Rådet for
Den Europæiske Union

Bruxelles, den 10. december 2019
(OR. en)

14972/19

HYBRID 56	**EDUC 478**
DISINFO 18	**AUDIO 118**
AG 68	**DIGIT 179**
PE 257	**INF 332**
DATAPROTECT 300	**COSI 252**
JAI 1307	**CSDP/PSDC 575**
CYBER 328	**COPS 360**
JAIEX 177	**POLMIL 129**
FREMP 176	**IPCR 23**
RELEX 1147	**PROCIV 100**
CULT 141	**CSC 294**

RESULTAT AF DRØFTELSERNE

fra:	Generalsekretariatet for Rådet
til:	delegationerne
Vedr.:	Supplerende tiltag for at styrke modstandsdygtigheden og imødegå hybride trusler - Rådets konklusioner (den 10. december 2019)

Vedlagt følger til delegationerne Rådets konklusioner om supplerende bestræbelser for at øge modstandsdygtigheden og imødegå hybride trusler, der blev vedtaget af Rådet på 3739. samling den 10. december 2019.

BILAG

Rådets konklusioner om supplerende tiltag for at styrke modstandsdygtighed og imødegå hybride trusler

1. Rådet minder om de relevante konklusioner fra Det Europæiske Råd[1] og Rådet[2] og er fortsat fast besluttet på at styrke EU's og medlemsstaternes modstandsdygtighed over for mangesidede hybride trusler, der er i konstant udvikling, og øge samarbejdet for at opdage, forhindre og imødegå dem.

2. Rådet anerkender de fremskridt, der er gjort med gennemførelsen af den fælles ramme for imødegåelse af hybride trusler (2016) og den fælles meddelelse om øget modstandsdygtighed og forbedrede kapaciteter til håndtering af hybride trusler (2018) samt handlingsplanen for bekæmpelse af desinformation (2018) i overensstemmelse med de relevante rådskonklusioner.

3. Hovedansvaret for at imødegå hybride trusler ligger hos medlemsstaterne. Tiltagene på EU-plan er supplerende og berører ikke medlemsstaternes eneansvar for den nationale sikkerhed. Det er nødvendigt med en tilgang til sikkerhed på tværs af ministerier og myndigheder og for hele samfundet, hvis de hybride trusler skal håndteres på en mere strategisk, koordineret og sammenhængende måde på tværs af alle relevante politikområder. Det er vigtigt, at der følges en tilgang, der går på tværs af ministerier og myndigheder, som også anvendes på EU-plan.

4. I disse konklusioner fastsætter Rådet prioriteter vedrørende beskyttelse af vores samfund, borgere og frihedsrettigheder og vores Unions sikkerhed mod hybride trusler i forbindelse med gennemførelsen af den nye strategiske dagsorden for 2019-2024 ved at fremme en samlet tilgang til sikkerhed med mere samordning, flere ressourcer og større teknologisk kapacitet, der bygger på det vigtige arbejde, der allerede er udført på forskellige politikområder, herunder som led i EU's sikkerheds- og forsvarssamarbejde.

---

1 Navnlig Det Europæiske Råds konklusioner fra juni 2019, marts 2019, december 2018, oktober 2018, juni 2018, marts 2018, juni 2015 og marts 2015.

2 Navnlig ST 10048/19, ST 6573/1/19 REV1, ST 10255/19, ST 12836/19, ST 7928/16.

5. Tiltagene for at beskytte vores demokratiske institutioner mod hybride trusler skal altid overholde de grundlæggende rettigheder, herunder beskyttelse af personoplysninger, ytrings- og informationsfrihed og foreningsfrihed som fastsat i chartret om grundlæggende rettigheder.

6. EU og dets medlemsstater bør fortsætte med at udvikle, uddanne og udnytte deres kapacitet til at afsløre, analysere kilderne til og reagere på hybride aktiviteter og støtte en styrkelse af modstandsdygtigheden i medlemsstaterne og i EU's institutioner, organer og agenturer over for hybride trusler på lang sigt, idet der drages fuld fordel af velegnede eksisterende instrumenter. Rådet understreger behovet for at ajourføre den operationelle EU-protokol for at imødegå hybride trusler på grundlag af identificerede og indhøstede erfaringer fra tidligere øvelser.

