Europeiska unionens råd

Bryssel 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

LÄGESRAPPORT

från:	Rådets generalsekretariat
till:	Delegationerna
Föreg. 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
Ärende:	Rådets slutsatser om EU:s politik för cyberförsvar

För delegationerna bifogas rådets slutsatser om EU:s politik för cyberförsvar, som godkändes av rådet vid mötet den 22 maj 2023.

Rådets slutsatser om EU:s politik för cyberförsvar

1. Med utgångspunkt i 2014 års ram för EU:s politik för it-försvar och dess uppdatering från 2018 välkomnar rådet det ambitiösa gemensamma meddelandet om EU:s politik för cyberförsvar som syftar till att investera ytterligare i våra moderna och interoperabla väpnade styrkor, spetsteknologi och avancerad cyberförsvarsförmåga samt stärka partnerskap för att ta itu med gemensamma utmaningar. Cyberrymden har blivit ett område för strategisk konkurrens i en tid av ökande beroende av digital teknik. Det är därför nödvändigt att upprätthålla en öppen, fri, stabil och säker cyberrymd. Användning av cyberinsatser har möjliggjort och åtföljt Rysslands oprovocerade och oberättigade anfallskrig mot Ukraina, vilket påverkar den globala stabiliteten och säkerheten, utgör en betydande risk för upptrappning och bidrar till den redan betydande ökningen av skadlig cyberverksamhet utanför väpnade konflikter under de senaste åren.

2. Kriget i Ukraina har skapat ett nytt strategiskt sammanhang och har bekräftat att EU, dess medlemsstater och deras partner ytterligare behöver stärka EU:s resiliens mot cyberhot och höja EU:s gemensamma cybersäkerhet och cyberförsvar mot skadligt beteende och aggressionshandlingar i cyberrymden. Det gemensamma meddelandet om EU:s politik för cyberförsvar ger uttryck för vår beslutsamhet att vidta omedelbara och långsiktiga åtgärder för att säkerställa handlingsfrihet i cyberrymden och genomföra insatser mot fientliga aktörer som, bland annat, försöker ta sig in i, störa eller förstöra EU:s och dess partners nätverks- och informationssystem. Som ett komplement till EU:s strategi för cybersäkerhet och i linje med den strategiska kompassen utgör det gemensamma meddelandet ett viktigt steg mot EU:s heltäckande strategi för resiliens, insatser, konfliktförebyggande, samarbete och stabilitet i cyberrymden. I detta sammanhang understryker rådet behovet av lämpliga och samstämmiga insatser från EU, dess medlemsstater och deras partner, och ser också fram emot översynen av riktlinjerna för genomförandet av EU:s verktygslåda för cyberdiplomati som ytterligare ett viktigt steg framåt i utvecklingen av EU:s arbete på cyberområdet.

3. Rådet betonar att den senaste tidens cyberattacker mot europeisk kritisk infrastruktur, den snabbt föränderliga cyberhotbilden och den snabba tekniska utvecklingen också visar på behovet av ökad civil-militär samordning och samverkan, samtidigt som det understryks att det inte finns någon hierarki mellan det civila och det militära.
EU:s politik för cyberförsvar gör det möjligt för EU och dess medlemsstater att stärka sin förmåga att skydda, upptäcka, försvara sig och avskräcka, genom att på lämpligt sätt använda alla de defensiva alternativ som det civila och det militära har till sitt förfogande för EU:s bredare säkerhet och försvar, i enlighet med internationell rätt, inbegripet människorättslagstiftning och internationell humanitär rätt.

