Rådet for
Den Europæiske Union

Bruxelles, den 23. maj 2022
(OR. en)

9364/22

CYBER 183	**EUMC 170**
COPEN 202	**IPCR 54**
COPS 228	**HYBRID 46**
COSI 142	**DISINFO 45**
DATAPROTECT 166	**COTER 126**
IND 189	**CSDP/PSDC 304**
JAI 698	**CFSP/PESC 685**
JAIEX 57	**CIVCOM 93**
POLMIL 120	**RECH 262**
RELEX 681	**PROCIV 65**
TELECOM 237	

RESULTAT AF DRØFTELSERNE

fra:	Generalsekretariatet for Rådet
dato:	23. maj 2022
til:	delegationerne
Vedr.:	Rådets konklusioner om udviklingen af Den Europæiske Unions cyberposition – Rådets konklusioner godkendt af Rådet på samlingen den 23. maj 2022

Vedlagt følger til delegationerne Rådets konklusioner om udviklingen af Den Europæiske Unions cyberposition, der blev godkendt af Rådet på samlingen den 23. maj 2022.

BILAG

Rådets konklusioner om udviklingen af Den Europæiske Unions cyberposition

RÅDET FOR DEN EUROPÆISKE UNION,

SOM MINDER OM sine konklusioner om:

– den fælles meddelelse af 25. juni 2013 til Europa-Parlamentet og Rådet om en EU-strategi for cybersikkerhed: "Et åbent, sikkert og beskyttet cyberspace"[1]

– rammen for EU's cyberforsvarspolitik[2]

– internetforvaltning[3]

– cyberdiplomati[4]

– styrkelse af Europas system for modstandsdygtighed over for cyberangreb og fremme af en konkurrencedygtig og innovativ cybersikkerhedsindustri[5]

– fælles meddelelse af 20. november 2017 til Europa-Parlamentet og Rådet: "Modstandsdygtighed, afskrækkelse og forsvar: opbygning af en stærk cybersikkerhed for EU"[6]

– en ramme for EU's fælles diplomatiske reaktion på ondsindede cyberaktiviteter ("cyberdiplomatisk værktøjskasse")[7]

– en koordineret EU-reaktion på væsentlige cybersikkerhedshændelser og -kriser[8]

– EU's retningslinjer for opbygning af ekstern cyberkapacitet[9]

---

1 12109/13.
2 15585/14.
3 16200/14.
4 6122/15 + COR 1.
5 14540/16.
6 14435/17 + COR 1.
7 10474/17.
8 10086/18.
9 10496/18.

– Rådets gennemførelsesafgørelse (EU) 2018/1993 af 11. december 2018 om EU's integrerede ordninger for politisk kriserespons[10]

– opbygning af cybersikkerhedskapacitet i EU[11]

– betydningen af 5G for den europæiske økonomi og behovet for at afbøde de sikkerhedsrisici, der er forbundet med 5G[12]

– fremtiden for et højdigitaliseret Europa efter 2020: "Styrke den digitale og økonomiske konkurrenceevne i hele Unionen og den digitale samhørighed"[13]

– supplerende tiltag for at styrke modstandsdygtighed og imødegå hybride trusler[14]

– Europas digitale fremtid i støbeskeen[15]

– cybersikkerheden ved forbundet udstyr[16]

– EU's strategi for cybersikkerhed for det digitale årti[17]

– sikkerhed og forsvar[18]

– undersøgelse af potentialet i initiativet om den fælles cyberenhed – supplement til en koordineret EU-reaktion på væsentlige cybersikkerhedshændelser og -kriser[19]

– Et strategisk kompas for sikkerhed og forsvar – For en Europæisk Union, der beskytter sine borgere, værdier og interesser og bidrager til international fred og sikkerhed[20],

---

10 EUT L 320 af 17.12.2018, s. 28.
11 7737/19.
12 14517/19.
13 9596/19.
14 14972/19.
15 8711/20.
16 13629/20.
17 7290/21.
18 8396/21.
19 13048/21.
20 7371/22.

1. UNDERSTREGER, at ondsindet adfærd i cyberspace, som hidrører fra både statslige og ikkestatslige aktører, er taget til i de seneste år, bl.a. i form af en kraftig og vedvarende stigning i ondsindede aktiviteter rettet mod EU's og dets medlemsstaters kritiske infrastruktur, forsyningskæder og intellektuel ejendom, øget risiko for afsmittende virkninger samt en stigning i ransomwareangreb mod vores virksomheder, organisationer og borgere. NOTERER SIG, at nogle lande med magtpolitikkens tilbagevenden i stigende grad forsøger at udfordre og underminere den regelbaserede internationale orden i cyberspace, hvilket i stigende grad gør såvel cybersfæren som det åbne hav, luftrummet og det ydre rum til omstridte områder. ANERKENDER, at omfattende cyberangreb og forsøg på at trænge ind i, afbryde eller destruere netværk og informationssystemer med systemiske virkninger er blevet mere udbredte, kan underminere vores økonomiske sikkerhed og påvirke vores demokratiske institutioner og processer og viser visse aktørers parathed til at bringe den internationale sikkerhed og stabilitet i fare. UNDERSTREGER, at Ruslands militære aggression mod Ukraine har påvist, at offensive cyberaktiviteter kan gennemføres som en integreret del af hybride strategier, der kombinerer intimidering, destabilisering og økonomiske forstyrrelser.