7. Rådet understreger det fortsatte behov for at samarbejde med internationale organisationer såsom FN, OSCE og Europarådet samt formater såsom G7 for at værne om den regelbaserede verdensorden, også i forbindelse med imødegåelse af hybride trusler, herunder gennem tillidsskabende foranstaltninger og andre relevante foranstaltninger.

8. Rådet understreger EU's tilsagn om at fortsætte det tætte og gensidigt forstærkende samarbejde med og støtten til alle relevante partnerlande, navnlig i EU's nabolande, vedrørende styrkelse af modstandsdygtighed og imødegåelse af hybride trusler.

9. Rådet opfordrer til en løbende og vedvarende indsats for at gøre yderligere fremskridt med gennemførelsen af alle foranstaltninger vedrørende imødegåelse af hybride trusler i henhold til det fælles sæt af forslag til gennemførelse af de fælles erklæringer om samarbejde mellem EU og NATO, herunder på områderne situationsbevidsthed, strategisk kommunikation, kriseforebyggelse og -respons og øget modstandsdygtighed. I denne forbindelse gentager det behovet for yderligere at styrke den politiske dialog om imødegåelse af hybride trusler samt regelmæssige parallelle og koordinerede øvelser (PACE) med deltagelse af alle EU-medlemsstater og NATO-allierede og opfordrer til en rettidig færdiggørelse af den nye PACE-plan. Rådet understreger behovet for at tage hensyn til de indhøstede erfaringer og betydningen af uhindret udveksling af oplysninger på en inklusiv og ikkeforskelsbehandlende måde.

Desuden fremhæver Rådet de værdifulde bidrag fra Det Europæiske Center for Imødegåelse af Hybride Trusler i Helsingfors og støtter dets samarbejde med de relevante NATO-ekspertisecentre. Det glæder sig også over den regelmæssige og strukturerede udveksling af personale, herunder samarbejdet mellem enheden for analyse og udveksling i EU's Efterretnings- og Situationscenter (INTCEN) og NATO's afdeling for analyse af hybride trusler ("Hybrid Analysis Branch").

10. Rådet anerkender den indsats, som medlemsstaterne har gjort i samarbejde med Kommissionen og Tjenesten for EU's Optræden Udadtil (EU-Udenrigstjenesten) ved gennemførelsen af undersøgelsen af hybride risici, der er omhandlet i foranstaltning 1 i den fælles ramme for imødegåelse af hybride trusler (2016), og opfordrer til videre arbejde og en mulig revision af undersøgelsen af hybride risici for bedre at afhjælpe sårbarheder.

Sammenhængende arbejde med henblik på at styrke modstandsdygtighed og imødegå hybride trusler

11. Når der udvikles og anvendes nye og fremspirende teknologier, herunder kunstig intelligens og dataindsamlingsteknikker, bør der for at mindske de samlede risici tages behørigt hensyn til nye muligheder for at styrke modstandsdygtigheden såvel som de potentielle sårbarheder og kaskadevirkninger i forbindelse med imødegåelse af hybride trusler, også i den strategiske planlægningsproces under rammeprogrammet for forskning og innovation.

12. Rådet noterer sig, at ondsindede cyberaktiviteter kan indgå i de hybride trusler, og understreger i denne forbindelse relevansen af EU's cyberdiplomatiske værktøjskasse.

13. Forholdet mellem hybride trusler og økonomisk sikkerhed er et relevant element, der bør tages i betragtning, og som fortsat er medlemsstaternes hovedansvar.

14. Nye instrumenter såsom mekanismen under EU's forordning om screening af udenlandske direkte investeringer bør anvendes effektivt til at styrke modstandsdygtighed og imødegå hybride trusler ved at give mulighed for at identificere og håndtere udenlandske direkte investeringer, der vil kunne påvirke sikkerheden eller den offentlige orden.

15. Rådet opfordrer Kommissionen til at inkludere modstandsdygtighed over for hybride trusler i konsekvensanalyseprocessen for relevante fremtidige lovgivningsforslag, herunder fremtidige rammeprogrammer for forskning og innovation.

16. Rådet understreger betydningen af regelmæssige øvelser og scenariebaserede drøftelser om imødegåelse af hybride trusler på ministerplan og andre niveauer samt af at inkludere hybride elementer i andre relevante EU-uddannelses- og øvelsesaktiviteter på alle forskellige niveauer med støtte fra dets medlemsstater og de relevante organer, navnlig Det Europæiske Center for Imødegåelse af Hybride Trusler, hvor det er relevant.

