Europeiska unionens råd

Bryssel 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	

LÄGESRAPPORT

från:	Rådets generalsekretariat
av den:	23 maj 2022
till:	Delegationerna
Ärende:	Rådets slutsatser om utvecklingen av Europeiska unionens arbete på cyberområdet – Rådets slutsatser, godkända av rådet vid mötet den 23 maj 2022

För delegationerna bifogas rådets slutsatser om utveckling av Europeiska unionens arbete på cyberområdet, som godkändes av rådet vid mötet den 23 maj 2022.

BILAGA

Rådets slutsatser om utvecklingen av Europeiska unionens arbete på cyberområdet

EUROPEISKA UNIONENS RÅD

SOM ERINRAR OM

– rådets slutsatser om det gemensamma meddelandet av den 25 juni 2013 till Europaparlamentet och rådet om EU:s strategi för cybersäkerhet: En öppen, säker och trygg cyberrymd,[1]

– ramen för EU:s politik för it-försvar[2],

– rådets slutsatser om förvaltning av internet[3],

– rådets slutsatser om cyberdiplomati[4],

– rådets slutsatser om att stärka Europas system för cyberresiliens och främja en konkurrenskraftig och innovativ cybersäkerhetsbransch[5],

– rådets slutsatser om det gemensamma meddelandet av den 20 november 2017 till Europaparlamentet och rådet Resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU[6]

– rådets slutsatser om en ram för en gemensam diplomatisk respons från EU mot skadlig it-verksamhet (”verktygslåda för cyberdiplomati”)[7],

– rådets slutsatser om EU:s samordnade insatser vid storskaliga cyberincidenter och cyberkriser[8],

– rådets slutsatser om EU-riktlinjer för extern kapacitetsuppbyggnad på cyberområdet[9],

– rådets genomförandebeslut (EU) 2018/1993 av den 11 december 2018 om EU-arrangemangen för integrerad politisk krishantering[10],

---

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.
10 EUT L 320, 17.12.2018, s. 28.

– rådets slutsatser om uppbyggnad av kapacitet och förmågor på cybersäkerhetsområdet i EU[11],

– rådets slutsatser om 5G:s betydelse för den europeiska ekonomin och behovet av att minska säkerhetsriskerna i samband med 5G[12],

– Framtiden för ett starkt digitaliserat Europa efter 2020: främjande av digital och ekonomisk konkurrenskraft i unionen och digital sammanhållning[13],

– rådets slutsatser om kompletterande insatser för förstärkning av motståndskraft och motverkande av hybridhot[14],

– rådets slutsatser om att forma Europas digitala framtid[15],

– rådets slutsatser om cybersäkerheten för uppkopplade enheter[16],

– rådets slutsatser om EU:s strategi för cybersäkerhet för ett digitalt decennium[17],

– rådets slutsatser om säkerhet och försvar[18],

– rådets slutsatser om att undersöka potentialen hos initiativet för den gemensamma cyberenheten – en komplettering av EU:s samordnade insatser vid storskaliga cyberincidenter och cyberkriser[19],

– En strategisk kompass för säkerhet och försvar – För ett EU som skyddar sina medborgare, värden och intressen och bidrar till internationell fred och säkerhet[20],

---

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. BETONAR att skadligt agerande i cyberrymden, som härrör från både statliga och icke-statliga aktörer, har intensifierats de senaste åren, inbegripet en kraftig och konstant ökning av skadlig verksamhet riktad mot EU:s och dess medlemsstaters kritiska infrastruktur, leveranskedjor och immateriella rättigheter, en ökad risk för spridningseffekter samt en ökning av angrepp med utpressningsprogram mot våra företag, organisationer och medborgare, NOTERAR att återgången till maktpolitik fått vissa länder att i allt högre grad försöka utmana och undergräva den regelbaserade internationella ordningen i cyberrymden, vilket gör cybersfären, tillsammans med det fria havet, luften och yttre rymden, till ett alltmer omtvistat område, ÄR MEDVETET OM att storskaliga cyberangrepp eller försök att ta sig in, störa eller förstöra nätverks- och informationssystem med åtföljande systemeffekter har blivit vanligare, kan undergräva vår ekonomiska säkerhet och påverka våra demokratiska institutioner och processer och visar att vissa aktörer är redo att hota den internationella säkerheten och stabiliteten, UNDERSTRYKER att Rysslands militära aggression mot Ukraina har visat att offensiv cyberverksamhet kan genomföras som en integrerad del av hybridstrategier som förenar hot, destabilisering och ekonomiska störningar,