2. GENTAGER, at over for de igangværende geopolitiske forandringer ligger vores Unions styrke i sammenhold, solidaritet og beslutsomhed, og at gennemførelsen af det strategiske kompas vil styrke EU's strategiske autonomi og EU's evne til at samarbejde med partnere for at beskytte sine værdier og interesser, herunder på cyberområdet. UNDERSTREGER, at et stærkere og mere kompetent EU på sikkerheds- og forsvarsområdet vil bidrage positivt til global og transatlantisk sikkerhed og er et supplement til NATO, der fortsat udgør grundlaget for dets medlemmers kollektive forsvar. BEKRÆFTER PÅ NY, at EU agter at intensivere støtten til den regelbaserede internationale orden med De Forenede Nationer i centrum.

3. GENTAGER i overensstemmelse med Rådets konklusioner om EU's strategi for cybersikkerhed og det strategiske kompas behovet for at udvikle Unionens cyberposition ved at styrke vores evne til at forebygge cyberangreb gennem kapacitetsopbygning, kapacitetsudvikling, uddannelse, øvelser og øget modstandsdygtighed og ved at reagere beslutsomt på cyberangreb mod EU og dets medlemsstater med brug af alle tilgængelige EU-værktøjer. Dette omfatter yderligere demonstration af, at EU er fast besluttet på at reagere øjeblikkeligt og langsigtet på trusselsaktører, der forsøger at nægte os sikker og åben adgang til cyberspace og påvirke vores strategiske interesser, herunder vores partneres sikkerhed. UNDERSTREGER i den forbindelse, at cyberpositionen sigter mod at kombinere de forskellige initiativer, som bidrager til EU-foranstaltninger, der konsoliderer fred og stabilitet i cyberspace og er til fordel for et åbent, frit, globalt, stabilt og sikkert cyberspace, samtidig med at aktioner på kort, mellemlang og lang sigt koordineres bedre for at forebygge, modvirke, afskrække fra og reagere på cybertrusler og -angreb, og cyberkapaciteter udnyttes. UNDERSTREGER, at disse elementer bør indarbejdes i EU's cyberposition i overensstemmelse med EU's fem funktioner på cyberområdet: styrke vores cyberrobusthed og beskyttelseskapacitet; øge solidarisk og omfattende krisestyring; fremme vores vision for cyberspace; forbedre samarbejdet med partnerlande og internationale organisationer; forebygge, forsvare mod og reagere på cyberangreb.

I. STYRKE VORES CYBERROBUSTHED OG BESKYTTELSESKAPACITET

4. GENTAGER behovet for øge det generelle EU-cybersikkerhedsniveau, SER FREM TIL den hurtige vedtagelse af udkastet til direktiv om foranstaltninger, der skal sikre et højt fælles cybersikkerhedsniveau i hele Unionen (NIS), udkastet til forordning om digital operationel modstandsdygtighed i den finansielle sektor (DORA), udkastet til direktiv om kritiske enheders modstandsdygtighed (CER) og NOTERER SIG forslaget til forordning om foranstaltninger til sikring af et højt cybersikkerhedsniveau i EU's institutioner, organer, kontorer og agenturer, der har til formål at fremme en Europæisk Union, der beskytter sine borgere, offentlige tjenester og virksomheder i cyberspace. OPFORDRER Kommissionen til at afslutte vedtagelsen af centrale forslag, der skal sikre, at digital infrastruktur, digitale teknologier, produkter og tjenester er sikre, med henblik på at sende et klart signal om EU's ambitioner på disse områder og for at støtte virksomheder, så de er rustet til udfordringen. OPFORDRER Kommissionen til at fremsætte forslag om fælles EU-krav til cybersikkerhed for forbundet udstyr og tilknyttede processer og tjenester gennem retsakten om cyberrobusthed, som Kommissionen bør fremsætte forslag om inden udgangen af 2022, under hensyntagen til behovet for en horisontal og holistisk tilgang, der omfatter hele livscyklussen for digitale produkter og tjenester, samt eksisterende lovgivning, navnlig på cybersikkerhedsområdet.

5. OPFORDRER de relevante myndigheder såsom Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation (BEREC), Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) og samarbejdsgruppen for net- og informationssystemer (NIS) TIL sammen med Europa-Kommissionen at udarbejde henstillinger på grundlag af en risikovurdering til medlemsstaterne og Europa-Kommissionen for at styrke modstandsdygtigheden i kommunikationsnet og -infrastruktur inden for Den Europæiske Union, herunder den fortsatte gennemførelse af EU's 5G-værktøjskasse.