4. Även om den nationella säkerheten, inbegripet på cyberområdet, också i fortsättningen ska vara varje medlemsstats eget ansvar, såsom anges i artikel 4.2 i EU-fördraget, betonar rådet samtidigt behovet av att både enskilt och gemensamt göra betydande investeringar i ökad resiliens och användning av heltäckande defensiv cyberförsvarsförmåga och att utnyttja EU:s samarbetsramar och ekonomiska incitament. Rådet betonar behovet av att ytterligare stärka de åtgärder som vidtas av medlemsstaterna och av EU:s institutioner, organ och byråer för att skydda unionen, våra medborgare, EU:s institutioner, organ och byråer samt GSFP-uppdrag och GSFP-insatser i cyberrymden. Rådet understryker vidare vikten av förstärka EU:s resiliens i cyberrymden genom att utveckla cyberförsvarsförmåga och förbättra samarbetet med ett betrott privat ekosystem.

I. **Gemensamma åtgärder för ett starkare cyberförsvar**

5. Rådet upprepar att en stegvis, transparent och inkluderande process är mycket viktig för att öka förtroendet, vilket är avgörande för den vidare utvecklingen av en EU-ram för hantering av cyberkriser, som ska ske i linje med den färdplan för hantering av cyberkriser som rådet har utarbetat. Rådet upprepar att vi behöver fortsätta att öka vår förmåga att skydda, upptäcka, försvara sig mot och avskräcka från cyberattacker med hjälp av förbättrad lägesuppfattning, kapacitetsuppbyggnad, förmågeutveckling, utbildning, övningar och ökad motståndskraft, och genom att med alla lämpliga medel reagera med kraft på cyberattacker mot EU, dess medlemsstater, EU:s institutioner, organ och byråer samt GSFP-uppdrag och GSFP-insatser. Därvid uppmanar rådet den höga representanten och kommissionen att minska komplexiteten på cyberområdet, undvika onödigt dubbelarbete och säkerställa samarbete och synergier med befintliga initiativ. Samarbetet och samordningen behöver stärkas mellan aktörer på cyberförsvarsområdet i EU och medlemsstaterna, mellan militära och civila cybergrupper och mellan allmänheten och ett betrott privat ekosystem. Medlemsstaterna uppmanas i detta sammanhang att ytterligare utforska och stärka de civil-militära nationella samordningsmekanismerna, underlätta gemensamt frivilligt informationsutbyte, utbyta tillvaratagna erfarenheter, bidra till utvecklingen av interoperabla standarder och utarbeta riskbedömningar och riskscenarier, samt genomföra gemensamma övningar, särskilt på europeisk nivå, med full respekt för bestämmelserna i direktivet om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS 2-direktivet).

6. Rådet erkänner insatserna för att ytterligare stärka unionens motståndskraft genom NIS 2-direktivet och direktivet om kritiska entiteters motståndskraft (CER-direktivet), och upprepar sin rekommendation om en EU-omfattande samordnad strategi för att stärka den kritiska infrastrukturens motståndskraft[1]. Det efterlyser åtgärder för att ytterligare stärka motståndskraften hos kritiska entiteter, infrastruktur samt digitala produkter och tjänster, men noterar samtidigt att ett korrekt genomförande av NIS 2-direktivet fortfarande är det viktigaste steget. Även om detta främst är ett civilt ansvar bidrar det också till ett starkare cyberförsvar. I detta sammanhang uppmanas EU:s institutioner, organ och byråer samt medlemsstaterna att stödja vidareutveckling och användning av nya och befintliga samordningsmekanismer på EU-nivå samt riskbedömningar, utvärderingar och scenarier, gemensamt frivilligt informationsutbyte och övningar, på ett sätt som tillför ett mervärde och undviker onödig överlappning med befintliga initiativ.

7. För att ytterligare stärka förtroendet, konsolidera samarbetet och underlätta snabbt informationsutbyte om betydande och storskaliga cyberincidenter som påverkar försvarssystem välkomnar rådet initiativet att vidareutveckla konferensen för EU:s cyberbefälhavare, som ska anordnas av varje ordförandeskap i Europeiska unionens råd, med stöd av Europeiska försvarsbyrån (EDA) och med deltagande av Europeiska utrikestjänsten. Rådet uppmanar alla medlemsstater att delta i dessa möten. I syfte att stärka EU:s motståndskraft mot storskaliga cybersäkerhetsincidenter uppmanar rådet Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe) och konferensen för EU:s cyberbefälhavare att identifiera möjliga sätt att samarbeta och dra nytta av ett gemensamt militärt och civilt perspektiv.

