Rådet for
Den Europæiske Union

Bruxelles, den 20. oktober 2021
(OR. en)

13048/21

CYBER 263
JAI 1117
TELECOM 384
CSC 362
CIS 116
RELEX 874
ENFOPOL 370
COPS 373
COSI 190
HYBRID 62
CSCI 133
POLGEN 177
DATAPROTECT 244

RESULTAT AF DRØFTELSERNE

fra:	Generalsekretariatet for Rådet
dato:	19. oktober 2021
til:	delegationerne
Tidl. dok. nr.:	12534/21
Vedr.:	Rådets konklusioner om en undersøgelse af potentialet i initiativet om den fælles cyberenhed – supplement til en koordineret EU-reaktion på væsentlige cybersikkerhedshændelser og -kriser – Rådets konklusioner (den 19. Oktober 2021)

Vedlagt følger til delegationerne Rådets konklusioner om en undersøgelse af potentialet i initiativet om den fælles cyberenhed – supplement til en koordineret EU-reaktion på væsentlige cybersikkerhedshændelser og -kriser, som vedtaget af Rådet på samlingen den 19. oktober 2021.

BILAG

Rådets konklusioner om en undersøgelse af potentialet i initiativet om den fælles cyberenhed – supplement til en koordineret EU-reaktion på væsentlige cybersikkerhedshændelser og -kriser

RÅDET FOR DEN EUROPÆISKE UNION,

SOM MINDER OM sine konklusioner om:

– EU's strategi for cybersikkerhed for det digitale årti[1],

– en koordineret EU-reaktion på væsentlige cybersikkerhedshændelser og -kriser[2],

– cyberdiplomati[3],

– en ramme for EU's fælles diplomatiske reaktion på ondsindede cyberaktiviteter ("cyberdiplomatisk værktøjskasse")[4],

– sikkerhed og forsvar[5],

– rammen for EU's cyberforsvarspolitik[6],

– Europas digitale fremtid i støbeskeen[7],

– Rådets gennemførelsesafgørelse (EU) 2018/1993 af 11. december 2018 om EU's integrerede ordninger for politisk kriserespons

1 Dok. 7290/21.
2 Dok. 10086/18.
3 Dok. 6122/15 + COR 1.
4 Dok. 10474/17.
5 Dok. 8396/21.
6 Dok. 15585/14.
7 Dok. 8711/20.

– fælles meddelelse til Europa-Parlamentet og Rådet: Modstandsdygtighed, afskrækkelse og forsvar: opbygning af en stærk cybersikkerhed for EU[8],

– opbygning af cybersikkerhedskapacitet i EU[9],

1. LÆGGER VÆGT PÅ betydningen af cybersikkerhed for opbygningen af et modstandsdygtigt, grønt og digitalt Europa, UNDERSTREGER, at cybersikkerhed er en forudsætning for EU's og dets medlemsstaters velstand og sikkerhed, dets befolkninger, virksomheder og institutioner samt for opretholdelse af vores frie og demokratiske samfunds integritet,

2. ANERKENDER mange cybersikkerhedstruslers grænseoverskridende og tværsektorielle karakter samt risiciene og de eventuelle konsekvenser af uophørlige ondsindede cyberaktivitetskampagner, der er mere virkningsfulde, sofistikerede, målrettede, komplekse, vedvarende og/eller omsiggribende[10]. Covid-19-pandemien har yderligere blotlagt vores samfunds sårbarheder og de mulige skader, som omfattende cyberhændelser kan forårsage på økonomien, demokratiet, væsentlige tjenester og kritisk infrastruktur, navnlig i sundhedssektoren. Den har også øget betydningen af konnektivitet og samfundets afhængighed af pålidelige, troværdige og sikre net- og informationssystemer. Endelig har den understreget behovet for et globalt, åbent, gratis, stabilt og sikkert internet og for tillid til informations-og kommunikationsteknologiske (IKT) produkter, processer og tjenester og sikkerheden i forbindelse hermed, herunder behovet for at sikre modstandsdygtighed i forsyningskæden,

