatører af kritisk infrastruktur og EU's analyseenhed for hybride trusler og med NATO som observatør. Her blev der indgået aftale om en fælles køreplan og fælles skridt for arbejdet fremover på baggrund af en rundspørge, som var blevet sendt til medlemsstaternes nationale myndigheder. Kommissionen vil foretage yderligere høringer med interessenterne i efteråret med henblik på at nå til enighed om indikatorerne inden udgangen af 2017.

Det Europæiske Forsvarsagentur (EDA) arbejder på at finde frem til mangler i den fælles kapacitet og forskning, som opstår i skæringspunktet mellem energiinfrastruktur og forsvarskapacitet. Det Europæiske Forsvarsagentur vil udarbejde et oplæg i løbet af efteråret 2017 og skabe pilotprojekter til helhedsorienterede metoder.

Forbedring af EU's energiforsyningssikkerhed

Foranstaltning 6: Kommissionen vil i samarbejde med medlemsstaterne støtte bestræbelserne på at diversificere energikilderne og fremme sikkerhedsnormerne, således at den nukleare infrastrukturs modstandsdygtighed øges.

Kommissionen fremsatte i december 2016 konkrete forslag i pakken om energiforsyningssikkerhed, og Rådet og Europa-Parlamentet nåede i april 2017 til enighed om den nye forordning om gasforsyningssikkerhed, hvis formål er at forhindre gasforsyningskriser. De nye regler vil sikre regional koordinering af og en fælles tilgang til forsyningssikkerhedsforanstaltninger blandt medlemsstaterne. Dette vil give EU et bedre udgangspunkt for at berede sig på og håndtere gasmangel, krisesituationer eller hybridangreb. Som noget helt nyt vil solidaritetsprincippet finde anvendelse: medlemsstaterne vil kunne bistå deres nabolande i tilfælde af en alvorlig krisesituation eller et angreb, således at Europas husstande og virksomheder ikke rammes af strømsvigt.

EU har også gjort fremskridt med at udvikle vigtige projekter, der skal diversificere EU's energiforsyningsruter og -kilder i overensstemmelse med rammestrategien for energiunionen og den europæiske energisikkerhedsstrategi. Eksempelvis pågår der konkrete bygge- og anlægsarbejder inden for den sydlige gaskorridor i forbindelse med alle større rørledningsprojekter: udvidelse af den sydkaukasiske, den transanatolske og den transadriatiske rørledning, Shah Deniz II opstrøms samt udvidelse af den sydlige gaskorridor til Centralasien, herunder navnlig til Turkmenistan. Importen af flydende naturgas til Europa er stigende og kommer fra nye kilder, bl.a. fra USA. Eksemplet fra terminalen i Litauen viser, hvordan diversificeringsprojekter kan mindske afhængigheden af én enkelt leverandør. Styrkelse af indsatsen på energiområdet og bedre udnyttelse af egne energikilder, navnlig vedvarende energikilder, bidrager også til at diversificere energiruterne og -kilderne.

For så vidt angår nuklear sikkerhed yder Kommissionen aktiv støtte – navnlig gennem workshops med nationale myndigheder og reguleringsorganer – til en ensartet og effektiv gennemførelse af de to direktiver om nuklear sikkerhed og grundlæggende sikkerhedsnormer, som medlemsstaterne skal have gennemført inden udgangen af henholdsvis 2017 og 2018. Herudover bidrager Euratom-programmet for forskning og uddannelse til at forbedre den nukleare sikkerhed.

Transportsikkerhed og sikkerhed i forsyningskæden

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

I overensstemmelse med meddelelsen om sikkerhedsunionen fremmer Kommissionen udførelsen af sikkerhedsrisikovurderinger på EU-plan sammen med medlemsstaterne, EU's Efterretningsanalysecenter og relevante agenturer med henblik på at opdage trusler mod transportsikkerheden og støtte udviklingen af effektive og forholdsmæssige beskyttelsesforanstaltninger. Nedskydningen af Malaysian Airlines' fly MH17 over det østlige Ukraine i 2014 bragte fokus på risikoen ved at overflyve konfliktområder. I overensstemmelse med henstillingerne fra den europæiske taskforce på højt plan om konfliktområder[11] har Kommissionen udarbejdet en metode for en "fælles EU-risikovurdering" med støtte fra nationale luftfarts- og sikkerhedseksperter og fra EU-Udenrigstjenesten, hvilket giver mulighed for at udveksle klassificerede oplysninger og fastlægge et fælles risikobillede. Det Europæiske Luftfartssikkerhedsagentur (EASA) udsendte i marts 2017 den første orientering om konfliktområder ("Conflict Zones Information Bulletin")[12] på grundlag af resultaterne af EU's fælles risikovurdering. Kommissionen overvejer at udvide risikovurderingerne af luftfartssikkerheden til også at omfatte andre transportformer (f.eks. jernbanetrafik og søfart) og vil fremsætte forslag herom i 2018. Kommissionen, EU-Udenrigstjenesten og medlemsstaterne iværksatte i juni 2017 en risikovurderingsøvelse vedrørende jernbanesikkerhed med henblik på at identificere mangler og mulige foranstaltninger til afbødning af risici.