[1] Förslag till rådets rekommendation om en samordnad strategi från unionens sida för att stärka den kritiska infrastrukturens motståndskraft, COM(2022) 551 final.

8. För att främja kraftfullare och mer samordnade insatser på EU-nivå välkomnar rådet inrättandet av EU:s nätverk för militära it-incidenthanteringsorganisationer (Micnet) för att förbättra det tekniska informationsutbytet mellan de deltagande medlemsstaterna om cyberincidenter som påverkar försvarssystemen, och ser fram emot att nätverket ska uppnå sin initiala operativa förmåga senast i mitten av 2024. Rådet uppmanar alla medlemsstater att delta i Micnet för att säkerställa att nätverket är ändamålsenligt. Rådet uppmanar dessutom medlemsstaterna att bygga vidare på erfarenheterna från nätverket för enheter för hantering av it-säkerhetsincidenter (CSIRT-nätverket) och uppmanar med kraft till att det skapas en effektiv mekanism för samarbete och samordning mellan de två nätverken vid en lämplig tidpunkt, med full respekt för varje enhets styrningsmekanismer och upptagningsområde.

9. Mot bakgrund av ökningen av skadlig cyberverksamhet från statliga och icke-statliga aktörer mot EU:s GSFP-uppdrag och GSFP-insatser, uppmanar rådet EU och dess medlemsstater att stärka sin förmåga att försvara och säkra GSFP-uppdrag och GSFP-insatser. I detta avseende välkomnar rådet målen att ytterligare stärka skyddet av EU:s militära nätverk och strukturer, i linje med bland annat EU:s militära vision och strategi för cyberrymden som operativt område[2].

[2] EEAS(2021) 706 REV4.

10. Rådet erinrar om sina slutsatser från maj 2022[3] och behovet av att investera i ömsesidigt bistånd i enlighet med artikel 42.7 i EU-fördraget och solidaritetsklausulen i artikel 222 i EUF-fördraget. Rådet betonar vikten av att ytterligare fördjupa EU:s och dess medlemsstaters samförstånd i fråga om genomförandet av artikel 42.7, däribland i komplexa scenarier som inbegriper en cyberattack, i överensstämmelse med relevanta principer i internationell rätt. Det välkomnar möjligheten till stöd från EU vid en cyberattack, på uttrycklig begäran av den eller de berörda medlemsstaterna, utan att det påverkar den särskilda karaktären hos vissa medlemsstaters säkerhets- och försvarspolitik.

11. Rådet understryker de framsteg som gjorts i Pesco-projektet för snabbinsatsteam och ömsesidigt bistånd på området för cybersäkerhet (CRRT) och framhåller att det är redo att på begäran agera för att svara mot medlemsstaternas och EU:s behov, till stöd för GSFP-uppdrag och GSFP-insatser och för att bistå EU:s partner. Rådet välkomnar den fortsatta utvecklingen av kapaciteten hos Pesco-projektet CRRT, nationella insatsteam på området för cybersäkerhet och, i tillämpliga fall, ytterligare incidenthanteringskapacitet, såsom de framtida snabbinsatsteam för hybridhot som planeras i den strategiska kompassen, inbegripet genom att främja deras samordning och samarbete på EU-nivå.

[3] Rådets slutsatser om utvecklingen av Europeiska unionens arbete på cyberområdet av den 23 maj 2022, dok. 9364/22.

