Rådet for
Den Europæiske Union

Bruxelles, den 22. maj 2023
(OR. en)

9618/23

COPS 269	**JAI 656**
POLMIL 123	**RELEX 639**
CYBER 130	**JAIEX 22**
HYBRID 31	**TELECOM 154**
EUMC 230	**IPCR 38**
CIVCOM 144	**PROCIV 35**
COPEN 162	**COTER 101**
COSI 103	**DISINFO 34**
DATAPROTECT 146	**CSC 252**
IND 256	**CSDP/PSDC 402**
RECH 191	**CFSP/PESC 748**

RESULTAT AF DRØFTELSERNE

fra:	Generalsekretariatet for Rådet
til:	delegationerne
Tidl. dok. nr.:	ST 9124/23 COPS 224 POLMIL 104 CYBER 113 HYBRID 20 EUMC 210 CIVCOM 111 COPEN 138 COSI 86 DATAPROTECT 129 IND 232 RECH 173 JAI 574 RELEX 563 JAIEX 16 TELECOM 135 IPCR 31 PROCIV 25 COTER 86 DISINFO 28 CSC 216 CSDP/PSDC 349 CFSP/PESC 674
Vedr.:	Rådets konklusioner om EU's cyberforsvarspolitik

Vedlagt følger til delegationerne Rådets konklusioner om EU's cyberforsvarspolitik som godkendt af Rådet på samlingen den 22. maj 2023.

Rådets konklusioner om EU's cyberforsvarspolitik

1. På grundlag af rammen for cyberforsvarspolitik fra 2014 og ajourføringen heraf i 2018 ser Rådet med tilfredshed på den ambitiøse fælles meddelelse om EU's cyberforsvarspolitik med henblik på at investere yderligere i vores moderne og interoperable væbnede styrker, banebrydende teknologier og avancerede cyberforsvarskapaciteter og styrke partnerskaber for at tackle fælles udfordringer. Cyberspace er blevet skueplads for et strategisk kapløb i en tid med stigende afhængighed af digitale teknologier. Det er derfor vigtigt at opretholde et åbent, frit, stabilt og sikkert cyberspace. Brugen af cyberoperationer, der har muliggjort og ledsaget Ruslands uprovokerede og uberettigede angrebskrig mod Ukraine, påvirker den globale stabilitet og sikkerhed, udgør en stor risiko for eskalering og øger den allerede betydelige stigning i ondsindede cyberaktiviteter uden for rammerne af de seneste års væbnede konflikter.

2. Krigen i Ukraine har skabt en ny strategisk kontekst og bekræftet behovet for, at EU og dets medlemsstater og deres partnere yderligere styrker EU's modstandsdygtighed over for cybertrusler og øger vores fælles cybersikkerhed og cyberforsvar mod ondsindet adfærd og aggressive handlinger i cyberspace. Den fælles meddelelse om EU's cyberforsvarspolitik signalerer, at vi er fast besluttede på at træffe øjeblikkelige og langsigtede foranstaltninger for at sikre handlefrihed i cyberspace og reaktioner over for trusselsaktører, der bl.a. søger at trænge ind i, forstyrre eller ødelægge EU's og dets partneres net- og informationssystemer. Som supplement til EU's cybersikkerhedsstrategi og i overensstemmelse med det strategiske kompas udgør denne fælles meddelelse et vigtigt skridt i retning af en fuldspektret EU-tilgang til modstandsdygtighed, reaktion, konfliktforebyggelse, samarbejde og stabilitet i cyberspace. I denne forbindelse understreger Rådet behovet for passende og sammenhængende reaktioner fra EU og dets medlemsstater og deres partnere og ser også frem til revisionen af gennemførelsesretningslinjerne for EU's cyberdiplomatiske værktøjskasse som endnu et vigtigt fremskridt inden for udviklingen af EU's cyberposition.