Der er gjort en betydelig indsats for luftfartssikkerhed og lufttrafikstyring i sikkerhedsforskningsprojekter under det syvende rammeprogram og Horisont 2020. Inden for den civile luftfart udarbejder Kommissionen sammen med EASA og andre interessenter to nye initiativer, der skal forstærke cybersikkerheden og imødegåelsen af hybride trusler: oprettelsen af IT-beredskabsenheden for luftfart og en taskforce for cybersikkerhed i fællesforetagendet til forskning i lufttrafikstyring i det fælles europæiske luftrum (SESAR) med ansvar for lufttrafikstyring i det fælles europæiske luftrum. Det Europæiske Forsvarsagentur yder militært input om cybersikkerhed inden for luftfart til fællesforetagendet SESAR og til EASA gennem den europæiske strategiske koordineringsplatform for cybersikkerhed, der efter anmodning fra medlemsstaterne og erhvervslivet vil bistå med koordinering på EU-plan af alle aktiviteter inden for luftfart. I overensstemmelse med køreplanen for cybersikkerhed inden for luftfart udførte EASA i 2016 analyser af mangler i de nuværende regler og især definitionen og oprettelsen af Det Europæiske Center for Cybersikkerhed inden for Luftfart (ECCSA). ECCSA er nu taget i drift og udarbejder i samarbejde med EU's IT-beredskabsenhed (CERT-EU; aftalememorandum blev underskrevet i februar 2017) trusselsanalyser inden for luftfart og samarbejder med Eurocontrol (køreplan for samarbejde er vedtaget), og der er blevet udviklet et websted for distribution af offentligt

[11] https://www.easa.europa.eu/system/files/dfu/208599_EASA_CONFLICT_ZONE_CHAIRMAN_REPORT_no_B_update.pdf

[12] https://ad.easa.europa.eu/czib-docs/page-1

tilgængelige analyser. Senest i august 2017 vil der blive vedtaget et standardiseringsprogram og et system for sikker udveksling af oplysninger.

Toldrisikostyring

På toldområdet fokuserer Kommissionen på en omfattende opgradering af systemet til forudgående fragtinformation og toldrisikoforvaltningssystemet. Dette omfatter hele spektret af toldrisici, herunder risici forbundet med trusler mod internationale forsyningskæders sikkerhed og integritet og mod relevant kritisk infrastruktur (f.eks. direkte trusler mod havneanlæg, lufthavne eller landegrænser, som hidrører fra import). Hensigten med opgraderingen er at sikre, at toldmyndighederne i EU får alle nødvendige fragtoplysninger fra de handlende; at de kan udveksle disse oplysninger mere effektivt medlemsstaterne imellem; at de anvender både de fælles regler og de regler, der er gælder specifikt for de pågældende medlemsstater; og at de kan fokusere mere effektivt på risikobetonede forsendelser gennem intensiveret samarbejde med andre myndigheder, navnlig med andre retshåndhævende myndigheder og sikkerhedstjenester. Den udvikling på IT-området, som er nødvendig for, at Kommissionen kan foretage opgraderingen, befinder sig endnu på forstadiet, og de relevante investeringer på centralt plan vil blive iværksat i de kommende måneder.

Verdensrummet

Foranstaltning 8: Inden for rammerne af rumstrategien 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.

I forbindelse med udarbejdelsen af den reguleringsmæssige ramme for statslig satellitkommunikation (GOVSATCOM) samt overvågning og sporing i rummet i 2018 vil Kommissionen medtage modstandsdygtighed mod hybride trusler i sin vurdering. I overensstemmelse med rumstrategien vil Kommissionen i forbindelse med videreudviklingen af Galileo og Copernicus vurdere disse tjenesters potentiale for at medvirke til at begrænse sårbarheden i kritisk infrastruktur. Evalueringsrapporten forventes at være klar i efteråret 2017, og forslaget om den næste generation af Copernicus og Galileo forventes at være klart i 2018. Det Europæiske Forsvarsagentur deltager i samarbejdsprojekter vedrørende kapacitetsudvikling inden for kommunikation i rummet, militær positionsbestemmelse, navigation og timing og jordobservation. Alle projekterne vil have fokus på krav om modstandsdygtighed set i lyset af aktuelle og begyndende hybride trusler.

Forsvarskapacitet

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.

I 2016 og 2017 gennemførte Det Europæiske Forsvarsagentur sammen med Kommissionen, EU-Udenrigstjenesten og eksperter fra medlemsstaterne tre skrivebordsøvelser om scenarier i forbindelse med hybride trusler. Deres konklusioner vil tjene som input ved revisionen af kapacitetsudviklingsplanen, således at de vigtigste punkter for kapacitetsudvikling, som resulterer heraf, og som er nødvendige for at imødegå hybride trusler, indarbejdes i EU's nye

prioriteter for kapacitetsudvikling. I forbindelse med revisionen af behovskataloget for 2005 vil der blive taget hensyn til hybride trusler. I april 2017 færdiggjorde Det Europæiske Forsvarsagentur en analyserapport om militære virkninger af hybridangreb rettet mod kritisk havneinfrastruktur, som vil blive genstand for drøftelser under en workshop med søfartseksperter i oktober 2017. Yderligere en specifik analyse af den militære rolle i forbindelse med bekæmpelse af minidroner er planlagt til 2018. Hertil kommer, at kapacitetsmæssige prioriteter med det formål at styrke modstandsdygtigheden mod de hybride trusler, som medlemsstaterne har identificeret, også kan være berettigede til støtte under Den Europæiske Forsvarsfond fra 2019. Kommissionen opfordrer Europa-Parlamentet og Rådet til at sørge for en hurtig vedtagelse og opfordrer medlemsstaterne til at fremsætte forslag til kapacitetsprojekter for at styrke EU's modstandsdygtighed mod hybride trusler.

Foranstaltning 10: 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.