17. For at sikre sammenhæng mellem de næste trin i EU-samarbejdet om styrkelse af modstandsdygtighed og imødegåelse af hybride trusler opfordrer Rådet Kommissionen og den højtstående repræsentant til, at der foretages en kortlægning, som tager hensyn til de foranstaltninger, der hidtil er truffet, og de relevante dokumenter, der er vedtaget på en samlet måde, med henblik på mulige nye initiativer.

Sammenhæng mellem intern og ekstern sikkerhed

18. Retshåndhævelses- og civilbeskyttelsesmyndigheder og andre relevante myndigheder bør fortsætte med at udvikle deres beredskab til at forebygge og imødegå hybride trusler. Samarbejdet mellem de relevante nationale myndigheder såvel som EU's institutioner, organer og agenturer på tværs af sammenhængen mellem intern og ekstern sikkerhed, der er baseret på deres respektive mandater, skal løbende forbedres og integreres, samtidig med at synergierne øges, og dobbeltarbejde undgås, herunder gennem horisontale arbejdsmetoder, frivillig udveksling af oplysninger og uddannelse og øvelser på tværs af sektorer. Med henblik herpå bør de relevante EU-mekanismers og EU-agenturers støtteroller og bidrag – inden for rammerne af deres respektive mandater og under overholdelse af eksisterende budgetmæssige begrænsninger – vurderes yderligere.

19. Anvendelsen af relevante EU-mekanismer og -instrumenter til støtte for medlemsstaternes reaktion på tværsektorielle og grænseoverskridende trusler bør videreudvikles af EU's institutioner og organer sammen med medlemsstaterne, herunder de integrerede ordninger for politisk kriserespons (IPCR), EU-civilbeskyttelsesmekanismen og Katastrofeberedskabskoordinationscentret (ERCC).

20. Rådet anerkender medlemsstaternes mulighed for at påberåbe sig solidaritetsbestemmelsen (artikel 222 i TEUF) for at håndtere en alvorlig krise, som skyldes hybrid aktivitet.

Situationsbevidsthed og efterretningsanalyse

21. EU-samarbejdet om styrkelse af modstandsdygtighed og imødegåelse af hybride trusler skal styres af en regelmæssigt ajourført trusselsvurdering og en omfattende situationsbevidsthed. Disse skal udarbejdes af EU's INTCEN og dets analyseenhed for hybride trusler med henblik på at styrke EU's og medlemsstaternes evne til at opdage, forhindre, afbryde og reagere på hybride aktiviteter, samtidig med at medlemsstaternes kompetence respekteres. Rådet finder, at arbejdet i EU's analyseenhed for hybride trusler bør styrkes yderligere under hensyntagen til et passende niveau af ressourcer, herunder faglig ekspertise.

22. Rådet minder om sine konklusioner om imødegåelse af hybride trusler af 19. april 2016, der opfordrer til mobilisering af EU-instrumenter til at forebygge og imødegå hybride trusler mod såvel Unionen og dens medlemsstater som dens partnere. Rådet understreger behovet for at videreudvikle medlemsstaternes og EU's eksisterende situationsbevidsthedsfunktioner, idet der tages højde for trusselskilderne og gøres bedre brug af efterretningsanalyserne fra EU's INTCEN og dets analyseenhed for hybride trusler, navnlig i EU's politiske beslutnings- og krisestyringsprocesser vedrørende imødegåelse af hybride trusler.

23. Rådet erkender, at FSFP-missioner og -operationer kunne yde et relevant bidrag, hvor og når det er hensigtsmæssigt, med henblik på at identificere og analysere indikatorer for mulige hybride handlinger fra tredjeparter, herunder desinformation med henblik på at miskreditere og hæmme EU's og dets medlemsstaters indsats, og anerkender værdien af at undersøge, hvordan dette bidrag kan videreudvikles.

Beskyttelse af kritisk infrastruktur

24. Beskyttelse af kritiske nationale og europæiske infrastrukturer samt funktioner og tjenester, der er kritiske for, at staten, økonomien og samfundet kan fungere korrekt, er en central prioritet, også når det gælder om at øge modstandsdygtigheden over for hybride trusler, hvilket kræver en tilgang på tværs af ministerier og myndigheder og hele samfundet. Dette arbejde skal tage hensyn til den stærke indbyrdes afhængighed mellem forskellige kritiske funktioner og tjenester, herunder finansielle tjenesteydelser, den private sektors centrale rolle, et sikkerhedsmiljø under forandring og nye risici, både fysisk og på cyberområdet.