3. Rådet fremhæver, at de nylige cyberangreb på kritisk europæisk infrastruktur, det hurtigt skiftende cybertrusselsbillede og den hastige teknologiske udvikling også viser, at der er behov for øget civil-militær koordinering og øget civil-militært samarbejde, samtidig med at det understreger, at der ikke er noget hierarki mellem det civile og det militære samfund. Med EU's cyberforsvarspolitik kan EU og dets medlemsstater styrke deres evne til at beskytte, opdage, forsvare og afskrække og gøre passende brug af alle de defensive muligheder, der er til rådighed for det civile og det militære samfund, med henblik på bredere sikkerhed i og forsvar af EU i overensstemmelse med folkeretten, herunder menneskerettighedslovgivningen og den humanitære folkeret.

4. Selv om national sikkerhed, herunder på cyberområdet, forbliver den enkelte medlemsstats eneansvar, jf. artikel 4, stk. 2, i TEU, understreger Rådet samtidig behovet for at investere væsentligt, både alene og sammen med andre, i øget modstandsdygtighed og udbredelse af cyberforsvarskapaciteter, der dækker hele spektret, og udnytte EU's samarbejdsrammer og finansielle incitamenter. Rådet fremhæver behovet for yderligere at styrke de tiltag, der iværksættes af medlemsstaterne og EU's institutioner, organer og agenturer med henblik på at beskytte Unionen, vores borgere, EU's institutioner, organer og agenturer samt FSFP-missioner og -operationer i cyberspace. Det understreger endvidere betydningen af EU-modstandsdygtighed i cyberspace ved at udvikle cyberforsvarskapaciteter og styrke samarbejdet med et pålideligt privat økosystem.

I. **Fælles handling med henblik på et stærkere cyberforsvar**

5. Rådet gentager, at en trinvis, gennemsigtig og inklusiv proces er central for at øge tilliden, hvilket er afgørende for videreudvikling af en EU-ramme for håndtering af cybersikkerhedskriser, der skal ske i overensstemmelse med køreplanen for cyberkrisestyring, som er udarbejdet i Rådet. Rådet gentager behovet for at fortsætte med at styrke vores evne til at beskytte, opdage, forsvare og afværge cyberangreb gennem forbedret situationsbevidsthed, kapacitetsopbygning, kapacitetsudvikling, uddannelse, øvelser og øget modstandsdygtighed og ved at reagere beslutsomt på cyberangreb mod EU og dets medlemsstater og EU's institutioner, organer og agenturer samt FSFP-missioner og -operationer med alle passende midler. I denne forbindelse tilskynder Rådet den højtstående repræsentant og Kommissionen til at mindske kompleksiteten på cyberområdet, undgå unødvendigt dobbeltarbejde og sikre samarbejde og synergier med eksisterende initiativer. Samarbejdet og koordineringen skal styrkes mellem cyberforsvarsaktører i og fra EU og medlemsstaterne, mellem militære og civile cybersamfund og mellem offentligheden og et pålideligt privat økosystem. I denne sammenhæng tilskyndes medlemsstaterne til yderligere at undersøge mulighederne for og styrke civil-militære nationale koordineringsmekanismer, lette fælles frivillig udveksling af oplysninger, udveksle erfaringer, bidrage til udvikling af interoperable standarder og foretage risikoevalueringer og opbygning af risikoscenarier samt fælles øvelser, navnlig på europæisk plan, under fuld overholdelse af bestemmelserne i direktivet om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen (NIS 2).

6. Rådet anerkender bestræbelserne på yderligere at øge Unionens modstandsdygtighed med NIS 2 og direktivet om kritiske enheders modstandsdygtighed og gentager sin henstilling om en EU-dækkende koordineret tilgang til styrkelse af kritisk infrastrukturs modstandsdygtighed[1]. Det opfordrer til foranstaltninger, der yderligere øger kritiske enheders, infrastrukturs, digitale produkters og tjenesters modstandsdygtighed, samtidig med at det bemærker, at en korrekt gennemførelse af NIS 2 fortsat er det vigtigste skridt. Selv om det overvejende er et civilt ansvar, bidrager dette også til et stærkere cyberforsvar. I denne forbindelse tilskyndes EU's institutioner, organer og agenturer samt medlemsstaterne til at støtte videreudvikling og anvendelse af nye og eksisterende EU-koordineringsmekanismer, risikovurderinger, evalueringer og scenarier, fælles frivillig informationsudveksling og øvelser på en måde, der skaber merværdi og undgår unødvendig overlapning med eksisterende initiativer.