---

8 Dok. 14435/17 + COR 1.
9 Dok. 7737/19.
10 ENISA's rapport om trusselsbilledet 2020.

3. GENTAGER vigtigheden af cyberrobusthed og videreudvikling af EU's ramme for håndtering af cybersikkerhedskriser[11] med henblik på en effektiv og rettidig reaktion på væsentlige cyberhændelser og -kriser på EU-plan og yderligere integration heraf i de eksisterende horisontale og sektorielle EU-krisereaktionsmekanismer, UNDERSTREGER den rolle, som Rådet og de integrerede ordninger for politisk kriserespons (IPCR) spiller med hensyn til at sikre rettidig koordination og respons på Unionens politiske niveau i forbindelse med kriser, som opstår i eller uden for Unionen, og som har vidtrækkende konsekvenser eller politisk betydning, FREMHÆVER betydningen af, at sådanne rammer og mekanismer afprøves under regelmæssige øvelser,

4. MINDER OM, at aktiviteter på EU-plan med hensyn til væsentlige cyberhændelser og -kriser finder sted i overensstemmelse med principperne om nærhed, proportionalitet, komplementaritet, ikkeoverlapning og fortrolighed, GENTAGER, at medlemsstaterne har det primære ansvar for at reagere i tilfælde af væsentlige cybersikkerhedshændelser og -kriser, der påvirker dem, MINDER OM vigtigheden af at respektere medlemsstaternes kompetence og deres eneansvar for den nationale sikkerhed i overensstemmelse med artikel 4, stk.2, i traktaten om Den Europæiske Union, herunder på cybersikkerhedsområdet

5. MINDER samtidig OM vigtigheden af at respektere EU-institutionernes, -organernes og -agenturernes kompetencer og mandater. Den højtstående repræsentant, Kommissionen og andre EU-institutioner, -organer og -agenturer har også en vigtig rolle at spille i henhold til EU-retten, herunder på grund af væsentlige cybersikkerhedshændelsers og -krisers mulige betydning for det indre marked samt for EU-institutionernes, -organernes og -agenturernes funktion i sig selv,

[11] Dok. 10086/18.

6. UNDERSTREGER behovet for at undgå unødvendig overlapning og for at stræbe efter komplementaritet og merværdi i den videre udvikling af EU's ramme for håndtering af cybersikkerhedskriser og sikre tilpasning til eksisterende mekanismer, initiativer, net, processer og procedurer på nationalt og europæisk plan, BETONER betydningen af at strømline eksisterende processer og strukturer for at mindske kompleksiteten og af hensyn til samhørigheden i Unionen for at forbedre tilgængeligheden og reaktionsevnen i forhold til dem, der søger bistand og solidaritet,

7. ANERKENDER anvendeligheden af folkeretten, herunder FN-pagten i sin helhed, den humanitære folkeret og menneskerettighedslovgivningen i cyberspace, og FREMMER tilslutningen til frivillige, ikkebindende normer, regler og principper for ansvarlig statslig adfærd i cyberspace, som alle FN's medlemsstater bakker op om,

8. SER MED TILFREDSHED PÅ de fremskridt, der er gjort i de seneste år i Rådet, navnlig i Den Horisontale Gruppe vedrørende Cyberspørgsmål (Cybergruppen) og andre relevante arbejdsgrupper i Rådet, samt med hensyn til oprettelsen af andre samarbejds- og informationsdelingsinitiativer, -netværker og -mekanismer blandt medlemsstaterne, navnlig NIS-samarbejdsgruppen og netværket af CSIRT'er oprettet ved Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016, Det Europæiske Netværk af Forbindelsesorganisationer for Cyberkriser (CyCLONe) samt relevante cyberforsvarsrelaterede projekter, der er iværksat inden for rammerne af det permanente strukturerede samarbejde (PESCO)[12], den fælles taskforce for cyberkriminalitet (J-CAT), Det Europæiske Retlige Netværk for Cyberkriminalitet (EJCN), medlemsstaternes frivillige bidrag til EU INTCEN samt koordination og samarbejde i forbindelse med den cyberdiplomatiske værktøjskasse,

---

[12] Navnlig holdene med henblik på cyberberedskab og gensidig bistand, der koordineres af Litauen, koordineringscentret på cyber- og informationsområdet, der koordineres af Tyskland og platformen til informationsudveksling om reaktion på cybertrusler og -hændelser, der koordineres af Grækenland.

