Europeiska unionens råd

Bryssel 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

LÄGESRAPPORT

från:	Rådets generalsekretariat
till:	Delegationerna
Ärende:	Kompletterande insatser för förstärkning av motståndskraft och motverkande av hybridhot – Rådets slutsatser (10 december 2019)

För delegationerna bifogas rådets slutsatser om kompletterande insatser för förstärkning av motståndskraft och motverkande av hybridhot, som antogs vid rådets 3739:e möte den 10 december 2019.

BILAGA

Rådets slutsatser om kompletterande insatser för förstärkning av motståndskraft och motverkande av hybridhot

1. Rådet erinrar om de relevanta slutsatserna från Europeiska rådet[1] och rådet[2] och uttrycker sitt fortsatta engagemang för att stärka unionens och dess medlemsstaters motståndskraft mot de mångfasetterade och ständigt föränderliga hybridhoten och för att öka samarbetet i syfte att upptäcka, förebygga och motverka hybridhot.

2. Rådet är medvetet om de framsteg som gjorts i genomförandet av den gemensamma ramen för att motverka hybridhot (2016) och det gemensamma meddelandet om ökad motståndskraft och stärkt förmåga att motverka hybridhot (2018) samt åtgärdsplanen mot desinformation (2018), i linje med relevanta rådsslutsatser.

3. Det främsta ansvaret för att motverka hybridhot vilar på medlemsstaterna. Insatserna på EU-nivå är kompletterande till sin natur och påverkar inte det faktum att det är medlemsstaterna som ensamma är ansvariga i frågor som rör den nationella säkerheten. För att man ska kunna motverka hybridhot behövs det en övergripande säkerhetsstrategi som inbegriper hela statsförvaltningen och hela samhället, samt ett mer strategiskt, samordnat och enhetligt arbete inom alla relevanta politikområden. Det är viktigt att en strategi som inbegriper hela statsförvaltningen även tillämpas på EU-nivå.

4. I dessa slutsatser fastställer rådet prioriteringar för skyddet av våra samhällen, medborgare och friheter samt av unionens säkerhet mot hybridhot i samband med genomförandet av den nya strategiska agendan 2019–2024, genom att främja en övergripande säkerhetsstrategi med bättre samordning, resurser och teknisk kapacitet, med utgångspunkt i det viktiga arbete som redan gjorts inom olika politikområden, bland annat inom ramen för EU:s säkerhets- och försvarssamarbete.

---

1 Särskilt Europeiska rådets slutsatser från juni 2019, mars 2019, december 2018, oktober 2018, juni 2018, mars 2018, juni 2015 och mars 2015.

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

5. Insatserna för att skydda våra demokratiska institutioner mot hybridhot måste alltid respektera de grundläggande rättigheterna, bland annat skyddet av personuppgifter, yttrandefriheten och informationsfriheten samt föreningsfriheten, i enlighet med EU-stadgan om de grundläggande rättigheterna.

6. EU och dess medlemsstater bör fortsätta att utveckla, tillhandahålla utbildning i samt öva förmågan att upptäcka, analysera källorna till och bemöta hybridverksamhet, samt stödja en ökad motståndskraft hos medlemsstaterna och EU:s institutioner, organ och byråer mot hybridhot på lång sikt, med fullt utnyttjande av befintliga instrument som är lämpade för detta ändamål. Rådet betonar behovet av att uppdatera EU:s operativa protokoll för att motverka hybridhot, på grundval av identifierade och tillvaratagna erfarenheter från tidigare arbete.

7. Rådet betonar det fortsatta behovet av att samarbeta med internationella organisationer såsom FN, OSSE och Europarådet och med format såsom G7 i syfte att skydda den regelbaserade världsordningen, även när det gäller motverkande av hybridhot, bland annat genom förtroendeskapande åtgärder och andra relevanta åtgärder.

8. Rådet betonar att EU är fast beslutet att fortsätta det nära och ömsesidigt förstärkande samarbetet med alla relevanta partnerländer liksom även stödet till dessa länder, särskilt i EU:s grannskap, när det gäller förstärkning av motståndskraft och motverkande av hybridhot.