7. For yderligere at styrke tilliden, konsolidere samarbejdet og lette rettidig udveksling af oplysninger om væsentlige og omfattende cyberhændelser, der påvirker forsvarssystemer, ser Rådet med tilfredshed på initiativet til videreudvikling af EU's konference for cyberøverstbefalende, der skal afholdes af hvert formandskab for EU-Rådet med støtte fra Det Europæiske Forsvarsagentur (EDA) og deltagelse af Tjenesten for EU's Optræden Udadtil (EU-Udenrigstjenesten). Rådet tilskynder alle medlemsstaterne til at deltage i disse møder. For at styrke EU's modstandsdygtighed over for omfattende cybersikkerhedshændelser opfordrer Rådet EU's Netværk af Forbindelsesorganisationer for Cyberkriser (EU-CyCLONe) og EU's konference for cyberøverstbefalende til at identificere mulige samarbejdsmåder og drage fordel af et fælles militært og civilt perspektiv.

---

[1] Forslag til Rådets henstilling om en koordineret tilgang fra Unionens side til styrkelse af kritisk infrastrukturs modstandsdygtighed (COM(2022) 551).

8. For at fremme et mere robust og koordineret beredskab på EU-plan glæder Rådet sig over etableringen af og ser frem til opnåelsen af indledende operationel kapacitet senest medio 2024 i EU's netværk for militære IT-beredskabsenheder (MICNET) for at forbedre udvekslingen mellem de deltagende medlemsstater af tekniske oplysninger om cyberhændelser, der påvirker forsvarssystemer. Rådet tilskynder alle medlemsstater til at deltage i MICNET for at sikre netværkets effektivitet. Desuden opfordrer Rådet medlemsstaterne til at bygge på erfaringerne fra netværket af enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er), og tilskynder kraftigt til at skabe en effektiv samarbejds- og koordineringsmekanisme mellem de to netværk på et passende tidspunkt med fuld respekt for hver enheds forvaltningsmekanismer og brugergrupper.

9. I lyset af forøgelsen af antallet af ondsindede cyberaktiviteter fra statslige og ikkestatslige aktørers side mod EU FSFP-missioner og -operationer opfordrer Rådet EU og dets medlemsstater til at styrke deres kapacitet til at forsvare og sikre FSFP-missioner og -operationer. I denne henseende ser Rådet med tilfredshed på målene om yderligere at fremme beskyttelsen af EU's militære netværk og strukturer i overensstemmelse med bl.a. EU's militære vision og strategi for cyberspace som et operationsområde[2].

[2] EEAS(2021) 706 REV 4.

10. Rådet gentager Rådets konklusioner fra maj 2022[3] og behovet for at investere i vores gensidige bistand i henhold til artikel 42, stk. 7, i TEU samt solidaritetsbestemmelsen i artikel 222 i TEUF. Rådet påpeger betydningen af en yderligere uddybning af EU's og dets medlemsstaters fælles forståelse af gennemførelsen af artikel 42, stk. 7, herunder i komplekse scenarier, der involverer et cyberangreb, i overensstemmelse med de relevante folkeretlige principper. Det glæder sig over muligheden for, at der efter udtrykkelig anmodning fra den eller de berørte medlemsstater kan ydes støtte fra EU, når et cyberangreb udspiller sig, uden at dette berører visse medlemsstaters sikkerheds- og forsvarspolitiks særlige karakter.

11. Rådet understreger de fremskridt, der er gjort i PESCO-projektet cyberberedskabshold og gensidig bistand inden for cybersikkerhed (CRRT'er), og at det er parat til efter anmodning at handle som en kapacitet for medlemsstaternes og EU's behov til støtte for FSFP-missioner og -operationer og til at yde bistand til EU-partnere. Rådet ser med tilfredshed på videreudvikling af PESCO's CRRT-kapacitet, nationale cyberberedskabshold og i givet fald yderligere hændelsesberedskabskapaciteter såsom de fremtidige hybridberedskabshold som planlagt i det strategiske kompas, herunder ved at fremme deres koordinering og samarbejde på EU-plan.