12. Rådet välkomnar det arbete som utförts av Pesco-projektet Samordningscentrum för cyber- och informationsområdet (CIDCC), som syftar till att tillhandahålla militär förmåga att samla in och analysera information som är relevant för en gemensam operativ cyberbild. Rådet välkomnar dessutom förslaget att från och med 2025 integrera koncepttestet, om centrumet visar sig vara framgångsrikt som ett samordningscentrum på informationsområdet, i ett EU:s samordningscentrum för cyberförsvar (EUCDCC), för att förbättra samordningen och lägesuppfattningen, särskilt när det gäller befälhavare för EU:s GSFP-uppdrag och GSFP-insatser samt förstärkning av EU:s bredare lednings- och kontrollstruktur. Rådet uppmanar den höga representanten att lägga fram ett koncept och en färdplan för inrättandet av EUCDCC, där man drar lärdom av liknande internationella enheter, identifierar de resurser som krävs, undviker onödigt dubbelarbete och söker komplementaritet med EU:s bredare ram för cybersäkerhet.

13. Rådet framhåller vikten av strategiskt underrättelsesamarbete om cyberhot och cyberverksamhet och uppmanar medlemsstaterna att genom sina behöriga myndigheter fortsätta att bidra till det arbete som utförs inom EU Intcen och EUMS underrättelsedirektorat och i medlemsstaterna inom ramen för den gemensamma kapaciteten för underrättelseanalys (SIAC). Rådet framhåller vidare att det är viktigt att vi stärker vår förmåga vad avser underrättelser om cyberhot i syfte att öka vår cyberresiliens och våra insatser på cyberområdet, och effektivt stödja våra civila och militära GSFP-uppdrag och GSFP-insatser samt våra väpnade styrkor och kapaciteten inom SIAC på cyberområdet, på grundval av frivilliga underrättelsebidrag från medlemsstaterna och utan att det påverkar deras befogenheter.

14. Rådet noterar Europeiska kommissionens läges- och analyscentrum på cyberområdet som syftar till att förbättra kommissionens lägesuppfattning. Rådet betonar vikten av att upprätta ett ömsesidigt gynnsamt samarbete mellan detta centrum och andra EU-organ, särskilt Europeiska unionens cybersäkerhetsbyrå (Enisa) och cybersäkerhetscentrumet för unionens institutioner, organ och byråer (CERT-EU). Rådet understryker vikten av att säkerställa ett nära samarbete med EU:s samarbetsnätverk vid utveckling av lägesuppfattning, och av att iaktta konfidentialitet. Rådet noterar behovet av att stärka den gemensamma lägesuppfattningen på EU-nivå och vidareutveckla EU-ramen för hantering av cyberkriser, samtidigt som onödigt dubbelarbete undviks.

15. Rådet erinrar om att utbildning och övningar på cyberområdet är avgörande för att säkerställa beredskap och ändamålsenlighet och välkomnar såväl nationell verksamhet som verksamhet som tillhandahålls av EU genom Europeiska säkerhets- och försvarsakademin (Esfa), Europeiska försvarsbyrån, Enisa och pågående Pesco-projekt, såsom Sammanslutningar av cyberranger och EU:s cyberakademi och innovationsknutpunkt (EU CAIH). I syfte att ytterligare stärka dessa insatser ser rådet fram emot inrättandet av Europeiska försvarsbyråns ramprojekt CyDef-X för att synkronisera och stödja cyberförsvarsövningar. Rådet uppmanar Europeiska försvarsbyrån att i nära samarbete med medlemsstaterna och utrikestjänsten undersöka hur CyDef-X ytterligare skulle kunna stödja övningar såsom Cyber Phalanx, bland annat i fråga om ömsesidigt bistånd enligt artikel 42.7 i EU-fördraget och solidaritetsklausulen i artikel 222 i EUF-fördraget, samt i samarbete med kommissionen och Enisa när det gäller civila övningar. Rådet uppmuntrar dessutom till användning och vidareutveckling inom CyDef-X av befintliga test- och övningsmiljöer för cyberförsvar, t.ex. genom projektet Sammanslutningar av cyberranger. För att säkerställa en smidig och effektiv beslutsprocess vid cyberkriser understryker rådet vikten av att hålla regelbundna skrivbordsövningar på beslutsfattande nivå i medlemsstaterna.