Med henblik på at styrke beredskabet og modstandsdygtigheden mod hybride trusler, herunder kapacitetsopbygning inden for fødevare- og sundhedssystemer, støtter Kommissionen medlemsstaterne gennem uddannelse og simuleringsøvelser og ved at fremme retningslinjer for udveksling af erfaringer og finansiering af fælles aktioner. Dette sker navnlig under EU-rammen for sundhedssikkerhed om alvorlige grænseoverskridende sundhedstrusler og under folkesundhedsprogrammet om at gennemføre det internationale sundhedsregulativ, en lovgivningsmæssig søjle, der er bindende for 196 lande, deriblandt medlemsstaterne, og som har til formål at forebygge og reagere på akutte grænseoverskridende sundhedsrisici på verdensplan. For at teste det tværsektorielle beredskab og den tværsektorielle reaktionsevne i sundhedssektoren vil Kommissionens tjenestegrene i efteråret 2017 gennemføre en øvelse om komplekse og flerdimensionelle hybride trusler. Kommissionen og medlemsstaterne er ved at udarbejde en fælles aktion om vaccination, som omfatter prognoser for udbud af og efterspørgsel på vacciner samt forskning i innovative fremstillingsprocesser inden for vaccineproduktion med henblik på at styrke vaccineudbuddet og forbedre sundhedssikkerheden på EU-plan (2018-2020). Kommissionen samarbejder ligeledes med Den Europæiske Fødevaresikkerhedsautoritet og Det Europæiske Center for Forebyggelse af og Kontrol med Sygdomme for at tilpasse sig til nye, mere effektive videnskabelige forskningsteknikker, for mere præcist at kunne opdage og spore sundhedstrusler og dermed hurtigt at kunne bringe udbrud mod fødevaresikkerheden under kontrol. Kommissionen har etableret det globale netværk for samarbejde inden for forskning i beredskab mod smitsomme sygdomme (GloPID-R), som er et netværk af forskningssponsorer, med henblik på at kunne mobilisere et samordnet forskningsberedskab inden for 48 timer i tilfælde af alvorlige udbrud.

Foranstaltning 11: Kommissionen opfordrer medlemsstaterne til at prioritere oprettelsen og fuld udnyttelse af et netværk af de 28 nationale CSIRT'er og IT-beredskabsenheden for EU-institutioner, -organer og -agenturer (CERT-EU) og en ramme for strategisk samarbejde. Kommissionen bør i samarbejde med medlemsstaterne sikre, at sektorinitiativer vedrørende cybertrusler (f.eks. inden for luftfart, energi og søfart) 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.

Den seneste tids globale cyberangreb, hvorved ransomware og malware er blevet anvendt til at sætte tusindvis af computersystemer ud af funktion, har på ny understreget det presserende behov for at optrappe EU's modstandsdygtighed over for cyberangreb og

sikkerhedsforanstaltninger. Som bebudet i midtvejsevalueringen af strategien for det digitale indre marked reviderer Kommissionen og den højtstående repræsentant for øjeblikket EU's strategi for cybersikkerhed fra 2013, navnlig ved vedtagelse af en pakke, planlagt til september 2017. Målet vil være at sikre en mere effektiv tværsektoriel reaktion på disse trusler og derved skabe større tillid i det digitale samfund og den digitale økonomi. Den vil også revidere mandatet for EU's Agentur for Net- og Informationssikkerhed (ENISA) for at fastlægge agenturets rolle i det forandrede "økosystem" for cybersikkerhed. Det Europæiske Råd[13] bifaldt Kommissionens hensigt om at tage strategien for cybersikkerhed op til fornyet behandling.

Vedtagelsen af direktivet om net- og informationssikkerhed[14] i juli 2016 udgjorde en vigtig milepæl hen imod opbygningen af modstandsdygtighed over for cyberangreb på EU-plan. I direktivet er der fastsat de første EU-dækkende regler for cybersikkerhed, en forbedring af cybersikkerhedskapaciteten samt en styrkelse af samarbejdet mellem medlemsstaterne. Direktivet indeholder desuden krav om, at virksomheder inden for kritiske sektorer skal træffe passende sikkerhedsforanstaltninger og indberette alvorlige cyberhændelser til den relevante nationale myndighed. Det drejer sig bl.a. om sektorerne for energi, transport, vand, sundhed, bankvæsen og finansiel markedsinfrastruktur. Det vil blive pålagt onlinemarkedspladser, cloudcomputing-tjenester og søgemaskiner at træffe lignende tiltag. Konsekvent gennemførelse på tværs af sektorer og grænser vil blive sikret af samarbejdsgruppen for net- og informationssikkerhed, som Kommissionen oprettede i 2016, og som har til opgave at modvirke opsplitning af markedet. I den forbindelse betragtes direktivet om net- og informationssikkerhed som referenceramme for alle sektorspecifikke initiativer inden for cybersikkerhed. Ifølge direktivet skal der desuden skabes et netværk af enheder, der håndterer cybersikkerhedshændelser (det såkaldte CSIRT-netværk), som samler alle relevante interessenter. Sideløbende hermed overvåger Kommissionen og CERT-EU aktivt cybertruslen og udveksler oplysninger med de nationale myndigheder for at sikre, at EU-institutionernes IT-systemer er sikre og modstandsdygtige over for cyberangreb. I maj 2017 indtraf et angreb med ransomwaren "WannaCry", hvilket muliggjorde, at netværket for første gang kunne udføre operationel udveksling af oplysninger og samarbejde ved at formidle rådgivning. EU's IT-beredskabsenhed har været i tæt kontakt med Europols Europæiske Center til Bekæmpelse af IT-Kriminalitet (EC3), de berørte landes enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er), enheder for cyberkriminalitet samt vigtige partnere inden for erhvervslivet for at mindske truslen og bistå ofre. Udvekslingen af nationale situationsrapporter affødte en fælles situationsbevidsthed for hele EU. Takket være denne erfaring var netværket bedre forberedt på de efterfølgende hændelser (f.eks. "NonPetya"). Der blev også konstateret en række udfordringer, som nu søges løst.