25. Ud over EU's og de nationale retlige, reguleringsmæssige og tilsynsmæssige krav for operationel modstandsdygtighed og forretningskontinuitet bør aftaler med den private sektors ejere og operatører af infrastruktur og tjenester fremmes for at garantere kontinuitet i og adgang til kritiske tjenester, ikke kun i force majeure-situationer, ved at sikre et acceptabelt beredskabsniveau til imødegåelse af alle relevante trusler samt fleksibilitet til at håndtere, afhjælpe og komme på fode igen efter hændelser med store konsekvenser, men lav sandsynlighed for at finde sted.

26. Rådet understreger, at selv om ansvaret for beskyttelse af kritisk infrastruktur primært henhører under national kompetence, kræver den høje grad af grænseoverskridende og tværsektoriel indbyrdes afhængighed en koordineret eller om nødvendigt harmoniseret indsats på EU-plan, herunder med henblik på det indre markeds uafbrudte funktion.

27. Efter evalueringen i juli 2019 af gennemførelsen af direktiv 2008/114/EF om indkredsning og udpegning af europæisk kritisk infrastruktur opfordrer Rådet Kommissionen til at rådføre sig med medlemsstaterne om et eventuelt forslag til en revision af direktivet tidligt i den nye lovgivningscyklus, herunder eventuelle yderligere foranstaltninger til styrkelse af den kritiske infrastrukturs beskyttelse og modstandsdygtighed i EU, idet der tages hensyn til den stærke indbyrdes afhængighed mellem kritiske funktioner og tjenester.

28. Rådet opfordrer Kommissionen til fortsat at samarbejde med medlemsstaterne og, hvor det er relevant, udvikle ikkebindende samarbejdsordninger mellem medlemsstater, der deler indbyrdes forbundne kritiske infrastrukturer.

29. Rådet anerkender betydningen af direktivet om sikkerhed for net- og informationssystemer (NIS-direktivet) for udviklingen af en risikostyrings- og sikkerhedskultur for operatørerne i kritiske sektorer samt for nationale kapaciteter og strategier, der sikrer et højt sikkerhedsniveau for net- og informationssystemer på deres område, herunder i forbindelse med hybride trusler. Rådet opfordrer medlemsstaterne, Kommissionen og Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) til at fortsætte udviklingen af deres samarbejde på grundlag af Kommissionens henstilling om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser ("planen") på alle relevante niveauer.

Bekæmpelse af desinformation og sikring af frie og retfærdige valg

30. Rådet ser med tilfredshed på rapporten om gennemførelsen af handlingsplanen for bekæmpelse af desinformation og anerkender, at handlingsplanens fortsatte gennemførelse fortsat står i centrum for EU's indsats. Rådet understreger behovet for regelmæssigt at revidere og om nødvendigt ajourføre handlingsplanen for at sikre en effektiv og langsigtet tilgang.

31. Rådet understreger, at arbejdet i EU-Udenrigstjenestens strategiske kommunikationsafdeling og navnlig de tre taskforcer (Øst, Vestbalkan, Syd) skal støttes med tilstrækkelige ressourcer til langsigtet planlægning, gennemførelse og evaluering. Blandt deres opgaver bør alle tre taskforcer være i stand til løbende at opdage, analysere og udfordre desinformationsaktiviteter fra udenlandske statslige aktører og eksterne statslige aktører. Taskforcerne bør også fortsat bidrage til en effektiv og faktabaseret positiv kommunikation og fremme af Unionens principper, værdier og politikker i EU's østlige og sydlige nabolande og på Vestbalkan og en styrkelse af det generelle mediemiljø og civilsamfundet i de tilsvarende regioner. Rådet opfordrer EU-Udenrigstjenesten til at vurdere behovene og mulighederne for at styrke det strategiske kommunikationsarbejde i andre geografiske områder såsom Afrika syd for Sahara og samtidig opretholde den nødvendige kapacitet til at udføre de eksisterende strategiske kommunikationsopgaver.