9. ERINDRER OM de eksisterende rammer for samarbejde mellem EU's institutioner, organer og agenturer såsom det strukturerede samarbejde mellem ENISE og CERT-EU samt aftalememorandummet mellem ENISA, Det Europæiske Forsvarsagentur (EDA), Europols Europæiske Center for Bekæmpelse af Cyberkriminalitet (EC3) og CERT-EU, UNDERSTREGER betydningen af fortsat regelmæssig informationsudveksling med Rådet om den videre udvikling inden for disse samarbejdsrammer,

10. FREMHÆVER vigtigheden af at styrke samarbejdet og informationsudvekslingen mellem de forskellige cyberfællesskaber inden for EU og dets medlemsstater på alle nødvendige niveauer – teknisk, operationelt og strategisk/politisk – og knytte eksisterende krisestyringsmekanismer, -netværker, -strukturer, -processer og -procedurer, hvor dette støtter og forbedrer håndteringen af væsentlige cyberhændelser og -kriser,

11. ANERKENDER de fremskridt, der er gjort af en gruppe medlemsstater med henblik på at oprette en fælles operationel cyberberedskabskapacitet "cyberberedskabshold" inden for rammerne af PESCO med sigte på at uddybe det frivillige samarbejde på cyberområdet gennem gensidig bistand, herunder som reaktion på væsentlige cyberhændelser og -kriser,

12. ANERKENDER de retshåndhævende myndigheders erfaringer og kapacitet til at reagere døgnet rundt på området operationelt samarbejde og sikker informationsudveksling mod større grænseoverskridende cyberangreb gennem beredskabsprotokollen for EU-retshåndhævelsesindsatsen,

13. ANERKENDER den fortsatte gennemførelse af rammen for EU's fælles diplomatiske reaktion på ondsindede cyberaktiviteter ("cyberdiplomatisk værktøjskasse"), ERINDRER OM, at enhver medlemsstat frit kan træffe sin egen suveræne beslutning med hensyn til tilskrivelse af en ondsindet cyberaktivitet, der træffes fra sag til sag, ERINDRER OM, at de foranstaltninger, der træffes inden for rammerne af EU's diplomatiske reaktion på ondsindede cyberaktiviteter bør baseres på en fælles situationsbevidsthed efter enighed blandt medlemsstaterne. EU INTCEN spiller en central rolle som knudepunkt for tilvejebringelsen af situationsbevidsthed og trusselsvurdering med hensyn til cyberspørgsmål for EU på grundlag af frivillige efterretningsbidrag fra medlemsstaterne, og uden at det berører deres kompetencer,

14. GENTAGER betydningen af gensidig bistand og solidaritet i overensstemmelse med artikel 42, stk. 7, i traktaten om Den Europæiske Union og artikel 222 i traktaten om Den Europæiske Unions funktionsmåde og OPFORDRER TIL yderligere øvelser med en cyberdimension, ERINDRER om behovet for at overveje sammenhængen mellem EU's ramme for håndtering af cybersikkerhedskriser, den cyberdiplomatiske værktøjskasse og bestemmelserne i ovennævnte artikler i tilfælde af en væsentlig cyberhændelse eller -krise, MINDER endvidere OM, at medlemsstaternes forpligtelser i medfør af artikel 42, stk. 7, i traktaten om Den Europæiske Union ikke berører den særlige karakter af visse medlemsstaters sikkerheds- og forsvarspolitik, ERINDRER ligeledes OM, at NATO fortsat er fundamentet for det kollektive forsvar af de stater, der er NATO-medlemmer,

15. ANERKENDER samarbejdet mellem EU og NATO om cybersikkerhed og -forsvar, herunder informationsudveksling mellem CERT-EU og NATO Computer Incident Response Capability (NCIRC) under fuld overholdelse af principperne om gennemsigtighed, gensidighed og inklusivitet samt begge organisationers selvstændige beslutningstagning,