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

I juli 2016 indgik Kommissionen og erhvervslivet, i samarbejde med medlemsstaterne, et kontraktmæssigt offentlig-privat partnerskab om cybersikkerhed, som indebærer investeringer på op til 450 mio. EUR under EU's forsknings- og innovationsprogram Horisont 2020 med

[13] Det Europæiske Råds konklusioner af 22.-23. juni 2017.
[14] Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016, s. 1).

henblik på at udvikle og teste teknologier, der yder brugerne og infrastrukturen bedre beskyttelse mod cybertrusler og hybride trusler. Partnerskabet mundede ud i den første fælleseuropæiske strategiske forskningsdagsorden, som fokuserede på at styrke modstandsdygtigheden i kritisk infrastruktur og at beskytte borgere mod cyberangreb. Partnerskabet afstedkom en øget koordinering interessenterne imellem, hvilket førte til produktivitets- og effektivitetsgevinster i finansieringen af cybersikkerhed under Horisont 2020. Partnerskabet opererer parallelt på spørgsmål vedrørende cybersikkerhedscertificering for informations- og kommunikationsteknologi samt på, hvordan man afhjælper den akutte mangel på fagfolk på markedet, som er kvalificerede inden for cybersikkerhed. Grundet det store behov for civil forskning og forsvarets behov for høj modstandsdygtighed bidrager Det Europæiske Forsvarsagenturs gruppe for IT-forskning og -teknologi til forskningen inden for de områder, der er blevet udpeget af Den Europæiske Organisation for Cybersikkerhed (ECSO) i dennes strategiske forsknings- og innovationsdagsorden.

Foranstaltning 13: Kommissionen vil udstede retningslinjer, så ejerne af intelligente net kan forbedre cybersikkerheden i deres anlæg. I forbindelse med initiativet vedrørende en ny udformning af elmarkedet vil Kommissionen overveje at foreslå "risikoberedskabsplaner" og procedureregler med henblik på udveksling af oplysninger og for at sikre solidaritet mellem medlemsstaterne i krisesituationer, herunder regler om, hvordan cyberangreb kan forebygges og afbødes.

Inden for energisektoren er Kommissionen i færd med at udarbejde en sektorstrategi om cybersikkerhed med oprettelsen af en cybersikkerhedsplatform for energieksperter for at styrke gennemførelsen af direktivet om net- og informationssikkerhed. I en undersøgelse i februar 2017 blev der udpeget bedste tilgængelige teknikker med henblik på at højne niveauet for cybersikkerhed af intelligente målersystemer til støtte for denne platform. Kommissionen oprettede også en webbaseret platform, "EU-Center for Udveksling af Oplysninger om Hændelser og Trusler", som analyserer og udveksler oplysninger om cybertrusler og -hændelser inden for energisektoren.

Forbedring af finanssektorens modstandsdygtighed over for hybride trusler

Foranstaltning 14: Kommissionen vil i samarbejde med ENISA[15], 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.

I anerkendelse af, at cybertrusler er blandt de største risici for den finansielle stabilitet, har Kommissionen gennemgået den reguleringsmæssige ramme for betalingstjenester i Den Europæiske Union, som nu er under gennemførelse. I kraft af det reviderede direktiv om betalingstjenester[16] blev der indført nye bestemmelser for at højne sikkerheden ved betalingsinstrumenter samt stærk kundeautentifikation med henblik på at reducere svig, især i forbindelse med onlinebetalinger. Den nye lovgivningsramme træder i kraft i januar 2018. Med bistand fra Den Europæiske Banktilsynsmyndighed og i samråd med interessenterne udarbejder Kommissionen for øjeblikket reguleringsmæssige tekniske standarder for stærk kundeautentifikation samt fælles og sikker kommunikation for at operationalisere sikkerheden

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

[16] Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked, om ændring af direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om ophævelse af direktiv 2007/64/EF (EUT L 337 af 23.12.2015, s. 35).

i betalingstransaktioner, og disse standarder forventes at blive offentliggjort ved udgangen af 2017. Internationalt har Kommissionen endvidere arbejdet tæt sammen med de respektive G7-partnere om "G7-landenes grundlæggende principper om cybersikkerhed i finanssektoren", som i oktober 2016 blev godkendt af G7-landenes finansministre og centralbankdirektører. Disse principper er udformet med henblik på enheder i finanssektoren (private og offentlige) og bidrager til en koordineret tilgang til cybersikkerhed i finanssektoren for i fællesskab at bekæmpe cybertrusler, bl.a. fra cyberangreb, som bliver stadigt flere og stadigt mere udspekulerede.

Transport

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

Gennemførelsen af handlingsplanen for EU's strategi for maritim sikkerhed[17] vil bidrage til at nedbryde silomentaliteten med hensyn til informationsudveksling og fælles udnyttelse af aktiver mellem civile og militære myndigheder. Den helhedsorienterede tilgang med inddragelse af hele statsapparatet ("whole-of-government approach") har ført til øget tværgående samarbejde mellem forskellige aktører. Kommissionen og EU-Udenrigstjenesten forventer at færdiggøre en fælles civil-militær strategisk forskningsdagsorden ved udgangen af 2017 med en afsluttende workshop om beskyttelse af kritisk maritim infrastruktur. Dette arbejde kunne i fremtiden udvides til at dække den begyndende trussel mod undersøiske rørledninger, energioverførsel, fiberoptiske og traditionelle kommunikationskabler i form af forstyrrelse kommende uden for de nationale territorialfarvande.

I en undersøgelse[18] for nylig blev risikovurderingskapaciteten evalueret blandt nationale myndigheder, der udfører kystvagtfunktioner. Undersøgelsen indeholdt de største hindringer for samarbejde og anbefalede praktiske måder til at forbedre samarbejdet mellem maritime myndigheder på EU-plan og på nationalt plan på dette specifikke område. Risikovurdering er af afgørende betydning for imødegåelsen af maritime trusler og endnu vigtigere i forbindelse med evaluering og forebyggelse af hybride trusler, eftersom disse kræver endnu flere og mere komplekse overvejelser. Resultaterne af denne undersøgelse vil blive fremlagt i forskellige fora med tilknytning til kystvagtfunktioner, så de foreslåede henstillinger kan vurderes og gennemføres med henblik på at øge samarbejdet på dette område med beredskab og reaktion på hybride trusler som hovedmål.