16. Rådet noterar förslaget till en cybersolidaritetsakt och avsikten att förbättra förmågan att upptäcka och reagera på cybersäkerhetshot och cyberincidenter i EU. Rådet understryker att förslag på detta område endast kan vara effektiva om de anpassas till medlemsstaternas ramar och behov för krishantering. Rådet understryker också att det är viktigt att, när detta bedöms vara till nytta, kritisk infrastruktur testas för potentiella sårbarheter, som en nationell behörighet och med beaktande av tillgängliga riskbedömningar på EU-nivå.

17. Rådet noterar kommissionens förslag om att inrätta en mekanism för cyberkriser, som skulle kunna stödja tillgången till cybersäkerhetstjänster från betrodda privata leverantörer som på begäran kan bistå medlemsstaterna vid storskaliga cybersäkerhetsincidenter, och understryker samtidigt behovet av att med stöd av Europeiska kompetenscentrumet för cybersäkerhet (ECCC) skala upp den europeiska cybersäkerhetsbranschen, som är avgörande för att denna mekanism ska kunna tas i drift. Rådet understryker varje medlemsstats centrala roll i övervakningen och bedömningen av sina nationella behov.

II. **Förstärkt säkerhet i EU:s försvarsekosystem**

18. Rådet erinrar om sin uppmaning till medlemsstaterna att vidareutveckla sin egen förmåga att genomföra cyberförsvarsinsatser, inbegripet proaktiva åtgärder för att skydda, upptäcka, försvara sig mot och avskräcka från cyberattacker. Med tanke på att NIS 2-direktivet inte är tillämpligt på offentliga förvaltningsenheter som bedriver verksamhet på försvarsområdet uppmanar rådet Europeiska försvarsbyrån att, vid behov med stöd av kommissionen och utrikestjänsten, bistå medlemsstaterna med att utarbeta icke rättsligt bindande, frivilliga rekommendationer på grundval av NIS 2-direktivet för att öka cybersäkerheten i försvarsgemenskapen, och uppmanar alla medlemsstater att aktivt engagera sig i detta arbete. Dessa rekommendationer bör ta hänsyn till liknande insatser som görs inom andra ramar.

19. Såsom framgår av den strategiska kompassen är EU:s kapacitet att agera beroende av dess förmåga att minska sitt strategiska beroende i fråga om cyberförsvarsförmåga och i leveranskedjorna samt att utveckla och behärska avancerad teknik på området för cyberförsvar. Detta inbegriper att förstärka den europeiska försvarstekniska och försvarsindustriella basen i hela EU och dess förmåga att samarbeta med likasinnade partner runt om i världen, på ömsesidig grund för att säkerställa ömsesidiga fördelar. Rådet uppmanar därför cybersäkerhets- och cyberförsvarsindustrin att samarbeta nära för att skapa synergier i syfte att utveckla och tillhandahålla en heltäckande cyberförsvarsförmåga. Rådet uppmanar kommissionen att, när så är lämpligt i nära samarbete med ECCC, ytterligare stödja utvecklingen av en stark, flexibel, globalt konkurrenskraftig och innovativ europeisk industriell och teknisk bas för cyberförsvar, som inbegriper små och medelstora företag, genom ytterligare investeringar och genom politiska åtgärder.

20. Med tanke på att det är viktigt att cyberförsvarsförmåga är interoperabel och enhetlig, även när det gäller den samarbetsinriktade utvecklingen av nästa generations cyberförsvarsförmåga, uppmanar rådet Europeiska försvarsbyrån och EU:s militära stab att utarbeta en uppsättning EU-krav på interoperabilitet på cyberförsvarsområdet, som skulle bygga på och vara förenliga med befintliga principer, processer och standarder som fastställts särskilt inom ramen för Nordatlantiska fördragsorganisationen (Nato). Vidare uppmanar rådet medlemsstaterna att inom ramen för den europeiska kommittén för försvarsstandardisering undersöka om specifika frivilliga standarder för försvarssystem kan vara nödvändiga, och att göra detta i nära samarbete med alla berörda parter, inbegripet europeiska standardiseringsorganisationer och Nato, beroende på vad som är lämpligt.