6. OPFORDRER EU og dets medlemsstater til at styrke indsatsen for at øge det generelle cybersikkerhedsniveau, f.eks. ved at lette fremkomsten af udbydere af cybersikkerhedstjenester, man kan have tillid til, og UNDERSTREGER, at fremme af udviklingen af sådanne udbydere bør være en prioritet for EU's industripolitik på cybersikkerhedsområdet. OPFORDRER, for bedre at kunne modstå og bekæmpe cyberangreb med potentielle systemiske virkninger og på grundlag af erfaringerne med håndteringen af sårbarhederne i Solarwinds, Microsoft Exchange og Apache Log4J, Kommissionen til at foreslå muligheder, der tilskynder til fremkomsten af en industri med cybersikkerhedstjenester, man kan have tillid til, styrker cybersikkerheden i IKT-forsyningskæden, tackler de potentielle virkninger af softwaresårbarheder for EU og dets medlemsstater, bl.a. med henblik på den kommende retsakt om cyberrobusthed, og forbedrer detektion af cybertrusler og deling af kapaciteter i og mellem medlemsstaterne.

7. SOM GENTAGER, at investering i innovation og bedre udnyttelse af civil teknologi er afgørende for at styrke vores teknologiske suverænitet, herunder på cyberområdet, OPFORDRER Kommissionen til hurtigt at gøre Det Europæiske Kompetencecenter for Cybersikkerhed operationelt med henblik på at udvikle et stærkt europæisk forskningsmæssigt, industrielt og teknologisk cyberøkosystem, og UNDERSTREGER behovet for at fremme forskning og innovation, investere mere i civile og forsvarsmæssige områder for at styrke EU's forsvarsteknologiske og -industrielle base (EDTIB) og udvikle EU's og dets medlemsstaters cyberkapaciteter, herunder strategiske støttekapaciteter. UNDERSTREGER betydningen af at gøre intensiv brug af nye teknologier, navnlig kvantecomputing, kunstig intelligens og big data, for at opnå komparative fordele, herunder med hensyn til operationer som reaktion på cyberhændelser.

8. SOM ANERKENDER, at styrkelse af vores cybersikkerhed er en måde, hvorpå vi kan øge effektiviteten og sikkerheden af vores indsats til lands, i luften, til vands og i det ydre rum, UNDERSTREGER vigtigheden af at integrere cybersikkerhedshensyn i alle EU's offentlige politikker, herunder sektorspecifik lovgivning, som supplerer NIS 2-direktivet, og OPFORDRER Kommissionen til at undersøge mulighederne for at øge cybersikkerheden i hele forsyningskæden i EU's forsvarsteknologiske og -industrielle base (EDTIB).

9. ANERKENDER, at det er afgørende at sikre tilstrækkelige finansielle og menneskelige ressourcer til cybersikkerhed og foranstaltninger, der sigter mod at skabe et gunstigt klima, så den private sektor kan være konkurrencedygtig, med henblik på at udvikle EU's cyberposition, og at spørgsmålet om stabil og langsigtet finansiering af cybersikkerhed også bør behandles på EU-plan ved at udarbejde og implementere en horisontal mekanisme, der kombinerer flere kilder til finansiering, herunder omkostningen ved højt kvalificerede menneskelige ressourcer. OPFORDRER derfor Kommissionen til at undersøge mulighederne for en sådan mekanisme inden udgangen af 2022, som skal drøftes i Rådets relevante organer.

10. UNDERSTREGER behovet for at styrke vores indsats og øge samarbejdet i kampen mod international cyberkriminalitet, navnlig ransomware, gennem EMPACT-mekanismen (europæisk tværfaglig platform mod kriminalitetstrusler), via udvekslinger mellem sektorerne for cybersikkerhed, retshåndhævelse og diplomati og ved styrkelse af retshåndhævelseskapaciteten inden for efterforskning og retsforfølgelse af cyberkriminalitet. GENTAGER sit tilsagn om at informere offentligheden om cybertrusler og de foranstaltninger, der er truffet på nationalt plan og EU-plan for at modvirke disse trusler ved at inddrage civilsamfundet, den private sektor og den akademiske verden med henblik på at øge kendskabet til og fremme et passende niveau af cyberbeskyttelse og cyberhygiejne. UNDERSTREGER behovet for at fokusere på borgernes cybersikkerhedsfærdigheder og -evner på EU- og medlemsstatsplan og behovet for aktivt at inddrage brugerne i deres egen beskyttelse.