9. Rådet efterlyser kontinuerliga och ihållande insatser i syfte att göra ytterligare framsteg i genomförandet av alla åtgärder för motverkande av hybridhot inom ramen för den gemensamma uppsättningen förslag för genomförande av de gemensamma förklaringarna om samarbetet mellan EU och Nato, bland annat på områdena för situationsmedvetenhet, strategisk kommunikation, krisförebyggande och krisåtgärder och ökad motståndskraft. Rådet upprepar i detta sammanhang behovet av att ytterligare intensifiera den politiska dialogen om motverkande av hybridhot samt av regelbundna parallella och samordnade övningar, med deltagande av alla EU-medlemsstater och Nato-allierade, och efterlyser att den nya planen för parallella och samordnade övningar slutförs i tid. Rådet betonar behovet av att beakta identifierade erfarenheter och vikten av ett obehindrat utbyte av information som bör ske på ett inkluderande och icke-diskriminerande sätt.

Vidare framhåller rådet de viktiga bidragen från Europeiska kompetenscentrumet för motverkande av hybridhot i Helsingfors och uppmuntrar dess samarbete med Natos relevanta kompetenscentrum. Rådet välkomnar också de regelbundna och strukturerade utbytena på tjänstemannanivå, däribland samarbetet mellan den gemensamma enheten för hybridhot vid EU:s underrättelse- och lägescentral (EU Intcen) och Natos sektion för hybridanalys.

10. Rådet erkänner de insatser som medlemsstaterna, i samarbete med kommissionen och Europeiska utrikestjänsten, gjort vid genomförandet av den undersökning av risker i samband med hybridhot som föreskrivs i åtgärd 1 i den gemensamma ramen för att motverka hybridhot (2016) och uppmanar till fortsatt arbete och en eventuell översyn av undersökningen av risker i samband med hybridhot för att bättre åtgärda sårbarheter.

Samstämmigt arbete för att förstärka motståndskraften och motverka hybridhot

11. Vid utveckling och användning av ny och framväxande teknik, inbegripet teknik för artificiell intelligens och datainsamling, bör man ta vederbörlig hänsyn till nya möjligheter att öka motståndskraften samt till potentiella sårbarheter och kaskadeffekter i samband med motverkande av hybridhot, i syfte att minska de totala riskerna, även i processen för den strategiska planeringen av ramprogrammet för forskning och innovation.

12. Rådet noterar att skadlig it-verksamhet kan vara en del av hybridhot och understryker i detta sammanhang betydelsen av EU:s verktygslåda för cyberdiplomati.

13. Förhållandet mellan hybridhot och ekonomisk säkerhet är en relevant faktor som bör beaktas och som fortfarande i första hand är medlemsstaternas ansvar.

14. Nya instrument såsom mekanismen enligt EU:s förordning om granskning av utländska direktinvesteringar bör användas effektivt för att öka motståndskraften och motverka hybridhot genom att tillhandahålla metoder för att identifiera och ta itu med utländska direktinvesteringar som sannolikt kommer att inverka på säkerheten eller den allmänna ordningen.

15. Rådet uppmanar kommissionen att inkludera motståndskraft mot hybridhot i konsekvensbedömningsförfarandet för relevanta framtida lagstiftningsförslag, inbegripet framtida ramprogram för forskning och innovation.

16. Rådet understryker vikten av regelbundna övningar och scenariobaserade diskussioner om motverkande av hybridhot på ministernivå och andra nivåer samt av att låta hybridinslag ingå i relevanta delar av EU:s utbildnings- och övningsverksamhet på alla olika nivåer, med stöd av medlemsstaterna och berörda organ, särskilt Europeiska kompetenscentrumet för motverkande av hybridhot, när så är lämpligt.

17. För att säkerställa samstämmigheten i de kommande åtgärderna i EU-samarbetet när det gäller att öka motståndskraften och motverka hybridhot uppmanar rådet kommissionen och den höga representanten att ta fram en kartläggning som beaktar de åtgärder som hittills har vidtagits och de relevanta dokument som antagits på ett övergripande sätt, med tanke på eventuella nya initiativ.