16. ANERKENDER betydningen af samarbejde, når det er relevant, med den private sektor med hensyn til informationsudvekslingsøvelser og tilvejebringelse af relevant ekspertise samt pålidelige løsninger og tjenester, herunder f.eks. støtte til reaktioner på hændelser og styrkelse af situationsbevidsthed mellem forskellige cyberfællesskaber,

17. UNDERSTREGER betydningen af sikre kommunikationskanaler til udveksling af klassificerede og følsomme informationer, FREMHÆVER behovet for yderligere fremskridt.

I den forbindelse og under hensyntagen til ovenstående

18. ANERKENDER RÅDET Kommissionens henstilling om oprettelse af en fælles cyberenhed som et initiativ, der skal overvejes i forbindelse med videreudvikling af EU's ramme for håndtering af cybersikkerhedskriser[13], og

19. OPFORDRER EU og dets medlemsstater til at fortsætte deres bestræbelser hen imod en mere omfattende og effektiv EU-ramme for håndtering af cybersikkerhedskriser, der bygger på eksisterende mekanismer og på de fremskridt, der allerede er gjort, og til at overveje potentialet i initiativet om en fælles cyberenhed til at supplere disse mekanismer ved at anvende en trinvis tilgang, UNDERSTREGER, at en trinvis, gennemsigtig og inklusiv proces er afgørende for at øge tilliden og derfor afgørende for videreudviklingen af EU's ramme for håndtering af cybersikkerhedskriser. Denne proces bør respektere medlemsstaternes og EU-institutionernes, -organernes og -agenturernes eksisterende roller, kompetencer og mandater samt principperne i disse konklusioner, herunder proportionalitet, nærhed, inklusivitet, komplementaritet, ikkeoverlapning og informationers fortrolighed, UNDERSTREGER samtidig, at enhver mulig deltagelse i eller bidrag fra medlemsstaterne til en potentiel fælles cyberenhed er frivillig,

[13] C(2021)4520 final (11155/21 og 11155/21 ADD1).

20. UNDERSTREGER behovet for at fastlægge passende arbejdsmetoder og styring med henblik på at muliggøre inddragelse og deltagelse af alle medlemsstaterne i drøftelserne, udviklingen og effektive beslutningsprocesser vedrørende EU's ramme for håndtering af cybersikkerhedskriser, herunder vedrørende initiativet om en potentiel fælles cyberenhed, OPFORDRER til, at Rådets beføjelser i henhold til traktaterne og princippet om loyalt samarbejde respekteres,

21. UNDERSTREGER betydningen af at identificere og inddrage alle relevante cyberfællesskaber i EU og dets medlemsstater, samtidig med at der tages hensyn til deres forskellige roller og ansvarsområder i forbindelse med forskellige typer af væsentlige cyberhændelser og -kriser, UNDERSTREGER Rådets afgørende rolle, navnlig gennem Cybergruppen, i politikudformnings- og koordineringsfunktionen med hensyn til videreudvikling af EU's ramme for håndtering af cybersikkerhedskriser, OPFORDRER derfor medlemsstaterne, Kommissionen, Tjenesten for EU's Optræden Udadtil (EU-Udenrigstjenesten), EU INTCEN, CERT-EU, ENISA, Europol (EC3), Eurojust (EJCN), Det Europæiske Industri-, Teknologi- og Forskningskompetencecenter for Cybersikkerhed og repræsentanter fra CSIRT-netværket, CyCLONe, NIS-samarbejdsgruppen, EDA og relevante PESCO-projekter samt andre mulige interessenter til at deltage i denne proces. Som foreslået i Kommissionens henstilling, kunne det undersøges nærmere at nedsætte en mulig arbejdsgruppe som, idet der sikres en passende repræsentation af alle medlemsstater og handles efter politisk vejledning fra Rådet, skal fungere som et midlertidigt forum, der samler repræsentanter for alle relevante cyberfællesskaber i medlemsstaterne og i EU. En sådan arbejdsgruppe bør regelmæssigt aflægge rapport om sine aktiviteter og forelægge Rådet eventuelle forslag til drøftelse, godkendelse og yderligere vejledning. Derudover kan der etableres andre former for dialog inden for og på tværs af fællesskaber, herunder gennem workshopper, seminarer, fælles uddannelse og øvelser,