[3] Rådets konklusioner af 23. maj 2022 om udviklingen af Den Europæiske Unions cyberposition (9364/22).

12. Rådet ser med tilfredshed på det arbejde, der udføres af PESCO-projektet koordineringscenter på cyber- og informationsområdet (CIDCC), som har til formål at tilvejebringe en militær kapacitet til at indsamle og analysere oplysninger, der er relevante for et fælles operationelt cyberbillede. Rådet ser endvidere med tilfredshed på forslaget om at integrere "proof of concept", hvis det bliver en succes som informationskoordinationscenter, fra og med 2025 i et EU-koordinationscenter for cyberforsvar (EUCDCC) for at forbedre koordineringen og situationsbevidstheden, navnlig for øverstbefalende for EU FSFP-missioner og -operationer, samt styrke den bredere EU's kommando- og kontrolstruktur. Rådet opfordrer den højtstående repræsentant til at fremlægge et koncept og en køreplan for oprettelse af EUCDCC, der trækker på erfaringer fra lignende internationale enheder, identificerer de nødvendige ressourcer, undgår unødvendigt dobbeltarbejde og søger komplementaritet med EU's bredere ramme for cybersikkerhed.

13. Rådet fremhæver betydningen af strategisk efterretningssamarbejde om cybertrusler og -aktiviteter og opfordrer medlemsstaterne til via deres kompetente myndigheder fortsat at bidrage til arbejdet i EU INTCEN, EUMS' Efterretningsdirektorat og medlemsstaterne inden for rammerne af den fælles efterretningsanalysekapacitet (SIAC). Rådet fremhæver endvidere betydningen af at styrke vores cyberefterretningskapacitet for at forbedre vores cyberrobusthed og -beredskab og yde effektiv støtte til vores civile og militære FSFP-missioner og -operationer samt til vores væbnede styrker og SIAC's kapacitet på cyberområdet på grundlag af frivillige efterretningsbidrag fra medlemsstaterne, og uden at det berører deres kompetencer.

14. Rådet noterer sig Europa-Kommissionens cybersituations- og analysecenter, der har til formål at øge Kommissionens situationsbevidsthed. Rådet fremhæver betydningen af at etablere et gensidigt fordelagtigt samarbejde mellem dette center og andre af EU's institutioner, organer og agenturer, navnlig ENISA og CERT-EU. Rådet understreger betydningen af at sikre et tæt samarbejde med EU's samarbejdsnetværk, når situationsbevidsthed udvikles, og at fortrolighed respekteres. Rådet bemærker behovet for at styrke den fælles situationsbevidsthed på EU-plan og videreudvikle EU's ramme for håndtering af cybersikkerhedskriser, samtidig med at unødvendigt dobbeltarbejde undgås.

15. Rådet minder om, at cyberuddannelse og -øvelser er afgørende for at sikre beredskab og effektivitet, og ser med tilfredshed på de nationale aktiviteter samt de aktiviteter, der udføres af EU gennem Det Europæiske Sikkerheds- og Forsvarsakademi (ESDC), EDA, ENISA og igangværende PESCO-projekter såsom sammenslutninger af cybertestmiljøer og EU's akademia- og innovationsknudepunkt på cyberområdet (CAIH). Med henblik på yderligere at styrke disse bestræbelser ser Rådet frem til oprettelsen af EDA's rammeprojekt CyDef-X for at synkronisere og støtte cyberforsvarsøvelser. Rådet tilskynder EDA til i tæt samarbejde med medlemsstaterne og EU-Udenrigstjenesten at undersøge, hvordan CyDef-X yderligere kan støtte øvelser såsom CYBER PHALANX, herunder om gensidig bistand i henhold til artikel 42, stk. 7, i TEU og solidaritetsbestemmelsen i artikel 222 i TEUF, samt med Kommissionen og ENISA for så vidt angår civile øvelser. Rådet tilskynder desuden til anvendelse og videreudvikling inden for CyDef-X af eksisterende cyberforsvarstestmiljøer og -øvelsesmiljøer, såsom sammenslutninger af cybertestmiljøer. For at sikre en smidig og effektiv beslutningsproces i forbindelse med cyberkriser understreger Rådet betydningen af at afholde regelmæssige skrivebordsøvelser for medlemsstaternes beslutningstagningsniveau.