Kopplingen mellan inre och yttre säkerhet

18. Brottsbekämpande myndigheter, myndigheter för civilskydd och andra relevanta myndigheter bör fortsätta att utveckla sin beredskap att förebygga och motverka hybridhot. Samarbetet mellan relevanta nationella myndigheter och EU:s institutioner, organ och byråer för hela kopplingen mellan inre och yttre säkerhet, baserat på deras respektive mandat, måste kontinuerligt förbättras och harmoniseras, samtidigt som man ökar synergieffekterna och undviker dubbelarbete, bland annat genom övergripande arbetsmetoder, frivilligt informationsutbyte och sektorsövergripande utbildning och övningar. I detta syfte bör relevanta EU-mekanismers och EU-organs stödjande funktioner och bidrag – inom ramen för deras respektive mandat och med respekt för befintliga budgetbegränsningar – utvärderas ytterligare.

19. Användningen av relevanta EU-mekanismer och EU-instrument för att stödja medlemsstaternas hantering av sektorsövergripande och gränsöverskridande hot bör vidareutvecklas av EU:s institutioner och organ tillsammans med medlemsstaterna, inbegripet arrangemangen för integrerad politisk krishantering (IPCR), unionens civilskyddsmekanism och Centrumet för samordning av katastrofberedskap (ERCC).

20. Rådet erkänner att det finns en möjlighet för medlemsstaterna att åberopa solidaritetsklausulen (artikel 222 i EUF-fördraget) när en allvarlig kris till följd av hybridverksamhet ska hanteras.

Situationsmedvetenhet och underrättelseanalys

21. EU:s samarbete för att öka motståndskraften och motverka hybridhot måste styras av en regelbundet uppdaterad hotbedömning och en övergripande situationsmedvetenhet. Dessa bör utvecklas av EU Intcen och dess gemensamma enhet för hybridhot för att stärka EU:s och dess medlemsstaters förmåga att upptäcka, förhindra, störa och reagera på hybridverksamhet, samtidigt som medlemsstaternas behörighet respekteras. Rådet anser att arbetet inom EU:s gemensamma enhet för hybridhot bör stärkas ytterligare, med beaktande av en lämplig resursnivå, inbegripet professionell expertis.

22. Rådet erinrar om sina slutsatser av den 19 april 2016 om motverkande av hybridhot där man efterlyser en mobilisering av EU-instrument för att förebygga och motverka hybridhot mot unionen och dess medlemsstater samt partner. Rådet understryker behovet av att vidareutveckla medlemsstaternas och EU:s befintliga funktioner för situationsmedvetenhet, med beaktande av hotkällorna, och av att bättre utnyttja underrättelseanalyser från EU Intcen och dess gemensamma enhet för hybridhot, särskilt i EU:s besluts- och krishanteringsprocesser för motverkande av hybridhot.

23. Rådet erkänner att GSFP-uppdrag och GSFP-insatser, när så är lämpligt och på lämpligt sätt, skulle kunna ge relevant stöd när det gäller att fastställa och analysera indikatorer på möjlig hybridverksamhet från tredje part, inbegripet desinformation som syftar till att misskreditera och hindra EU:s och dess medlemsstaters åtgärder, och inser värdet av att ytterligare undersöka möjligheten att utveckla detta stöd.

Skydd av kritisk infrastruktur

24. Att skydda såväl nationell och europeisk kritisk infrastruktur som funktioner och tjänster av avgörande betydelse för att staten, ekonomin och samhället ska fungera väl är en huvudprioritering, även när det gäller att öka motståndskraften mot hybridhot, vilket kräver ett deltagande av hela statsförvaltningen och hela samhället. I detta arbete måste hänsyn tas till de starka ömsesidiga beroenden som finns mellan olika kritiska funktioner och tjänster, också finansiella sådana, den privata sektorns nyckelroll, den föränderliga säkerhetsmiljön och framväxande risker, både i det fysiska rummet och på it-området.