Bekæmpelse af finansiering af terrorisme

Foranstaltning 16: Kommissionen vil anvende gennemførelsen af handlingsplanen for bekæmpelse af finansiering af terrorisme til også at imødegå hybride trusler.

Gerningsmændene bag hybride trusler og deres støtter kræver finansiering for at kunne gennemføre deres planer. EU's indsats mod kriminalitet og finansiering af terrorisme under den europæiske dagsorden om sikkerhed og handlingsplanen for bekæmpelse af finansiering

[17] https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf og den 2. rapport om gennemførelsen af handlingsplanen for EUMSS, som blev forelagt for medlemsstaterne den 21. juni 2017.

[18] "Evaluation of risk assessment capacity at the level of Member States' authorities performing coast guard functions", 2017, https://ec.europa.eu/maritimeaffairs/documentation/studies.

af terrorisme kan også bidrage til at imødegå hybride trusler. Kommissionen fremsatte i december 2016 tre lovgivningsforslag, heriblandt forslag om strafferetlige sanktioner for hvidvaskning af penge og ulovlige kontantbetalinger samt indefrysning og konfiskation af aktiver[19].
Samtlige medlemsstater skal senest den 26. juni 2017 have gennemført det fjerde direktiv om bekæmpelse af hvidvaskning af penge[20], og i juli 2016 fremsatte Kommissionen et målrettet lovgivningsforslag med henblik på at supplere og forstærke direktivet med yderligere foranstaltninger[21].

Den 26. juni 2017 fremlagde Kommissionen den overnationale risikovurdering i henhold til det fjerde direktiv om bekæmpelse af hvidvaskning af penge. Kommissionen fremsatte desuden et forslag til en forordning om at forhindre import og oplagring i EU af kulturgenstande, der er blevet ulovligt udført fra tredjelande[22]. Senere på året vil Kommissionen aflægge rapport om sin løbende vurdering af behovet for eventuelle yderligere foranstaltninger for at spore finansieringen af terrorisme i EU. Kommissionen reviderer desuden lovgivningen om bekæmpelse af svig og forfalskning i forbindelse med andre betalingsmidler end kontanter[23].

Den ottende statusrapport om indførelsen af en effektiv og ægte sikkerhedsunion indeholder nærmere oplysninger om status over gennemførelsen af handlingsplanen om bekæmpelse af terrorfinansiering.

Fremme af EU's fælles værdier og af inklusive, åbne og robuste samfund

Opbygning af modstandsdygtighed over for radikalisering og voldelig ekstremisme

Religiøs og ideologisk radikalisering, etniske konflikter og konflikter mellem minoritetsgrupper kan anstiftes af udefrakommende aktører gennem støtte til bestemte grupper eller bestræbelser på at optrappe konflikter mellem grupper. Der er fremkommet yderligere udfordringer, bl.a. trusler fra soloaktører, nye metoder til radikalisering, herunder i forbindelse med migrationskrisen, højreekstremisme (herunder vold mod indvandrere) og risiko for polarisering. Selv om arbejdet vedrørende radikalisering drives fremad inden for rammerne af sikkerhedsunionen, kan det også indirekte være relevant for arbejde med hybride trusler, idet personer, der er sårbare over for radikalisering, også kan blive manipuleret af gerningsmændene bag hybride trusler.

Foranstaltning 17: 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.

[19] Tredje statusrapport om indførelsen af en effektiv og ægte sikkerhedsunion (COM(2016) 831 final).
[20] Europa-Parlamentets og Rådets direktiv (EU) 2015/849 af 20. maj 2015 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme, om ændring af Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 og om ophævelse af Europa-Parlamentets og Rådets direktiv 2005/60/EF samt Kommissionens direktiv 2006/70/EF (EUT L 141 af 5.6.2015, s. 73-117).
[21] Nærmere oplysninger kan findes i den tredje statusrapport om indførelsen af en effektiv og ægte sikkerhedsunion (COM(2016) 831 final) og den ottende statusrapport om indførelsen af en effektiv og ægte sikkerhedsunion (COM(2017) 354 final).
[22] COM(2017) 26.6.2017, COM(2017) 340 final, SWD(2017) 275 final 0.
[23] Ottende statusrapport om indførelsen af en effektiv og ægte sikkerhedsunion (COM(2017) 354 final).

Forebyggelse af radikalisering

Kommissionen fortsætter gennemførelsen af sin mangesidige respons på radikalisering, som er fastsat i meddelelsen fra juni 2016 om at støtte forebyggelsen af radikalisering, der fører til voldelig ekstremisme[24], med nøgleaktioner som f.eks. fremme af en inklusiv uddannelse og fælles værdier, bekæmpelse af ekstremistpropaganda online og radikalisering i fængsler, styrkelse af samarbejdet med tredjelande samt øget forskning for bedre at forstå den stadige udvikling af radikalisering og mere information om politiske løsninger. Netværket til bevidstgørelse omkring radikalisering (RAN) har stået i spidsen for Kommissionens arbejde med at støtte medlemsstaterne på dette område, i samarbejde med lokale aktører på lokalt plan. Nærmere oplysninger kan findes i den ottende statusrapport om indførelsen af en effektiv og ægte sikkerhedsunion[25].

Radikalisering og hadefulde udtalelser online

I overensstemmelse med den europæiske dagsorden om sikkerhed[26] har Kommissionen truffet foranstaltninger til at reducere tilgængeligheden af ulovligt indhold online, navnlig gennem EU-enheden for indberetning af internetindhold under Europol samt EU's internetforum[27]. Der er ligeledes gjort betydelige fremskridt i henhold til adfærdskodeksen til bekæmpelse af ulovlig hadefuld tale på internettet[28]. Nærmere oplysninger kan findes i den ottende statusrapport om indførelsen af en effektiv og ægte sikkerhedsunion[29]. Disse tiltag vil blive forstærket, bl.a. i lyset af Det Europæiske Råds konklusioner[30], G7-topmødet[31] og G20-topmødet i Hamburg[32].