II. ØGE SOLIDARISK OG OMFATTENDE KRISESTYRING

11. UNDERSTREGER ud fra erfaringerne med de årlige cyberøvelser, andre øvelser med en cyberdimension og EU CyCLES 2022-øvelsen betydningen af at oprette et program for regelmæssige cyberøvelser på tværs af samfund og på flere niveauer med henblik på at afprøve og udvikle EU's interne og eksterne reaktion på omfattende cyberhændelser med deltagelse af Rådet, EU-Udenrigstjenesten, Kommissionen og relevante interessenter såsom ENISA og den private sektor, og som vil blive formuleret og bidrage til EU's generelle øvelsespolitik. UNDERSTREGER betydningen af at videreudvikle Cyber Europe- og BlueOLEx-øvelserne ved at kombinere reaktionen på tværs af forskellige niveauer. ANERKENDER behovet for at evaluere og konsolidere de eksisterende øvelser og undersøge muligheden for yderligere øvelser inden for specifikke segmenter af cyberområdet, navnlig en militær CERT-øvelse og en øvelse med fokus på krisesamarbejde mellem EU-institutioner, -organer og -agenturer. ANERKENDER, at Unionens cyberposition vil styrke vores evne til at forebygge cyberangreb gennem forskellige tiltag, herunder uddannelse, og OPFORDRER derfor medlemsstaterne til at styrke det civil-militære samarbejde om cyberuddannelse og fælles øvelser.

12. UNDERSTREGER behovet for yderligere at afprøve og styrke operationelt samarbejde og fælles situationsbevidsthed blandt medlemsstaterne, herunder gennem etablerede netværk såsom CSIRT-netværket og Det Europæiske Netværk af Forbindelsesorganisationer for Cyberkriser (EU-CyCLONe), med henblik på at fremme EU's beredskab over for omfattende cyberhændelser. UNDERSTREGER betydningen af at arbejde på at udvikle et fælles sprog blandt medlemsstaterne og med EU-institutioner, -organer og -agenturer, som er skræddersyet til drøftelse på politisk plan, for at støtte udarbejdelsen af en konsolideret vurdering af alvoren og virkningen af relevante cyberhændelser samt mulige udviklingsscenarier og de behov, der opstår som følge heraf, hvor det er relevant. UNDERSTREGER i den forbindelse behovet for at forbedre komplementariteten af fælles situationsvurderingsrapporter, herunder EU-CyCLONes rapporter om virkningen og alvoren af omfattende cyberhændelser på tværs af EU's medlemsstater og trusselsvurderinger leveret af EU INTCEN inden for rammerne af EU's cyberdiplomatiske værktøjskasse. OPFORDRER Kommissionen, den højtstående repræsentant og NIS-samarbejdsgruppen TIL i samordning med relevante civile og militære organer og agenturer og etablerede netværk, herunder EU-CyCLONe, inden udgangen af 2022 at foretage en risikoevaluering og opstille risikoscenarier ud fra et cybersikkerhedsperspektiv i en situation, hvor der er en trussel eller et muligt angreb mod medlemsstater eller partnerlande, og forelægge dem for de relevante rådsorganer. UNDERSTREGER behovet for passende og koordineret offentlig kommunikation om EU's reaktion på omfattende cyberhændelser.

13. UNDERSTREGER i tilfælde af en omfattende cyberhændelse behovet for at styrke koordineringen og, hvor det er relevant, idet der bygges videre på de fremskridt, der er gjort, og det arbejde, som PESCO-cyberberedskabshold har udført, og idet der trækkes på det arbejde, som CSIRT-netværket og EU-CyCLONe har udført, den frivillige sammenlægning af vores hændelsesberedskabskapaciteter blandt medlemsstaterne. ANERKENDER, at udvikling af forbindelser med den private sektor kan forstærke de offentlige kapaciteter, navnlig i en situation med mangel på kvalificeret arbejdskraft i hele EU, og at identificering og koordinering af disse private partnere kan gøre en forskel i tilfælde af omfattende hændelser. OPFORDRER Kommissionen TIL med henblik på fuldt ud at forberede sig på at stå over for omfattende cyberhændelser at forelægge et forslag om en ny katastrofeberedskabsfond for cybersikkerhed inden udgangen af tredje kvartal 2022.

14. GENTAGER i overensstemmelse med det strategiske kompas, at der er behov for at investere i vores gensidige bistand i henhold til artikel 42, stk. 7, i traktaten om Den Europæiske Union samt solidaritet i henhold til artikel 222 i traktaten om Den Europæiske Unions funktionsmåde, navnlig gennem hyppige øvelser. UNDERSTREGER i denne forbindelse behovet for at arbejde videre med levering og koordinering af bilateral civil og/eller militær støtte, bl.a. ved at undersøge mulig støtte fra EU efter udtrykkelig anmodning fra medlemsstaterne, og med fastlæggelse af passende beredskabsforanstaltninger, herunder ved at udvikle en koordineret kommunikationsstrategi, i forbindelse med gennemførelsen af artikel 42, stk. 7. BEMÆRKER, at dette også bør omfatte undersøgelse af forbindelserne med EU's eksisterende krisestyringsmekanismer og EU-civilbeskyttelsesmekanismen.