25. Utöver de rättsliga, regleringsmässiga och tillsynsmässiga krav på EU-nivå och nationell nivå som styr den operativa motståndskraften och driftskontinuiteten, bör överenskommelser med privata ägare och verksamhetsutövare på infrastruktur- och tjänsteområdet främjas för att garantera kontinuitet inom och tillgång till kritiska tjänster även vid force majeure, genom att säkerställa en godtagbar nivå av beredskap för hantering av alla relevanta hot samt flexibilitet för att ta itu med och mildra händelser med stora konsekvenser och låg sannolikhet och för återhämtning efter sådana händelser.

26. Rådet betonar, bland annat med tanke på den inre marknadens oavbrutna funktion, att den höga graden av gränsöverskridande och tvärsektoriella ömsesidiga beroenden kräver att det finns samordnade eller, vid behov, harmoniserade insatser på EU-nivå, även om ansvaret för skyddet av kritisk infrastruktur främst omfattas av nationell behörighet.

27. Efter utvärderingen i juli 2019 av genomförandet av direktivet (2008/114/EG) om identifiering av, och klassificering som, europeisk kritisk infrastruktur uppmanar rådet kommissionen att samråda med medlemsstaterna om ett eventuellt förslag till översyn av direktivet i ett tidigt skede av den nya lagstiftningscykeln, inbegripet eventuella ytterligare åtgärder för att stärka skyddet av och motståndskraften hos kritisk infrastruktur i EU, med beaktande av det starka ömsesidiga beroendet mellan kritiska funktioner och tjänster.

28. Rådet uppmanar kommissionen att fortsätta att samarbeta med medlemsstaterna och, när så är lämpligt, utarbeta icke-bindande samarbetsavtal mellan medlemsstater som delar sammanlänkad kritisk infrastruktur.

29. Rådet konstaterar att direktivet om nät- och informationssäkerhet (NIS-direktivet) är viktigt för utvecklingen av en riskhanterings- och säkerhetskultur bland verksamhetsutövare inom kritiska sektorer och för nationella kapaciteter och strategier som säkerställer en hög säkerhetsnivå i nätverks- och informationssystem på det egna territoriet, även i samband med hybridhot. Rådet uppmanar medlemsstaterna, kommissionen och Europeiska unionens cybersäkerhetsbyrå (Enisa) att fortsätta att utveckla sitt samarbete på grundval av kommissionens rekommendation om samordnade insatser vid storskaliga cyberincidenter och cyberkriser på alla relevanta nivåer.

Motverkande av desinformation och säkerställande av fria och rättvisa val

30. Rådet välkomnar rapporten om genomförandet av åtgärdsplanen mot desinformation och konstaterar att åtgärdsplanens fortsatta genomförande står i centrum för EU:s insatser. Rådet understryker behovet av att regelbundet se över och vid behov uppdatera åtgärdsplanen för att säkerställa en effektiv långsiktig strategi.

31. Rådet understryker att arbetet i utrikestjänstens avdelning för strategisk kommunikation och i synnerhet de tre arbetsgrupperna (Öst, Västra Balkan och Syd) behöver stödjas med tillräckliga resurser för att möjliggöra långsiktig planering, genomförande och utvärdering. Till arbetsgruppernas uppgifter hör att de alla tre bör kunna kontinuerligt upptäcka, analysera och utmana desinformationsverksamhet från utländska statliga aktörer och externa icke-statliga aktörer. Arbetsgrupperna bör också fortsätta att bidra till effektiv och faktabaserad positiv kommunikation och främjandet av unionens principer, värden och politik i EU:s östra och södra grannskap och på västra Balkan, och stärka den sammantagna mediemiljön och det civila samhället i motsvarande regioner. Rådet uppmanar Europeiska utrikestjänsten att bedöma behoven av och möjligheterna till att förstärka det strategiska kommunikationsarbetet i andra geografiska områden, såsom Afrika söder om Sahara, samtidigt som man behåller den kapacitet som krävs för att utföra befintliga strategiska kommunikationsuppgifter.