Onlineplatforme spiller en nøglerolle i bekæmpelsen af ulovligt eller potentielt skadeligt indhold. Kommissionen vil under strategien for det digitale indre marked, som er fastsat i midtvejsevalueringen[33], sikre bedre koordinering af platformdialoger, med særlig vægt på mekanismer og tekniske løsninger til fjernelse af ulovligt indhold. Hvor det er relevant, bør formålet være at underbygge disse mekanismer med vejledning om aspekter som f.eks. anmeldelse og fjernelse af ulovligt indhold. Kommissionen vil desuden yde vejledning om ansvarsregler.

[24] https://webgate.ec.testa.eu/docfinder/extern/aHR0cDovLw==/ZXVyLWxleC5ldXJvcGEuZXU=/legal-content/DA/TXT/PDF/?uri=CELEX:52016DC0379&rid=2
[25] COM(2017) 354 final.
[26] Nærmere oplysninger kan findes i den ottende statusrapport om indførelsen af en effektiv og ægte sikkerhedsunion (COM(2017) 354 final).
[27] Nærmere oplysninger kan findes i den ottende statusrapport om indførelsen af en effektiv og ægte sikkerhedsunion (COM(2017) 354 final).
[28] Adfærdskodeks om ulovlig hadefuld tale på internettet, den 31. maj 2016, http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf
[29] Nærmere oplysninger kan findes i den ottende statusrapport om indførelsen af en effektiv og ægte sikkerhedsunion (COM(2017) 354 final).
[30] Rådets konklusioner af 22.-23. juni 2017.
[31] G7-topmødet i Taormina, Italien, 26.-27. maj 2017.
[32] G20-topmødet i Hamburg, Tyskland, 7.-8. juli 2017.
[33] Jf. ovennævnte meddelelse fra Kommissionen (COM(2017) 228 final).

Øget samarbejde med tredjelande

Foranstaltning 18: 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.

Den Europæiske Union har sat øget fokus på at opbygge kapacitet og modstandsdygtighed i partnerlande inden for sikkerhedssektoren, bl.a. ved at udnytte forbindelsen mellem sikkerhed og udvikling, styrke den sikkerhedsmæssige dimension i EU's reviderede naboskabspolitik samt indgå i dialog med landene rundt om Middelhavet vedrørende terrorbekæmpelse og sikkerhed. I denne henseende blev der i samarbejde med Republikken Moldova iværksat en risikoundersøgelse som et pilotprojekt. Formålet hermed er at identificere det pågældende lands centrale svagheder og sikre, at EU's bistand er målrettet mod netop disse områder. Resultaterne af pilotprojektet viste, at undersøgelsen i sig selv blev anset for nyttig. Kommissionen og EU-Udenrigstjenesten vil på baggrund af de indhøstede erfaringer fremsætte henstillinger for at prioritere tiltag under udgiftsområdet for opbygning af effektivitet, strategisk kommunikation, beskyttelse af kritisk infrastruktur og cybersikkerhed.

Fremadrettet vil også andre nabolande kunne drage fordel af undersøgelsen ved at bygge videre på denne første erfaring, om end med skræddersyede tilpasninger for at afspejle de forskellige nationale og lokale forhold samt specifikke trusler og for at undgå overlapning med igangværende dialoger om terrorbekæmpelse og sikkerhed. Mere generelt vedtog Kommissionen og den højtstående repræsentant den 7. juni 2017 en fælles meddelelse om "en strategisk tilgang til resiliens i forbindelse med EU's indsats udadtil"[34]. Målet hermed er at støtte partnerlandene til at blive mere modstandsdygtige over for de aktuelle globale udfordringer. I meddelelsen anerkendes behovet for at bevæge sig væk fra kriseinddæmning og i retning af en mere strukturel, langsigtet og ikke-lineær tilgang til sårbarheder, med særlig vægt på foregribelse, forebyggelse og beredskab.

Opbygning af modstandsdygtighed over for cyberangreb

EU støtter lande uden for Europa i at styrke modstandsdygtigheden i disse landes informationsnetværk. Den stadigt tiltagende digitalisering indebærer i sagens natur en sikkerhedsdimension, hvilket skaber særlige udfordringer for informationsnetværkenes modstandsdygtighed over for cyberangreb på globalt plan, idet disse angreb ikke kender nogen grænser. EU støtter tredjelande i at opbygge deres evne til på passende vis at forebygge og reagere på utilsigtede fejl og cyberangreb. Som opfølgning på et pilotprojekt om cybersikkerhed i Den Tidligere Jugoslaviske Republik Makedonien, Kosovo[35] og Moldova, som blev afsluttet i 2016, vil Kommissionen iværksætte et nyt program for at forstærke modstandsdygtigheden over for cyberangreb i tredjelande, navnlig lande i Afrika og Asien i

[34]Fælles meddelelse til Europa-Parlamentet og Rådet: En strategisk tilgang til resiliens i forbindelse med EU's indsats udadtil (JOIN(2017) 21 final).

[35] Denne betegnelse indebærer ingen stillingtagen til Kosovos status, og den er i overensstemmelse med FN's Sikkerhedsråds resolution 1244 og Den Internationale Domstols udtalelse om Kosovos uafhængighedserklæring.

perioden 2017-2020, men også i Ukraine. Formålet hermed er at øge sikkerheden og beredskab i kritiske informationsinfrastrukturer og -netværk i tredjelande ud fra en helhedsorienteret tilgang med inddragelse af hele statsapparatet ("whole-of-government approach"), samtidig med at der sikres overholdelse af menneskerettighederne og retsstatsprincippet.