32. Rådet erkender, at der er behov for en samlet tilgang på alle niveauer for med bedst mulig brug af alle tilgængelige værktøjer online og offline at tackle de udfordringer, der er forbundet med desinformation, herunder indblanding, der forsøger at underminere frie og retfærdige valg til Europa-Parlamentet. Dette skal omfatte overvågning og analyse af desinformation og manipulerende indblanding, håndhævelse af europæiske databeskyttelsesregler, anvendelse af valgbeskyttelsesforanstaltninger, bestræbelser på at styrke pluralistiske medier, professionel journalistik og mediekendskab samt bevidsthed blandt borgerne. Rådet anbefaler yderligere konsolidering af et aktivt uafhængigt tværeuropæisk netværk af faktatjekkere og forskere mod desinformation. Rådet anerkender civilsamfundets, den akademiske verdens og den private sektors betydning og rolle med hensyn til at tackle desinformation og opbygge modstandsdygtighed.

33. Rådet anerkender det potentiale, der ligger i det hurtige varslingssystem for så vidt angår bekæmpelse af desinformation, navnlig med hensyn til indblanding i valg. Det opfordrer Kommissionen og EU-Udenrigstjenesten til sammen med medlemsstaterne at videreudvikle det hurtige varslingssystem hen imod en omfattende platform for medlemsstater og EU-institutioner til at styrke samarbejde, koordinering og informationsudveksling, såsom forskning og analytisk indsigt, bedste praksis og kommunikationsprodukter til støtte for tackling af desinformationskampagner som led i en række europæiske og nationale bestræbelser.

34. Rådet anerkender nytten af de foranstaltninger og henstillinger, som Kommissionen forelagde den 12. september 2018 i sin valgpakke til sikring af valget til Europa-Parlamentet. Rådet opfordrer Kommissionen og medlemsstaterne til at undersøge mulighederne for at fortsætte aktiviteterne i de europæiske valgsamarbejdsnetværk for at støtte udvekslingen af oplysninger og bedste praksis. Rådet ser med tilfredshed på Kommissionens bestræbelser på at inddrage alle relevante interessenter og støtte en bred vifte af foranstaltninger, såsom øvelsen vedrørende cybersikkerhed ved valget til Europa-Parlamentet (EU ELEx19), under hensyntagen til de nationale kompetencer på dette område.

35. Rådet anerkender, at det er nødvendigt at fortsætte arbejdet med sociale medieplatforme for at opnå højere standarder for ansvar, gennemsigtighed og ansvarlighed i forbindelse med bekæmpelse af desinformation. Desuden bør der gives uhindret adgang til anonymiserede data fra udbydere af sociale medieplatforme til akademisk forskning for at lette evidensbaserede politikker. Rådet opfordrer Kommissionen til at forelægge initiativer om vejen frem i bekæmpelsen af desinformation på onlineplatforme. Disse initiativer bør baseres på en vurdering af gennemførelsen af adfærdskodeksen om desinformation, som bør tage hensyn til det analytiske arbejde i og rapporterne fra den akademiske verden og civilsamfundsorganisationer, overvågningsrapporten om kodeksen fra Gruppen af Europæiske Tilsynsmyndigheder for Audiovisuelle Medietjenester og ligeledes erfaringerne fra valget til Europa-Parlamentet i maj 2019. I denne forbindelse opfordrer Rådet Kommissionen til at overveje måder, herunder eventuelle håndhævelsesmekanismer for onlineplatforme, til yderligere at styrke gennemførelsen af adfærdskodeksen, navnlig ved at medtage en uafhængig vurdering af underskrivernes overholdelse af deres forpligtelser.

Sikkerhed for EU's institutioner, organer og agenturer

36. Sikkerheden for EU's personale, institutioner, organer og agenturer mod hybride trusler og andre ondsindede aktiviteter er en fælles interesse for EU og dets medlemsstater. Rådet opfordrer EU's institutioner, organer og agenturer til med støtte fra medlemsstaterne at sikre Unionens evne til at beskytte sin integritet og øge sikkerheden i EU's informations- og kommunikationsnetværk og beslutningsprocesser mod ondsindede aktiviteter af enhver art på grundlag af en omfattende trusselsvurdering. Med henblik herpå bør institutioner, organer og agenturer med støtte fra medlemsstaterne udvikle og gennemføre et omfattende sæt foranstaltninger for at sikre deres sikkerhed i overensstemmelse med mandatet fra Det Europæiske Råd i juni 2019. Rådet understreger betydningen af at sikre interoperabilitet mellem EU's IT-infrastruktur for udveksling af klassificerede informationer mellem EU's institutioner, organer, agenturer og medlemsstater.