15. UNDERSTREGER, at en styrket EU-cyberposition vil kræve skærpet sikker kommunikation. GENTAGER med henblik herpå retningslinjerne i det strategiske kompas i den henseende og OPFORDRER Kommissionen og andre relevante institutioner, organer og agenturer TIL inden udgangen af 2022 at kortlægge de eksisterende redskaber til sikker kommunikation på cyberområdet, der skal drøftes i relevante rådsorganer og med relevante samarbejdsgrupper såsom CSIRT-netværket og EU-CyCLONe.

III. FREMME VORES VISION FOR CYBERSPACE

16. MINDER OM, at den fælles og samlede EU-tilgang til cyberdiplomati har til formål at bidrage til konfliktforebyggelse, afbødning af cybersikkerhedstrusler og større stabilitet i internationale forbindelser. BEKRÆFTER i denne sammenhæng PÅ NY EU's tilsagn om at bilægge internationale tvister i cyberspace med fredelige midler og anvendelsen af folkeretten, herunder den internationale menneskerettighedslovgivning og den humanitære folkeret, på staternes handlinger i cyberspace. UNDERSTREGER EU's og dets medlemsstaters tilsagn om at handle i overensstemmelse med de frivillige, ikkebindende normer for ansvarlig statslig adfærd i cyberspace, som alle FN's medlemsstater er blevet enige om. FREMHÆVER betydningen af et åbent, frit, globalt, stabilt og sikkert cyberspace, hvor menneskerettighederne, de grundlæggende frihedsrettigheder og retsstatsprincippet fuldt ud anvendes til støtte for vores frie og demokratiske samfunds sociale trivsel, økonomiske vækst, velstand og integritet, og BEKRÆFTER PÅ NY EU's og dets medlemsstaters tilsagn om at vedblive med at fremme disse værdier og principper. UNDERSTREGER med henblik på at udvikle kanaler for konstruktiv, ærlig og åben dialog med centrale interessenter på cyberspaceområdet betydningen af at gøre cyberspørgsmål, herunder EU's cyberdiplomatiske værktøjskasse, til en integreret del af Unionens tiltrædelsesforhandlinger og af EU's strategiske og politiske dialoger med både internationale partnere og konkurrenter, og OPFORDRER samtidig den højtstående repræsentant til at gennemgå de eksisterende bilaterale cyberdialoger og om nødvendigt foreslå, at der indledes et lignende samarbejde med nye lande eller relevante internationale organisationer.

17. MINDER OM betydningen af samarbejde mellem flere interessenter, da andre interessenter også har ansvar for cybersikkerhed, navnlig med hensyn til at gennemføre de henstillinger og beslutninger, der træffes i internationale og regionale fora. OPFORDRER EU og dets medlemsstater TIL i endnu højere grad at fremme vores model for cyberspace og internettet på grundlag af multiinteressenttilgangen og gennem initiativer såsom Parisopfordringen om tillid og sikkerhed i cyberspace og erklæringen om internettets fremtid, idet de understreger de fælles fordele ved stabilitet i cyberspace og gør globalt opmærksom på farerne ved en statscentreret og autoritær vision for internettet, og OPFORDRER EU og dets medlemsstater TIL at styrke samarbejdet med multiinteressentsamfundet yderligere, herunder ved at gøre brug af relevante projekter såsom EU's udenrigspolitiske instruments EU-initiativ vedrørende cyberdiplomati.

18. FORPLIGTER SIG TIL løbende at engagere sig i relevante internationale organisationer, navnlig i processer i forbindelse med FN's 1. og 3. Komité, og understreger samtidig, at gældende folkeret finder anvendelse uden forbehold i og med hensyn til cyberspace. FREMHÆVER betydningen af fortsatte bestræbelser på at opretholde og fremme FN's ramme for ansvarlig statslig adfærd og UNDERSTREGER, at EU og dets medlemsstater vil arbejde aktivt for at styrke gennemførelsen heraf, herunder gennem oprettelsen af handlingsprogrammet til fremme af ansvarlig statslig adfærd i cyberspace. UNDERSTREGER, at EU og dets medlemsstater vil deltage aktivt i forhandlingerne om en kommende FN-konvention, der skal tjene som et effektivt instrument for retshåndhævende og judicielle myndigheder i den globale kamp mod cyberkriminalitet, under fuld hensyntagen til de eksisterende rammer i form af internationale og regionale instrumenter på dette område, navnlig Budapestkonventionen om IT-kriminalitet. FREMHÆVER betydningen af at støtte udviklingen og operationaliseringen af tillidsskabende foranstaltninger på regionalt og internationalt plan yderligere og tilskynde endnu mere til brug af eksisterende tillidsskabende foranstaltninger på cyberområdet i OSCE, også i tider med internationale spændinger.