Luftfartssikkerhed

Civil luftfart er fortsat et vigtigt og symbolsk mål for terrorister, men kan også rammes som led i en hybrid angrebskampagne. Selv om EU har udviklet en solid ramme for luftfartssikkerhed, kan flyvninger fra tredjelande være mere sårbare. I overensstemmelse med FN's Sikkerhedsråds resolution 2309 fra 2016 optrapper Kommissionen for øjeblikket sin indsats for at opbygge kapacitet i tredjelande. Kommissionen iværksatte i januar 2017 en ny integreret risikovurdering med henblik på at sikre prioritering og koordinering af den indsats for kapacitetsopbygning, der udføres på EU-plan, i medlemsstaterne og sammen med internationale partnere. I 2016 iværksatte Kommissionen et 4-årigt projekt om sikkerhed inden for civil luftfart i Afrika og på Den Arabiske Halvø med henblik på at imødegå terrortruslen mod civil luftfart. Projektet har fokus på udveksling af erfaringer mellem partnerlande og eksperter fra medlemslande i Den Europæiske Konference for Civil Luftfart (ECAC) og yder desuden vejledning, uddannelse og coaching. Disse aktiviteter vil blive yderligere intensiveret i løbet af 2017.

c. FOREBYGGELSE AF OG REAKTION PÅ KRISESITUATIONER SAMT TILBAGEVENDEN TIL NORMALTILSTAND

Selv om følgevirkninger 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 normaltilstand. Det er vigtigt hurtigt at kunne reagere på hændelser, der skyldes hybride trusler. Der er i de seneste år gjort store fremskridt på dette område, bl.a. har EU nu indført en fælles operationel protokol, som fastlægger proceduren for krisestyring i tilfælde af et hybridangreb. Regelmæssig overvågning og gennemførelse af øvelser vil finde sted fremover.

Foranstaltning 19: 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 proceduren for krisestyring og for integrerede ordninger for politisk kriserespons.

I den fælles ramme anbefales indførelse af mekanismer til hurtig reaktion på hændelser, der skyldes hybride trusler, med henblik på at samordne EU's beredskabsmekanismer[36] og systemer for tidlig varsling. Med henblik herpå udsendte Kommissionens tjenestegrene og EU-Udenrigstjenesten EU's fælles operationel protokol for imødegåelse af hybride trusler (EU-drejebogen)[37], der beskriver de nærmere bestemmelser for koordinering, samling og analyse af efterretninger, input til beslutningsprocesser, øvelser og uddannelse samt samarbejde med partnerorganisationer, navnlig NATO, i tilfælde af en hybrid trussel.

[36] Rådets integrerede ordninger for politisk kriserespons (IPCR), Kommissionens ARGUS-system og EU-Udenrigstjenestens kriseberedskabsmekanisme (Crisis Response Mechanism).
[37] SWD(2013) 227, vedtaget den 7. juli 2016.

Ligeledes har NATO udarbejdet en drejebog med henblik på bedre samspil mellem NATO og EU for at forebygge og imødegå hybride trusler inden for cyberforsvar, strategisk kommunikation, situationsbevidsthed og krisestyring. EU-drejebogen vil blive afprøvet under en øvelse i efteråret 2017, som en del af EU's parallelle og koordinerede øvelsesprogram, som også omfatter samspil med NATO.

Foranstaltning 20: 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 konkrete følger heraf.

Artikel 42, stk. 7, i TEU omhandler væbnede angreb på en medlemsstats område, mens artikel 222 TEUF ("solidaritetsbestemmelsen") omhandler terrorangreb, naturkatastrofer eller menneskeskabte katastrofer på en medlemsstats område. Det er mere sandsynligt, at sidstnævnte bestemmelse vil blive anvendt i tilfælde af hybridangreb, som er en blanding af kriminelle og undergravende aktiviteter. Påberåbelsen af solidaritetsbestemmelsen udløser koordinering fra Rådets side (integrerede ordninger for politisk kriserespons; IPCR) og inddragelse af EU's relevante institutioner, agenturer og organer samt EU's bistandsprogram og bistandsmekanisme. I Rådets afgørelse 2014/415/EU er der fastsat ordninger til Unionens gennemførelse af solidaritetsbestemmelsen. Disse nærmere gennemførelsesbestemmelser gælder fortsat, og der er ikke behov for at ændre Rådets afgørelse. Såfremt et hybridangreb omfatter et væbnet angreb, vil bestemmelsen om gensidigt forsvar (artikel 42, stk. 7) eventuelt også kunne påberåbes. Der skal i givet fald ydes hjælp og bistand både af medlemsstaterne og af EU. Kommissionen og den højtstående repræsentant vil fortsat vurdere de mest effektive metoder til at imødegå sådanne angreb.

Vedtagelsen af ovennævnte operationelle protokol understøtter direkte denne vurdering og vil indgå i EU's parallelle og koordinerede øvelse (PACE) i oktober 2017. Denne øvelse vil teste EU's forskellige mekanismer og evne til at interagere med det formål at fremskynde beslutningstagning, hvor usikkerhed som følge af en hybrid trussel svækker klarheden.

Foranstaltning 21: 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.

Som svar på tildelingen af opgaven med at integrere militær kapacitet til støtte for FUSP/FSFP, og som opfølgning på et seminar med militære eksperter i december 2016 og rådgivning fra EU-Militærkomitéens Arbejdsgruppe (EUMCWG) i maj 2017 blev den militære rådgivning om "EU's militære bidrag til at imødegå hybride trusler inden for FSFP" afsluttet i juli 2017. Den vil blive videreudviklet gennem programmet for gennemførelse af konceptudviklingen (CDIP).

d. SAMARBEJDET MELLEM EU OG NATO

Foranstaltning 22: Den højtstående repræsentant vil i samarbejde med Kommissionen fortsætte den uformelle dialog og øge samarbejdet og koordineringen med NATO om situationsbevidsthed, strategisk kommunikation, cybersikkerhed, kriseforebyggelse og kriseforanstaltninger for at bekæmpe hybride trusler, samtidig med at principperne om ensartet deltagelse og hver organisations selvstændige beslutningstagning respekteres.