21. Rådet välkomnar kommissionens arbete med att lägga fram en plan för att främja användningen av befintliga standarder för civil användning av cybersäkerhet och cyberförsvar samt utvecklingen av nya frivilliga standarder. Rådet betonar att standarderna för cybersäkerhet och cyberförsvar vid behov måste anpassas till varandra. Rådet inser att sådana frivilliga standarder skulle kunna vara användbara för EU:s cybersäkerhets- och cyberförsvarsindustri och efterlyser ett närmare samarbete mellan civila standardiseringsorgan och standardiseringsorgan på försvarsområdet.

22. Rådet uppmanar till ett skyndsamt utarbetande av rekommendationer på grundval av en kartläggning av befintliga verktyg för säker kommunikation på cyberområdet som utförs av kommissionen och relevanta institutioner. När så är möjligt bör rekommendationerna anpassas till befintliga initiativ om informationsutbyte och även beakta de risker som ny och disruptiv teknik innebär för de nuvarande krypteringsmetoderna.

23. Rådet välkomnar dessutom det inledande arbetet med de riskbedömningar och riskscenarier för, inledningsvis, energi- och telekommunikationssektorerna som kommissionen, den höga representanten och samarbetsgruppen för nät- och informationssäkerhet håller på att utarbeta på rådets begäran. Rådet är medvetet om att riktade riskbedömningar av cybersäkerheten för kommunikationsinfrastruktur och kommunikationsnät i EU också håller på att utarbetas. Rådet upprepar att det är av yttersta vikt att medlemsstaterna, och även EU:s institutioner, organ och byråer, har en samsyn om möjliga konsekvenser av cyberincidenter. Det uppmanar därför de ovannämnda aktörerna att se till att riskbedömningar, riskscenarier och efterföljande rekommendationer beaktas när åtgärder och stöd fastställs och prioriteras, på såväl EU-nivå som, i förekommande fall, nationell nivå. Rådet uppmanar vidare alla relevanta aktörer att beakta riskscenarierna i riskbedömningsprocesser och vid utvecklingen av cyberövningar.

III. **Investeringar i cyberförsvarsförmåga**

24. Rådet uppmanar medlemsstaterna att öka sina investeringar för att bygga upp, upprätthålla och vidareutveckla interoperabel cyberförsvarsförmåga. Rådet stöder utvecklingen av en uppsättning frivilliga åtaganden för vidareutvecklingen av nationell cyberförsvarsförmåga, med beaktande av liknande insatser som gjorts inom andra ramar.

25. Rådet uppmanar medlemsstaterna och Europeiska försvarsbyrån att ta tillfället i akt att i samband med översynen av förmågeutvecklingsplanen fastställa en hög ambitionsnivå när det gäller utvecklingen av ett samarbetsinriktat cyberförsvar på EU-nivå. Rådet uppmanar vidare medlemsstaterna att bygga vidare på den uppdaterade uppsättningen prioriteringar och på sina åtaganden inom ramen för Pesco för att öka sitt engagemang i samarbetsinriktade EU-projekt för utveckling av cyberförsvarsförmåga, och erkänner den direkta nyttan av samarbetsprojekt på EU-nivå för att stödja utvecklingen av nationell cyberförsvarsförmåga.

26. Rådet välkomnar forskningssamverkan på EU-nivå för att undersöka möjliga tillämpningar av ny och disruptiv teknik i försvarsrelaterade system, och noterar även behovet av att säkerställa att denna tekniska utveckling snabbt införlivas i befintlig och framtida förmåga. Rådet uppmanar medlemsstaterna och EU:s industri att på bästa sätt utnyttja möjligheterna till forskningssamverkan på EU-nivå, till exempel inom ramen för Europeiska försvarsbyrån och pågående Pesco-projekt, såsom EU:s cyberakademi och innovationsknutpunkt (EU CAIH), liksom inom ramen för Europeiska försvarsfonden och, i förekommande fall, Horisont Europa och programmet för ett digitalt Europa för projekt med dubbla användningsområden. Rådet välkomnar dessutom att man utnyttjar de särskilda ramarna för att stödja försvarsinnovation med hjälp av spinin-effekter från det civila området, särskilt EU:s system för försvarsinnovation och knutpunkten för försvarsinnovation. Vidare uppmanar rådet ECCC och Europeiska försvarsbyrån att utveckla ett samarbetsavtal för att underlätta informationsutbyte mellan deras respektive personal om civila och dubbla användningsområden och försvarstekniska prioriteringar, i syfte att skapa synergier och undvika dubbelarbete.