16. Rådet noterer sig forslaget til retsakt om cybersolidaritet og hensigten om at forbedre kapaciteten til at opdage og reagere på cybersikkerhedstrusler og -hændelser i EU. Rådet understreger, at forslag på dette område kun kan være effektive, hvis de er i overensstemmelse med medlemsstaternes krisestyringsrammer og -behov. Rådet understreger betydningen af at teste kritisk infrastruktur for potentielle sårbarheder, hvor det vurderes at være gavnligt, som en national kompetence under hensyntagen til tilgængelige EU-risikovurderinger.

17. Rådet noterer sig Kommissionens forslag om at oprette en cyberberedskabsmekanisme, som kan støtte tilgængeligheden af cybersikkerhedstjenester fra pålidelige private udbydere til efter anmodning at bistå medlemsstaterne i tilfælde af omfattende cybersikkerhedshændelser, samtidig med at det fremhæver behovet for at opskalere en europæisk cybersikkerhedsindustri med støtte fra Det Europæiske Kompetencecenter for Cybersikkerhed som en væsentlig søjle med henblik på, at denne mekanisme kan blive operationel. Rådet understreger, at hver medlemsstat har en central rolle inden for overvågning og vurdering af deres nationale behov.

II. **Sikring af EU's forsvarsøkosystem**

18. Rådet minder om sin tilskyndelse til medlemsstaterne om at videreudvikle deres egne kapaciteter til at gennemføre cyberforsvarsoperationer, herunder, når det er relevant, proaktive defensive foranstaltninger for at beskytte mod, opdage, forsvare mod og afskrække fra cyberangreb. I betragtning af at NIS 2 ikke finder anvendelse på offentlige forvaltningsenheder, der udfører aktiviteter på forsvarsområdet, opfordrer Rådet EDA til med støtte fra Kommissionen og EU-Udenrigstjenesten, alt efter hvad der er relevant, at bistå medlemsstaterne med at udarbejde ikke juridisk bindende frivillige henstillinger inspireret af NIS 2 for at øge cybersikkerheden i forsvarssektoren og opfordrer alle medlemsstaterne til at engagere sig aktivt i denne indsats. Disse henstillinger bør tage hensyn til lignende bestræbelser inden for andre rammer.

19. Som anerkendt i det strategiske kompas afhænger EU's handleevne af, om det kan mindske sin strategiske afhængighed på tværs af sine cyberforsvarskapaciteter og forsyningskæder og udvikle og beherske banebrydende cyberforsvarsteknologier. Dette omfatter en styrkelse af den europæiske forsvarsteknologiske og -industrielle base (EDTIB) i hele EU og dets evne til at samarbejde med ligesindede partnere i hele verden på et gensidigt grundlag for at sikre gensidige fordele. Rådet opfordrer derfor til, at cybersikkerhedsindustrien og cyberforsvarsindustrien arbejder tæt sammen for at skabe synergier med henblik på at udvikle og levere hele spektret af cyberforsvarskapaciteter. Rådet opfordrer Kommissionen til i tæt samarbejde med Det Europæiske Kompetencecenter for Cybersikkerhed, hvor det er relevant, yderligere at støtte udviklingen af en stærk, smidig, globalt konkurrencedygtig og innovativ industriel og teknologisk base for europæisk cyberforsvar, herunder små og mellemstore virksomheder (SMV'er), gennem yderligere investeringer og politiktiltag.

20. I betragtning af betydningen af interoperabilitet mellem og ensartethed inden for cyberforsvarskapaciteter, herunder hvad angår den samarbejdsbaserede udvikling af næste generation af cyberforsvarskapaciteter, opfordrer Rådet EDA og EU's Militærstab til at arbejde på et sæt EU-krav til cyberforsvarsinteroperabilitet, som vil bygge på og være foreneligt med eksisterende principper, processer og standarder, der navnlig er fastsat inden for rammerne af Den Nordatlantiske Traktats Organisation (NATO). Desuden opfordrer Rådet medlemsstaterne til inden for rammerne af Den Europæiske Standardiseringsorganisation for Forsvar at undersøge, om der kan være behov for specifikke frivillige standarder for forsvarssystemer, i tæt samarbejde med alle relevante interessenter, herunder europæiske standardiseringsorganisationer og NATO, alt efter hvad der er relevant.