19. MINDER OM, at det for at sikre, at internettet forbliver globalt, ufragmenteret og åbent, er afgørende at anlægge en proaktiv menneskerettighedsbaseret tilgang til sikring af internationale standarder inden for nye teknologier og den centrale internetarkitektur i overensstemmelse med demokratiske værdier og principper, og STØTTER princippet om, at anvendelsen og udviklingen af teknologier respekterer menneskerettighederne og er privatlivsorienteret, og at brugen heraf er lovlig, sikker og etisk. TILSKYNDER den højtstående repræsentant og Kommissionen TIL at udvikle en strategisk vision for tekniske spørgsmål på det digitale område, som har udenrigspolitiske konsekvenser og kan have indvirkning på cyberspaces og især internettets stabilitet, herunder i de relevante specialiserede internationale organisationer (Den Internationale Telekommunikationsunion osv.).

IV. FORBEDRE SAMARBEJDET MED PARTNERLANDE OG INTERNATIONALE ORGANISATIONER

20. UNDERSTREGER behovet for at forbinde EU's cyberkapacitetsopbygningsstrategi bedre med FN's normer for ansvarlig statslig adfærd i cyberspace, herunder ved at udvikle skræddersyede samarbejds- og kapacitetsopbygningsprogrammer for at støtte tredjelande i deres gennemførelsesbestræbelser og i den forbindelse fortsætte og udvide vores bestræbelser på at fremme FN's handlingsprogram til fremme af ansvarlig statslig adfærd i cyberspace. FREMHÆVER betydningen af fuldt ud at integrere cyberkapacitetsopbygning som en del af EU's tilbud som sikkerhedsgarant med passende koordinering af indsatsen mellem medlemsstaterne og EU-institutioner,-organer og -agenturer og SER navnlig MED TILFREDSHED PÅ samarbejdet mellem medlemsstaterne og med partnere i den offentlige og private sektor, navnlig gennem EU's CyberNet (EU-netværket for cyberkapacitetsopbygning) og det globale forum for cybereksperter (GFCE), for at sikre koordinering og undgå overlapning.

OPFORDRER den højtstående repræsentant og Kommissionen til at nedsætte et råd for EU's cyberkapacitetsopbygning senest i tredje kvartal af 2022 og til at afholde regelmæssige drøftelser i Den Horisontale Gruppe vedrørende Cyberspørgsmål. OPFORDRER Kommissionen og den højtstående repræsentant TIL at mobilisere instrumentet for naboskab, udviklingssamarbejde og internationalt samarbejde (NDICI), instrumentet til førtiltrædelsesbistand (IPA III) og andre finansielle redskaber såsom den europæiske fredsfacilitet og Global Gateway-initiativet yderligere for at støtte styrkelse af vores partneres modstandsdygtighed og deres kapacitet til at identificere og håndtere cybertrusler og efterforske og retsforfølge cyberkriminalitet samt udviklingen af samarbejdsprojekter,

herunder i forbindelse med især kriser, TILSKYNDER TIL samarbejde med partnere på Vestbalkan og i EU's østlige og sydlige nabolande og udsendelse af eksperter fra EU og medlemsstaterne, der kan tilbyde støtte i cyberkriser under hensyntagen til eksisterende juridiske mandater.

21. FREMHÆVER behovet for at intensivere bestræbelserne på at udvikle en struktureret og åben EU-outreachtilgang til, hvordan man fremmer en global fælles forståelse af anvendelsen af folkeretten i cyberspace, FN's ramme for ansvarlig statslig adfærd i cyberspace, herunder initiativet til et handlingsprogram til fremme af ansvarlig statslig adfærd i cyberspace, samt til EU's og dets medlemsstaters holdning i de igangværende forhandlinger om en FN-konvention om IT-kriminalitet og ANMODER som led i disse bestræbelser den højtstående repræsentant OM at forelægge en outreachplan for Rådet inden udgangen af 2022. TILSKYNDER den højtstående repræsentant og Kommissionens tjenestegrene TIL at gøre fuld og systematisk brug af de 145 delegationer og udvikle et regelmæssigt og frugtbart samarbejde mellem dem og medlemsstaternes ambassader i tredjelande inden for rammerne af det planlagte cyberdiplomatiske EU-netværk. OPFORDRER den højtstående repræsentant TIL senest i tredje kvartal af 2022 at oprette det cyberdiplomatiske EU-netværk, der skal bidrage til informationsudveksling, fælles uddannelsesaktiviteter for EU's og medlemsstaternes personale, sammenhængende kapacitetsopbygningsbestræbelser og styrkelse af gennemførelsen af FN's ramme for ansvarlig statslig adfærd samt tillidsskabende foranstaltninger mellem stater.