27. Rådet välkomnar kommissionens avsikt att i samarbete med Europeiska försvarsbyrån och ECCC, i linje med deras respektive mandat, och med medlemsstaterna och i samråd med berörda parter, såsom industrin, utarbeta en färdplan för kritisk cyberteknik, som genom att identifiera kritisk cyberteknik, kartlägga den tekniska utvecklingen och strategiska beroenden erbjuder sätt att minska dessa beroenden, som stöd för EU:s strategiska oberoende och tekniska suveränitet, samtidigt som en öppen ekonomi bevaras. Rådet noterar att färdplanen för kritisk cyberteknik kan ligga till grund för strategiska prioriteringar för EU:s finansieringsinstrument, samtidigt som den följer de respektive villkor som gäller för dessa. Rådet erinrar om att EU bör föra en ambitiös och bestämd europeisk industripolitik för att skapa ett hållbart, attraktivt och konkurrenskraftigt företagsklimat som också kan göra det möjligt för europeiska enheter på cyberområdet att expandera.

28. Rådet uppskattar avsikten att ta itu med den betydande kompetensklyftan på området för cybersäkerhet genom att locka till sig nya yrkesverksamma, även kvinnor, och genom kompetensutveckling och omskolning samt genom att investera i och anordna utbildning och övningar för att bygga upp en diversifierad och inkluderande arbetsstyrka på cyberområdet. Rådet är medvetet om de utmaningar som EU står inför när det gäller humankapital inom cybersäkerhet och cyberförsvar, och välkomnar initiativet från akademin för cyberkompetens, som också kan gynna arbetsstyrkan på cyberförsvarsområdet.

29. Rådet uppmanar medlemsstaterna att utbyta information om bästa praxis för att utbilda kvalificerade yrkesverksamma inom cybersäkerhet och utnyttja synergierna mellan militära, civila och brottsbekämpande initiativ, och uppmanar Esfa att, med stöd och sakkunskap från Europeiska försvarsbyrån och Enisa, överväga alternativ för att förbättra utbytet av bästa praxis och ytterligare synergier mellan de militära och civila områdena när det gäller utbildning och utveckling av cyberspecifika försvarsfärdigheter.

30. Rådet understryker vikten av en samsyn när det gäller sammansättningen av arbetsstyrkan inom cybersäkerhet och av tillhörande färdigheter för att kunna identifiera och åtgärda bristerna på arbetsmarknaden för cybersäkerhet, samt behovet av att engagera alla berörda parter, inbegripet medlemsstaterna och industrin. Rådet är medvetet om att fastställandet av indikatorer för övervakning av arbetsmarknaden för cybersäkerhet skulle bidra till att identifiera kompetensbehoven inom cybersäkerhet och kanalisera finansiering på lämpligt sätt, och samtidigt bidra till att fullgöra de politiska skyldigheterna, särskilt de som följer av NIS 2-direktivet. Rådet välkomnar förslaget om en ram för certifiering av färdigheter inom cyberförsvar och uppmanar den höga representanten att i egenskap av chef för Esfa utveckla denna i samarbete med utrikestjänsten, kommissionen och medlemsstaterna genom att utnyttja civila initiativ.