21. Rådet udtrykker tilfredshed med Kommissionens bestræbelser på at forelægge en plan for fremme af anvendelsen af eksisterende standarder for anvendelse af civil cybersikkerhed og cyberforsvar samt udviklingen af nye frivillige standarder. Rådet påpeger behovet for at gensidig tilpasning af standarderne for cybersikkerhed og cyberforsvar, hvor det er relevant. Rådet anerkender, at sådanne frivillige standarder kan være nyttige for EU's cybersikkerheds- og cyberforsvarsindustri, og opfordrer indtrængende til et tættere samarbejde mellem civile og forsvarsrelaterede standardiseringsorganer.

22. Rådet opfordrer til hurtig udarbejdelse af henstillinger baseret på en kortlægning af eksisterende værktøjer til sikker kommunikation på cyberområdet, som Kommissionen og relevante institutioner foretager. Hvor det er muligt, bør henstillingerne tilpasses eksisterende initiativer vedrørende informationsudveksling og bør også tage hensyn til de risici, som nye og disruptive teknologier udgør for de nuværende krypteringsmetoder.

23. Desuden ser Rådet med tilfredshed på det indledende arbejde med risikoevaluering og -scenarier, der er ved at blive udført af Kommissionen, den højtstående repræsentant og NIS-samarbejdsgruppen vedrørende i første omgang energi- og telekommunikationssektorerne efter anmodning fra Rådet. Rådet anerkender, at der også er ved at blive udarbejdet målrettede cybersikkerhedsrisikovurderinger for kommunikationsinfrastruktur og -net i EU. Rådet gentager, at det er af allerstørste betydning at have en fælles forståelse mellem medlemsstaterne, men også mellem EU's institutioner, organer og agenturer, af cyberhændelsers mulige virkninger. Rådet opfordrer derfor ovennævnte aktører til at sikre, at der tages hensyn til risikoevalueringer, scenarier og efterfølgende henstillinger, når der fastlægges og prioriteres foranstaltninger og støtte på EU-plan og, hvor det er relevant, på nationalt plan. Rådet opfordrer endvidere alle relevante aktører til at overveje risikoscenarierne i risikovurderingsprocesser og i forbindelse med udvikling af cyberøvelser.

III. **Investering i cyberforsvarskapacitet**

24. Rådet tilskynder medlemsstaterne til at øge deres investeringer i opbygning, opretholdelse og videreudvikling af interoperable cyberforsvarskapaciteter. Rådet støtter udarbejdelse af et sæt frivillige tilsagn om videreudvikling af nationale cyberforsvarskapaciteter under hensyntagen til lignende bestræbelser inden for andre rammer.

25. Rådet opfordrer medlemsstaterne og EDA til at benytte lejligheden i forbindelse med revisionen af kapacitetsudviklingsplanen til at fastsætte et højt ambitionsniveau for udvikling af et samarbejdsbaseret cyberforsvar på EU-plan. Rådet tilskynder endvidere medlemsstaterne til at bygge på det ajourførte sæt prioriteter og deres PESCO-tilsagn om at øge deres engagement i samarbejdsbaserede EU-projekter vedrørende udvikling af cyberforsvarskapacitet og anerkender den direkte fordel ved samarbejdsprojekter på EU-plan til støtte for udvikling af nationale cyberforsvarskapaciteter.