2. UPPREPAR att vår unions styrka, inför de nuvarande geopolitiska förändringarna, ligger i enighet, solidaritet och beslutsamhet, och att genomförandet av den strategiska kompassen kommer att stärka EU:s strategiska oberoende och dess förmåga att samarbeta med partner för att skydda sina värden och intressen, också på cyberområdet, FRAMHÅLLER att ett EU som är starkare och har större förmåga på säkerhets- och försvarsområdet, på ett positivt sätt kommer att bidra till global och transatlantisk säkerhet och kompletterar Nato, som förblir grunden för sina medlemmars kollektiva försvar, BEKRÄFTAR EU:s avsikt att intensifiera stödet för den regelbaserade internationella ordningen med Förenta nationerna i centrum,

3. UPPREPAR, i linje med rådets slutsatser om EU:s strategi för cybersäkerhet och med den strategiska kompassen, att unionens arbete på cyberområdet behöver utvecklas genom att vi ökar vår förmåga att förebygga cyberattacker med hjälp av kapacitetsuppbyggnad, förmågeutveckling, utbildning, övningar, ökad motståndskraft och genom ett fast bemötande av cyberattacker mot EU och dess medlemsstater med användning av samtliga tillgängliga EU-verktyg; detta inbegriper att ytterligare visa EU:s beslutsamhet att vidta omedelbara och långsiktiga åtgärder mot fientliga aktörer som försöker neka EU och dess partner säker och öppen tillgång till cyberrymden och påverka våra strategiska intressen, inbegripet våra partners säkerhet, BETONAR härvid att arbetet på cyberområdet syftar till att kombinera befintliga initiativ till EU-åtgärder som konsoliderar fred och stabilitet i cyberrymden och främjar en öppen, fri, global, stabil och säker cyberrymd, samtidigt som insatser på kort, medellång och lång sikt samordnas bättre för att förebygga, avskräcka, motverka och bemöta cyberhot och cyberattacker och stärka cyberkapaciteten, UNDERSTRYKER att dessa aspekter bör införlivas i EU:s arbete på cyberområdet i enlighet med dess fem funktioner på cyberområdet: stärka vår cyberresiliens och vår skyddskapacitet, göra krishanteringen mer solidarisk och heltäckande, främja vår vision för cyberrymden, stärka vårt samarbete med partnerländer och internationella organisationer, förebygga, försvara sig mot och bemöta cyberattacker,

I. STÄRKA VÅR CYBERRESILIENS OCH VÅR SKYDDKAPACITET

4. UPPREPAR att den övergripande nivån på EU:s cybersäkerhet behöver höjas, SER FRAM EMOT ett snabbt antagande av utkastet till direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS-direktivet), utkastet till förordning om digital operativ motståndskraft för finanssektorn (DORA-förordningen), utkastet till direktiv om kritiska entiteters motståndskraft och NOTERAR förslaget till förordning om åtgärder för en hög gemensam cybersäkerhetsnivå vid unionens institutioner, organ och byråer, som syftar till att verka för en Europeisk union som skyddar sina medborgare, offentliga tjänster och företag i cyberrymden, UPPMANAR kommissionen att slutföra antagandet av viktiga förslag för att säkerställa att digital infrastruktur, digital teknik, digitala produkter och digitala tjänster är säkra för att sända en tydlig signal om EU:s ambitioner på dessa områden och möjliggöra stöd till företag så att de kan klara denna utmaning, UPPMANAR kommissionen att lägga fram EU- gemensamma cybersäkerhetskrav för uppkopplade enheter, tillhörande processer och tjänster genom rättsakten om cyberresiliens, som kommissionen väntas föreslå före utgången av 2022, med beaktande av behovet av en övergripande och heltäckande strategi som omfattar digitala produkters hela livscykel, samt gällande lagstiftning, särskilt på cybersäkerhetsområdet,