22. UNDERSTREGER den rolle, som Det Europæiske Industri-, Teknologi- og Forskningskompetencecenter for Cybersikkerhed og Netværket af Nationale Koordinationscentre spiller i forhold til den potentielle fælles cyberenhed, navnlig i betragtning af dens rolle med hensyn til væsentligt at øge Unionens teknologiske kapacitet, teknologiske løsninger, kapacitet og færdigheder på området cybersikkerhed,

23. OPFORDRER EU og dets medlemsstater til at deltage i videreudviklingen af EU's ramme for håndtering af cybersikkerhedskriser, herunder ved at udforske potentialet i initiativet om en fælles cyberenhed, ved at fastlægge og definere processen, herunder milepæle og en tidsplan samt præcisere målene og de mulige roller og ansvarsområder, FREMHÆVER behovet for som en prioritet at konsolidere eksisterende netværk og interaktioner inden for hvert enkelt fælleskab samt at etablere en grundig kortlægning af eventuelle informationsudvekslingsmangler og -behov inden for og på tværs af cyberfællesskaber og også inden for og på tværs af EU-institutioner, -organer og -agenturer og efterfølgende nå til enighed om mulige primære mål og prioriteter for en potentiel fælles cyberenhed, UNDERSTREGER uden at foregribe resultatet behovet for at fokusere på indkredsning af behov for informationsudveksling med henblik på at opbygge en fælles situationsbevidsthed blandt alle relevante fællesskaber. I forbindelse med indkredsningen af informationsudvekslingsmangler og -behov, herunder eventuel brug af virtuelle platforme, bør der fortsat lægges behørig vægt på sikre kommunikationskanaler til udveksling af klassificerede og følsomme informationer, mens Rådet samtidig UNDERSTREGER betydningen af at anvende allerede eksisterende infrastruktur. Hensigten med at indføre en gradvis tilgang er at opbygge tillid og et grundlag for eventuelle yderligere skridt i forbindelse med forbedring af beredskabet og det operationelle samarbejde. ANERKENDER, at forskellige mål kan berettige til forskellige løsninger og inddragelse af et andet sæt repræsentanter for relevante cyberfællesskaber i EU og dets medlemsstater,

24. OPFORDRER til yderligere overvejelser om et retsgrundlag for den potentielle fælles cyberenhed gennem hele processen, herunder en vurdering af opgaverne og rollerne i forhold til dem, der er tildelt ENISA i henstillingen i lyset af artikel 7 i Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019, OPFORDRER til yderligere overvejelser om de enkelte elementer i henstillingen om den fælles cyberenhed, herunder med hensyn til idéen om EU-beredskabsholdene for cybersikkerhed og EU's hændelses- og kriseberedskabsplan for cybersikkerhed, FREMHÆVER, at en potentiel fælles cyberenhed skal respektere de mulige fremtidige deltageres kompetencer, mandater og retlige beføjelser,

25. OPFORDRER EU og dets medlemsstater til at overveje potentialet i initiativet om en fælles cyberenhed, også set fra EU's institutionernes, -organernes og -agenturernes perspektiv med henblik på at supplere den igangværende indsats på medlemsstatsniveau, SER MED TILFREDSHED PÅ, at Kommissionen agter at styrke de relevante EU-institutioners, -organers og -agenturers robusthed gennem sit kommende forslag til en forordning om fælles bindende regler om cybersikkerhed for alle EU-institutioner, -organer og -agenturer,

26. GENTAGER afslutningsvis sit tilsagn om at styrke cyberrobustheden og videreudvikle EU's ramme for håndtering af cybersikkerhedskriser og VIL REGELMÆSSIGT FØLGE fremskridtene og udstikke yderligere retningslinjer for supplering af EU's ramme for håndtering af cybersikkerhedskriser.