26. Rådet ser med tilfredshed på den fælles forskning på EU-plan, der skal undersøge mulige anvendelser i forsvarsrelaterede systemer af nye og disruptive teknologier, og bemærker også behovet for at sikre, at denne teknologiske udvikling hurtigt indarbejdes i eksisterende og fremtidige kapaciteter. Rådet tilskynder medlemsstaterne og EU's industri til at gøre bedst mulig brug af forskningssamarbejdsmuligheder på EU-plan, f.eks. inden for EDA-rammen og i igangværende PESCO-projekter såsom EU's akademia- og innovationsknudepunkt på cyberområdet (CAIH), Den Europæiske Forsvarsfond og, hvor det er relevant, Horisont Europa og programmet for et digitalt Europa for projekter med dobbelt anvendelse. Desuden ser Rådet med tilfredshed på udnyttelsen af de særlige rammer til støtte for forsvarsinnovation ved hjælp af "spin-ins" fra det civile område, navnlig EU-ordningen for forsvarsinnovation og knudepunktet for europæisk forsvarsinnovation. Rådet tilskynder derudover Det Europæiske Kompetencecenter for Cybersikkerhed og EDA til at udvikle en samarbejdsordning for at lette udvekslingen af oplysninger mellem de respektive medarbejdere om henholdsvis civile prioriteter og prioriteter vedrørende dobbelt anvendelse og forsvarsteknologi med henblik på at skabe synergier og undgå overlapning.

27. Rådet glæder sig over Kommissionens hensigt om at udarbejde en teknologikøreplan for kritiske cyberteknologier i samarbejde med EDA og Det Europæiske Kompetencecenter for Cybersikkerhed i overensstemmelse med deres respektive mandater, med medlemsstaterne og i samråd med relevante interessenter såsom industrien, som ved at identificere kritiske cyberteknologier og kortlægge den teknologiske udvikling og strategiske afhængighedsforhold giver mulighed for at reducere disse til støtte for EU's strategiske autonomi og teknologiske suverænitet og samtidig bevare en åben økonomi. Rådet bemærker, at teknologikøreplanen for kritiske cyberteknologier kan danne grundlag for strategiske prioriteter for EU's finansieringsinstrumenter og samtidig være i overensstemmelse med de respektive nærmere bestemmelser herom. Rådet minder om, at EU bør føre en ambitiøs og assertiv europæisk industripolitik for at skabe et bæredygtigt, attraktivt og konkurrencedygtigt erhvervsklima, som også kan muliggøre, at europæiske enheder på cyberområdet kan opskalere.

28. Rådet værdsætter hensigten om at afhjælpe den betydelige mangel på cybersikkerhedsfærdigheder ved at tiltrække nye fagfolk, herunder kvinder, opkvalificere og omskole samt investere i og tilrettelægge uddannelse og øvelser med henblik på at opbygge en mangfoldig og inklusiv cyberarbejdsstyrke. Rådet anerkender de udfordringer, som EU står over for med hensyn til menneskelig kapital inden for cybersikkerhed og cyberforsvar, og ser med tilfredshed på initiativet vedrørende et akademi for cyberfærdigheder, som også kan være til gavn for arbejdsstyrken inden for cyberforsvar.

29. Rådet opfordrer medlemsstaterne til at udveksle oplysninger om bedste praksis for udvikling af kvalificerede cybersikkerhedsfagfolk, der udnytter synergierne mellem militære, civile og retshåndhævende initiativer, og opfordrer ESDC til med støtte og ekspertise fra EDA og ENISA at overveje mulighederne for at forbedre udvekslingen af bedste praksis og yderligere synergier mellem det militære og civile område med hensyn til uddannelse og udvikling af cyberspecifikke forsvarsfærdigheder.

30. Rådet understreger betydningen af en fælles forståelse af sammensætningen af arbejdsstyrken inden for cybersikkerhed og af tilknyttede færdigheder med henblik på at identificere og afhjælpe manglerne på arbejdsmarkedet for cybersikkerhed samt behovet for at inddrage alle interessenter, herunder medlemsstaterne og industrien. Rådet anerkender, at fastlæggelse af indikatorer for overvågning af arbejdsmarkedet for cybersikkerhed vil hjælpe med at identificere behovene for cybersikkerhedsfærdigheder og kanalisere midler i tilstrækkeligt omfang og samtidig bidrage til at opfylde politikrelaterede forpligtelser, navnlig dem, der følger af NIS 2. Rådet hilser forslaget om en ramme for certificering af cyberforsvarsfærdigheder velkommen og opfordrer den højtstående repræsentant til som ESDC-chef at udvikle dette i samarbejde med EU-Udenrigstjenesten, Kommissionen og medlemsstaterne ved at udnytte civile initiativer.