IV. **Partnerskap för att hantera gemensamma utmaningar**

31. Rådet uppmanar den höga representanten och kommissionen att stärka och främja sitt samarbete och utforska ömsesidigt fördelaktiga och skräddarsydda partnerskap om cyberförsvarspolitik, inbegripet kapacitetsuppbyggnad på cyberförsvarsområdet genom den europeiska fredsfaciliteten. Cyberförsvar bör därför läggas till som en punkt i EU:s dialoger och samråd om cyberfrågor och i de övergripande samråden om säkerhet och försvar med olika partner. Dessutom bör dialogen och samarbetet med den privata sektorn stärkas. Rådet understryker att internationellt samarbete om cybersäkerhetsstandarder och cybersäkerhetscertifiering skulle vara ett mervärde för den europeiska industrin. Det välkomnar därför kommissionens åtagande att göra detta till en väsentlig del av EU:s cyberdialoger med tredjeländer och internationella organisationer.

32. Rådet betonar vikten av internationellt samarbete för att förebygga eller minska riskerna för konflikter i cyberrymden, särskilt genom vidareutveckling och operativt genomförande av förtroendeskapande åtgärder på regional och internationell nivå, inbegripet inom FN, och genom att ytterligare uppmuntra användningen av befintliga förtroendeskapande åtgärder på cyberområdet, såsom inom Organisationen för säkerhet och samarbete i Europa (OSSE), även i tider av internationella spänningar.

    EU och dess medlemsstater framhåller att befintlig internationell rätt är tillämplig i cyberrymden och betonar betydelsen av fortsatta ansträngningar för att upprätthålla och främja FN:s ram för ansvarsfullt statligt agerande och arbeta för dess genomförande, bland annat genom att inrätta ett handlingsprogram för att främja ett ansvarsfullt statligt agerande i cyberrymden.

33. I linje med de gemensamma förklaringarna om samarbetet mellan EU och Nato uppmanar rådet den höga representanten, även i egenskap av chef för Europeiska försvarsbyrån, och kommissionen att stärka, fördjupa och utvidga partnerskapet med Nato på cyberområdet, med full respekt för principerna om delaktighet, ömsesidighet, ömsesidig öppenhet och transparens samt de båda organisationernas beslutsautonomi. Med hänsyn till behovet av att säkerställa kompletterande och samordnade insatser, med största möjliga deltagande av medlemsstater som inte är medlemmar i Nato, och av att undvika onödigt dubbelarbete, efterlyser rådet att man etablerar förbindelser på relevanta nivåer mellan EU och Nato när det gäller utbildning, lägesuppfattningar, övningar och FoU-plattformar, och eftersträvar potentiella synergier mellan de respektive frivilliga åtagandena för utvecklingen av nationell cyberförsvarsförmåga och krishanteringsramarna, skyddet av kritisk infrastruktur och förbättrat utbyte av lägesuppfattning, samordnade insatser mot skadlig cyberverksamhet samt kapacitetsuppbyggnad i tredjeländer. Detta inbegriper det tekniska avtalet mellan Natos centrala it-incidenthanteringsorgan (NCIRC) och CERT-EU och samt en förstärkt politisk dialog om cyberförsvarsfrågor på alla nivåer.

V. **Slutsats**

34. Med utgångspunkt i slutsatserna om EU:s politik för cyberförsvar uppmanar rådet den höga representanten och kommissionen att senast andra kvartalet 2023 utarbeta en plan för genomförandet av denna politik, och lägga fram den för medlemsstaternas godkännande. Rådet uppmanar också medlemsstaterna att frivilligt meddela sina ambitioner och åtgärder avseende cyberförsvar inom ramen för EU:s politik för cyberförsvar och fullt ut utnyttja icke rättsligt bindande frivilliga rekommendationer och åtaganden för att intensifiera sina nationella och multinationella cyberförsvarsinsatser i syfte att maximera deras inverkan på EU-nivå. Den höga representanten, kommissionen och medlemsstaterna uppmanas att från och med andra kvartalet 2024 årligen rapportera och diskutera framstegen med genomförandet av de olika delarna i det gemensamma meddelandet och genomförandeplanen för detta.