22. FREMHÆVER sit tilsagn om yderligere samarbejde med internationale organisationer og partnerlande for at fremme den fælles forståelse af cybertrusselsbilledet, udvikle samarbejdsmekanismer og fastlægge en samarbejdsbaseret diplomatisk indsats proaktivt. ERINDRER OM de vigtigste resultater af samarbejdet mellem EU og NATO på cybersikkerhedsområdet inden for rammerne af gennemførelsen af de fælles erklæringer fra Warszawa i 2016 og Bruxelles i 2018 med fuld respekt for begge organisationers beslutningsautonomi og procedurer på grundlag af principperne om gennemsigtighed, gensidighed og inklusivitet, UNDERSTREGER behovet for at styrke cybersamarbejdet med NATO yderligere gennem øvelser, informationsudveksling og udvekslinger mellem eksperter, herunder om kapacitetsudvikling, kapacitetsopbygning for partnere og missioner og operationer, samt om anvendeligheden af folkeretten og FN's normer for ansvarlig statslig adfærd i cyberspace og mulige koordinerede reaktioner på ondsindede cyberaktiviteter.

V. FOREBYGGE, FORSVARE MOD OG REAGERE PÅ CYBERANGREB

23. ANERKENDER, at cyberspace er blevet en skueplads for geopolitisk konkurrence, og GENTAGER derfor, at EU skal være i stand til hurtigt og virkningsfuldt at reagere på cyberangreb såsom statsstøttede ondsindede cyberaktiviteter rettet mod EU og dets medlemsstater og derfor må styrke EU's cyberdiplomatiske værktøjskasse og gøre fuld brug af alle deres instrumenter, herunder de tilgængelige politiske, økonomiske, diplomatiske, retlige og strategiske kommunikationsredskaber til at forebygge, modvirke, afskrække fra og reagere på ondsindede cyberaktiviteter. UNDERSTREGER, at fjendtlige aktører må være opmærksomme på, at cyberangreb mod medlemsstater og EU-institutioner vil blive opsporet tidligt, identificeret omgående og mødt med alle nødvendige redskaber og politikker. OPFORDRER medlemsstaterne og den højtstående repræsentant TIL, navnlig med udgangspunkt i de elementer af cyberpositionen, som er indeholdt deri, og erfaringerne fra gennemførelsen af den cyberdiplomatiske værktøjskasse siden dens indførelse og fra EU CyCLES-øvelsen, med støtte fra Kommissionen at arbejde hen imod en revideret udgave af retningslinjerne for gennemførelsen af EU's cyberdiplomatiske værktøjskasse inden udgangen af første kvartal 2023, navnlig ved at undersøge supplerende beredskabsforanstaltninger.

24. UNDERSTREGER behovet for at afholde regelmæssige drøftelser om cybertrusselsbilledet i Rådets relevante organer og udvalg, samtidig med at der regelmæssigt samarbejdes med den private sektor og trækkes på vurderingen af konsekvenserne og alvoren af de seneste hændelser, for at øge den generelle bevidsthed om og beredskab med henblik på nye anvendelser af EU's cyberdiplomatiske værktøjskasse og udvikle flere værktøjer til støtte for dens gennemførelse. BEMÆRKER, at der, selv om den nationale sikkerhed forbliver den enkelte medlemsstats eneansvar, er behov for at styrke efterretnings- og informationsudvekslingen og -samarbejdet mellem medlemsstaterne samt med EU INTCEN for at kunne udveksle efterretninger i begyndelsen af beslutningsprocessen, herunder om spørgsmålet om tilskrivning, og derved muliggøre en hurtig, effektiv og velunderbygget reaktion på ondsindede cyberaktiviteter rettet mod EU og dets partnere. GENTAGER, at det er vigtigt at styrke EU INTCEN's kapacitet på cyberområdet på grundlag af frivillige efterretningsbidrag fra medlemsstaterne, og uden at dette berører deres kompetencer, og at undersøge forslaget om en mulig oprettelse af en arbejdsgruppe om cyberintelligens for medlemsstaterne.

25. ANERKENDER, at EU's erklæringer og restriktive foranstaltninger, der er truffet inden for rammerne af EU's cyberdiplomatiske værktøjskasse, har sendt et stærkt signal om, at ondsindede cyberaktiviteter, der udgør en ekstern trussel mod EU, dets medlemsstater og dets partnere, er uacceptable og dermed bidrager til at forebygge, modvirke, afskrække fra og reagere på ondsindede cyberaktiviteter, GENTAGER sit tilsagn om at anvende disse foranstaltninger med henblik på at gøre opmærksom på de forpligtelser, der gælder for cyberspace i henhold til folkeretten, herunder FN-pagten i sin helhed, og fremme FN's ramme for ansvarlig statslig adfærd i cyberspace, herunder alle staters due diligence-forpligtelse til ikke bevidst at tillade, at deres område anvendes til ondsindet cyberaktivitet, med henblik på at videreudvikle og fremme EU's fælles holdning til anvendelsen af folkeretten i cyberspace. OPFORDRER i betragtning af, at passende og hurtige budskaber afbøder risikoen for eskalering og kan afskrække angribere, der går efter af europæiske interesser, den højtstående repræsentant til at udvikle og forelægge medlemsstaterne en sammenhængende kommunikationsstrategi for anvendelsen af EU's cyberdiplomatiske værktøjskasse.