IV. **Partnerskaber for at tackle fælles udfordringer**

31. Rådet opfordrer den højtstående repræsentant og Kommissionen til at styrke og fremme deres samarbejde og undersøge mulighederne for gensidigt fordelagtige og skræddersyede partnerskaber om cyberforsvarspolitikker, herunder om opbygning af cyberforsvarskapacitet gennem den europæiske fredsfacilitet (EPF). Med henblik herpå bør cyberforsvar tilføjes som et punkt i EU's cyberdialoger og -konsultationer og i de overordnede sikkerheds- og forsvarskonsultationer med partnere. Desuden bør dialogen og samarbejdet med den private sektor styrkes. Rådet understreger, at internationalt samarbejde om cybersikkerhedsstandarder og -certificering vil være en merværdi for den europæiske industri. Det glæder sig derfor over Kommissionens tilsagn om at gøre dette til en væsentlig del af EU's cyberdialoger med tredjelande og internationale organisationer.

32. Rådet påpeger betydningen af internationalt samarbejde for at forebygge eller mindske risikoen for konflikter i cyberspace, navnlig gennem videreudvikling og operationalisering af tillidsskabende foranstaltninger på regionalt og internationalt niveau, herunder i FN, og yderligere tilskynde til brug af eksisterende tillidsskabende cyberforanstaltninger som i Organisationen for Sikkerhed og Samarbejde i Europa (OSCE), herunder i tider med internationale spændinger.
EU og dets medlemsstater fremhæver, at den eksisterende folkeret finder anvendelse i cyberspace, og understreger betydningen af fortsatte bestræbelser på at opretholde og fremme FN's ramme for ansvarlig statslig adfærd og arbejde hen imod dens gennemførelse, herunder gennem udarbejdelse af et handlingsprogram for fremme af ansvarlig statslig adfærd i cyberspace.

33. I overensstemmelse med de fælles erklæringer om samarbejdet mellem EU og NATO opfordrer Rådet den højtstående repræsentant, også som leder af EDA, og Kommissionen til yderligere at styrke, uddybe og udvide partnerskabet inden for cyberområdet med NATO med fuld respekt for principperne om inklusivitet, gensidighed, gensidig åbenhed og gennemsigtighed samt beslutningsautonomi for begge organisationer. Under hensyntagen til behovet for at sikre en supplerende og koordineret indsats med størst mulig inddragelse af medlemsstater, der ikke er NATO-medlemmer, og undgå unødvendige overlapninger opfordrer Rådet til, at der etableres forbindelser på relevante niveauer mellem EU og NATO om uddannelse, situationsbevidsthed, øvelser og FoU-platforme, og til at søge potentielle synergier mellem de respektive frivillige tilsagn om udvikling af nationale cyberforsvarskapaciteter og krisestyringsrammerne, beskyttelse af kritisk infrastruktur og øget udveksling af situationsbevidsthed, koordinerede reaktioner på ondsindede cyberaktiviteter samt kapacitetsopbygningsbestræbelser i tredjelande. Dette omfatter den tekniske ordning mellem NATO Computer Incident Response Capability (NCIRC) og EU's IT-Beredskabsenhed (CERT-EU) samt en styrket politisk dialog om cyberforsvarsspørgsmål på alle niveauer.

V. **Konklusion**

34. På grundlag af Rådets konklusioner om EU's cyberforsvarspolitik opfordrer Rådet den højtstående repræsentant og Kommissionen til at udarbejde en plan for politikkens gennemførelse senest i andet kvartal af 2023 med henblik på medlemsstaternes godkendelse. Rådet opfordrer også medlemsstaterne til frivilligt at tilkendegive deres ambitioner og tiltag med hensyn til cyberforsvar inden for rammerne af EU's cyberforsvarspolitik og gøre fuld brug af ikke juridisk bindende frivillige henstillinger og tilsagn for at intensivere deres nationale og multinationale cyberforsvarsindsats med henblik på at maksimere indvirkningen på EU-niveau. Den højtstående repræsentant, Kommissionen og medlemsstaterne opfordres til fra andet kvartal af 2024 hvert år at aflægge rapport og drøfte fremskridtene med gennemførelsen af elementerne i den fælles meddelelse og dens gennemførelsesplan.