På grundlag af den fælles erklæring, som blev underskrevet af Det Europæiske Råds formand, Europa-Kommissionens formand og NATO's generalsekretær den 8. juli 2016 i Warszawa,

har EU og NATO udviklet et fælles sæt på 42 gennemførelsesforslag, som siden er blevet godkendt i separate, sideløbende processer den 6. december 2016 af både EU og NATO's råd[38]. I juni 2017 udsendte den højtstående repræsentant/næstformanden og NATO's generalsekretær en rapport om de generelle fremskridt, der er gjort med de 42 tiltag i den fælles erklæring. Imødegåelse af hybride trusler er et af de syv samarbejdsområder, der er udpeget i den fælles erklæring, og dækker 10 af de 42 tiltag. Rapporten viser, at de seneste års fælles bestræbelser har givet betydelige resultater. Mange af de specifikke foranstaltninger med henblik på at bekæmpe hybride trusler er allerede nævnt, herunder det europæiske ekspertisecenter for imødegåelse af hybride trusler, bedre situationsbevidsthed, oprettelse af EU's analyseenhed for hybride trusler og dennes samspil med NATO's nyoprettede afdeling for analyse af hybride trusler samt samarbejde mellem holdene for strategisk kommunikation. For første gang vil personel fra NATO og EU sammen afholde øvelse for at teste deres reaktionsevne over for scenarier i forbindelse med hybride trusler. Under denne øvelse er det planlagt at afprøve gennemførelsen af over en tredjedel af de fælles forslag. Sideløbende hermed vil EU i år afholde sin egen samordnede øvelse og forbereder sig på at indtage en lederrolle i 2018.

For så vidt angår modstandskraft, har både EU's og NATO's personel deltaget i gensidige briefinger, bl.a. om IPCR. Regelmæssig kontakt mellem NATO's og EU's personel, bl.a. gennem workshopper eller NATO's deltagelse i Det Europæiske Forsvarsagenturs styringskomité, har muliggjort informationsudveksling om NATO's grundlæggende krav til national modstandsdygtighed. Yderligere informationsudveksling mellem Kommissionen og NATO om styrkelse af modstandsdygtigheden er planlagt til efteråret. Den næste statusrapport om samarbejdet mellem EU og NATO vil indeholde forslag til muligheder for at udvide samarbejdet mellem de to organisationer.

3. KONKLUSION

I den fælles ramme skitseres en række foranstaltninger, der er udformet henblik på at imødegå hybride trusler og opbygge modstandsdygtighed på EU-plan, på nationalt plan og hos partnerne. Selv om Kommissionen og den højtstående repræsentant i tæt samarbejde med medlemsstaterne og partnerne leverer resultater på alle områder, er det afgørende, at dette momentum opretholdes set i lyset af den igangværende og fortsatte udvikling af hybride trusler. Medlemsstaterne bærer hovedansvaret for at bekæmpe hybride trusler, der vedrører hvert enkelt lands sikkerhed og opretholdelse af lov og orden. National modstandsdygtighed og kollektive bestræbelser på beskyttelse mod hybride trusler skal opfattes som gensidigt forstærkende elementer af én og samme overordnede indsats. Medlemsstaterne opfordres derfor til at udføre disse undersøgelser af hybride risici så hurtigt som muligt, da de vil give værdifulde oplysninger om omfanget af sårbarhed og beredskab i hele Europa. Potentialet i EU's analyseenhed for hybride trusler bør maksimeres ved at bygge videre på de betydelige fremskridt med hensyn til at øge bevidstheden. Den højtstående repræsentant opfordrer medlemsstaterne til at støtte det arbejde, der udføres af taskforcerne for strategisk kommunikation, med henblik på at imødegå stigningen i hybride trusler mere effektivt. EU vil give sin fulde opbakning til det europæiske center til imødegåelse af hybride trusler under ledelse af Finland.

EU's særlige styrke består i at bistå medlemsstaterne og partnere i at opbygge deres modstandsdygtighed ved brug af en bred vifte af eksisterende instrumenter og programmer.

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

Der er gjort betydelige fremskridt i indsatsen for at opbygge modstandsdygtighed på områder såsom transport, energi, cybersikkerhed, kritisk infrastruktur, beskyttelse af de finansielle systemer mod misbrug og bestræbelser på at bekæmpe voldelig ekstremisme og radikalisering. EU vil fortsætte sin indsats for at opbygge modstandsdygtighed i takt med, at de hybride trusler udvikler sig. EU vil navnlig udarbejde indikatorer til at forbedre beskyttelse og modstandsdygtighed mod hybride trusler hos kritisk infrastruktur i de relevante sektorer.

Eventuelt kan Den Europæiske Forsvarsfond sammen med medlemsstaterne medfinansiere kapacitetsmæssige prioriteter med henblik på at styrke modstandsdygtigheden mod hybride trusler. Den forestående pakke for cybersikkerhed vil sammen med tværsektorielle foranstaltninger, der sigter mod gennemførelsen af direktivet om net- og informationssikkerhed, skabe nye platforme for imødegåelse af hybride trusler i hele EU.

Kommissionen og den højtstående repræsentant opfordrer medlemsstaterne og interessenterne til om nødvendigt hurtigt at nå frem til en aftale og for at sikre en hurtig og effektiv gennemførelse af de mange foranstaltninger til styrkelse af modstandsdygtighed, der er skitseret i denne meddelelse. EU vil udbygge og uddybe sit allerede givtige samarbejde med NATO.

Unionen fastholder til beslutning om at ibrugtage alle relevante EU-instrumenter til at imødegå komplekse og hybride trusler. Støtte til medlemsstaternes indsats er fortsat en prioritet for EU, som vil fungere som en stærkere og mere fleksibel garant for sikkerheden, side om side med sine nøglepartnere.