26. TILSKYNDER TIL, at der udvikles gradvise, målrettede og vedvarende tilgange til og reaktioner på ondsindede cyberaktiviteter ved at anvende den lange række værktøjer, som EU's cyberdiplomatiske værktøjskasse indeholder, herunder EU's cybersanktionsordning, og ved at overveje yderligere foranstaltninger. UNDERSTREGER behovet for at øge muligheden for fra sag til sag at mobilisere alle tilgængelige interne og eksterne værktøjer for at forebygge, modvirke, afskrække fra og reagere på cyberangreb, idet disse gennemføres med en hurtig, effektiv, gradvis, målrettet og vedvarende tilgang baseret på langsigtet strategisk engagement. OPFORDRER den højtstående repræsentant TIL i samarbejde med Kommissionen at kortlægge mulige fælles EU-reaktioner på cyberangreb, herunder sanktionsmuligheder, i hele spektret for at være klar til at træffe hurtige og effektive foranstaltninger, når det er nødvendigt, og forelægge disse reaktioner for Rådet inden udgangen af første kvartal 2023.

27. TILSKYNDER, idet det bemærker, at cyberforsvar primært er et nationalt ansvar, medlemsstaterne TIL at videreudvikle deres egne kapaciteter til at udføre cyberforsvarsoperationer, herunder proaktive foranstaltninger til at beskytte mod, opspore, forsvare mod og modvirke cyberangreb, og eventuelt til støtte for andre medlemsstater og EU. Hver medlemsstat tilskyndes til om nødvendigt at øge sin egen kapacitet til at yde og modtage hjælp og bistand. UNDERSTREGER, at videreudvikling af disse kapaciteter bør være et af de vigtigste mål for EU's kommende cyberforsvarspolitik. BEMÆRKER, at der i overvejelserne over EU's cyberforsvarspolitik bør lægges mere vægt på, hvilken rolle de relevante EU-institutioner og -organer kan spille for at øge samarbejdet mellem EU's og medlemsstaternes relevante cyberforsvarsaktører og udvikle deres egne kapaciteter i henhold til deres respektive mandater. OPFORDRER den højtstående repræsentant TIL sammen med Kommissionen at supplere udviklingen af en EU-cyberposition ved i 2022 at fremsætte et ambitiøst forslag om en EU-cyberforsvarspolitik, som skal bane vej for Rådets videreudvikling af EU's cyberposition.

28. UNDERSTREGER behovet for at øge interoperabiliteten og informationsudvekslingen gennem samarbejde mellem militære IT-beredskabsenheder. OPFORDRER medlemsstaterne TIL på grundlag af EDA's arbejde at oprette et netværk af militære IT-beredskabsenheder for at udvikle samarbejdet og lette informationsudvekslingen, hvilket også vil bidrage til at fremme koordinering med andre cybersamfund, samt et netværk af militære cyberledere med henblik på at styrke det strategiske samarbejde mellem EU's medlemsstaters cyberkommandoer eller andre tilsvarende myndigheder. Oprettelsen af disse netværk vil sammen med PESCO-projekter på cyberområdet bidrage til et styrket cyberforsvar på EU-plan. Understreger betydningen af samarbejde mellem det foreslåede netværk af militære IT-beredskabsenheder og det allerede eksisterende civile netværk (CSIRT) for at øge informationsudvekslingen og forbedre situationsbevidstheden.

29. GENTAGER på grundlag af "Military Vision and Strategy on Cyberspace as a Domain of Operations" (militær vision og strategi for cyberspace som et operationsområde) og i betragtning af den igangværende udvikling af det militære koncept for cyberforsvar for EU-ledede militære operationer og missioner behovet for at integrere cyberdimensionen i planlægningen og gennemførelsen af FSFP-missioner og -operationer, herunder ved at forbedre deres cyberkapaciteter, og UNDERSTREGER, at dette vil bidrage til øget cybersituationsbevidsthed på EU-plan.

30. BEMÆRKER afslutningsvis, at cyberpositionen vil være et skridt i retning af at fastlægge en EU-doktrin for optræden i cyberspace baseret på øget modstandsdygtighed og bedre kapaciteter og reaktionsmuligheder samt en fælles position om anvendelsen af folkeretten i cyberspace. Rådet VIL GØRE STATUS over de fremskridt, der er gjort med gennemførelsen af disse konklusioner i 2023 for at sikre videreudviklingen af EU's cyberposition.