32. Rådet inser att det behövs en övergripande strategi på alla nivåer för att ta itu med utmaningarna med desinformation, inklusive sådan inblandning som syftar till att undergräva fria och rättvisa val till Europaparlamentet, och på bästa sätt utnyttja alla tillgängliga verktyg online och offline. Detta måste inbegripa övervakning och analys av desinformation och manipulativ inblandning, efterlevnad av EU:s dataskyddsregler, tillämpning av valrelaterade skyddsåtgärder, insatser för att förstärka pluralistiska medier, professionell journalistik och mediekompetens, liksom medvetenhet bland medborgarna. Rådet rekommenderar ytterligare konsolidering av ett aktivt, oberoende, europeiskt nätverk av faktagranskare och forskare mot desinformation. Rådet erkänner betydelsen av och den roll som spelas av det civila samhället, den akademiska världen och den privata sektorn när det gäller att motverka desinformation och bygga upp motståndskraft.

33. Rådet erkänner potentialen i systemet för tidig varning när det gäller kampen mot desinformation, särskilt när det gäller inblandning i val. Rådet uppmanar kommissionen, utrikestjänsten och medlemsstaterna att vidareutveckla systemet för tidig varning till en heltäckande plattform som medlemsstaterna och EU:s institutioner kan använda för förstärkt samarbete, samordning och utbyte av information, såsom forsknings- och analysresultat, bästa praxis och kommunikationsprodukter, för att stödja arbetet mot desinformationskampanjer som en del av en uppsättning insatser på nationell nivå och EU-nivå.

34. Rådet erkänner nyttan av de åtgärder och rekommendationer som kommissionen lade fram den 12 september 2018 i sitt valpaket för att säkerställa fria och rättvisa val till Europaparlamentet. Rådet uppmanar kommissionen och medlemsstaterna att undersöka möjligheterna att fortsätta verksamheten i europeiska samarbetsnätverk för val för att stödja utbytet av information och bästa praxis. Rådet välkomnar kommissionens insatser för att engagera alla berörda aktörer och stödja ett brett spektrum av åtgärder, såsom övningen för it-säkerhet i samband med valet till Europaparlamentet (EU ELEx19), med beaktande av de nationella befogenheterna på detta område.

35. Rådet erkänner behovet av att fortsätta att arbeta med plattformar för sociala medier för att uppnå högre standarder för ansvar, öppenhet och ansvarsskyldighet när det gäller att hantera desinformation. Dessutom bör obehindrad tillgång till anonymiserade data från leverantörer av plattformar för sociala medier för akademisk forskning beviljas för att underlätta evidensbaserad politik. Rådet uppmanar kommissionen att lägga fram initiativ om hur man ska gå vidare med att hantera desinformation på onlineplattformar. Dessa initiativ bör grundas på en bedömning av genomförandet av uppförandekoden om desinformation, som bör beakta det analytiska arbete och de rapporter som utförs av den akademiska världen och det civila samhällets organisationer, övervakningsrapporten om koden från den europeiska gruppen av regleringsmyndigheter för audiovisuella medietjänster samt de tillvaratagna erfarenheterna från valen till Europaparlamentet i maj 2019. I detta sammanhang uppmanar rådet kommissionen att överväga olika sätt, inbegripet eventuella efterlevnadsmekanismer för onlineplattformar, att ytterligare förbättra genomförandet av uppförandekoden, framför allt genom att inbegripa en oberoende bedömning av undertecknarnas efterlevnad av deras åtaganden.

Säkerheten vid EU:s institutioner, organ och byråer

36. Säkerheten för EU:s personal, institutioner, organ och byråer mot hybridhot och annan skadlig verksamhet ligger i EU:s såväl som i medlemsstaternas intresse. Rådet uppmanar EU:s institutioner, organ och byråer att med stöd av medlemsstaterna säkerställa unionens förmåga att skydda den egna integriteten och öka säkerheten i EU:s informations- och kommunikationsnätverk och beslutsprocesser mot skadlig verksamhet av alla slag, på grundval av en övergripande bedömning av hotbilden. I detta syfte bör institutioner, organ och byråer, med stöd av medlemsstaterna, utarbeta och genomföra en omfattande uppsättning åtgärder för att garantera sin säkerhet, i enlighet med Europeiska rådets mandat från juni 2019. Rådet understryker betydelsen av att säkerställa interoperabilitet inom EU:s it-infrastruktur för utbyte av säkerhetsskyddsklassificerade uppgifter mellan EU:s institutioner, organ, byråer och medlemsstater.