5. UPPMANAR de berörda myndigheterna, såsom organet för europeiska regleringsmyndigheter för elektronisk kommunikation (Berec), Europeiska unionens cybersäkerhetsbyrå (Enisa) och samarbetsgruppen för nät- och informationssäkerhet, att tillsammans med Europeiska kommissionen, på grundval av en riskbedömning, utarbeta rekommendationer till medlemsstaterna och Europeiska kommissionen för att stärka motståndskraften hos kommunikationsnät och kommunikationsinfrastruktur inom Europeiska unionen, inbegripet det fortsatta genomförandet av EU:s 5G-verktygslåda,

6. UPPMANAR EU och dess medlemsstater att öka ansträngningarna för att höja den övergripande cybersäkerhetsnivån, till exempel genom att underlätta nyetablering av tillförlitliga leverantörer av cybersäkerhetstjänster, och BETONAR att främjande av framväxten av sådana leverantörer bör vara en prioritering för EU:s industripolitik på cybersäkerhetsområdet, UPPMANAR kommissionen att lägga fram olika alternativ för att främja framväxten av en tillförlitlig bransch för cybersäkerhetstjänster, stärka cybersäkerheten i IKT-leveranskedjan, ta itu med de potentiella effekterna av programvarusårbarheter för EU och dess medlemsstater, bland annat mot bakgrund av den kommande rättsakten om cyberresiliens, samt förbättra förmågan att upptäcka cyberhot och dela information om cyberhot i och mellan medlemsstaterna för att bättre kunna stå emot och motverka cyberattacker med potentiella systemeffekter och dra lärdom av hanteringen av sårbarheterna i Solarwinds, Microsoft Exchange och Apache Log4J,

7. UPPREPAR att det är av största vikt att investera i innovation och bättre utnyttja civil teknik för att stärka vår tekniska suveränitet, även på cyberområdet, UPPMANAR kommissionen att snabbt operationalisera Europeiska kompetenscentrumet för cybersäkerhet för att få till stånd ett starkt europeiskt ekosystem för cyberforskning, cyberindustri och teknik, UNDERSTRYKER behovet av att främja forskning och innovation, investera mer i civila och försvarsrelaterade områden för att stärka EU:s försvarstekniska och försvarsindustriella bas och utveckla EU:s och dess medlemsstaters cyberkapacitet, inbegripet strategisk stödkapacitet, FRAMHÅLLER betydelsen av att intensivt använda ny teknik, särskilt kvantdatorteknik, artificiell intelligens och stordata, för att få komparativa fördelar, inbegripet i fråga om insatser för hantering av cyberincidenter,

8. KONSTATERAR att förbättrad cybersäkerhet är ett sätt att öka effektiviteten och säkerheten i våra insatser på land, i luften, till sjöss och i yttre rymden, BETONAR vikten av att integrera cybersäkerhetsöverväganden i all EU-politik, inbegripet sektorslagstiftning som komplement till NIS 2-direktivet, och UPPMANAR kommissionen att undersöka alternativ för att öka cybersäkerheten i hela leveranskedjan för EU:s försvarstekniska och försvarsindustriella bas,

9. INSER att säkerställandet av tillräckliga ekonomiska och mänskliga resurser för cybersäkerhet och åtgärder som syftar till att skapa en gynnsam miljö för den privata sektorns konkurrenskraft är avgörande för att utveckla EU:s arbete på cyberområdet och att frågan om en stabil och långsiktig cybersäkerhetsfinansiering också bör behandlas på EU-nivå genom utformning och genomförande av en övergripande mekanism som kombinerar flera finansieringskällor, inbegripet för kostnaderna för en högt kvalificerad arbetskraft, UPPMANAR därför kommissionen att undersöka olika alternativ för en sådan mekanism före utgången av 2022, så att de kan diskuteras i relevanta rådsorgan,

10. FRAMHÅLLER behovet av att stärka våra insatser och öka samarbetet i kampen mot internationell it-brottslighet, särskilt utpressningsprogram, genom Empact-mekanismen (Europeiska sektorsövergripande plattformen mot brottshot), genom utbyten mellan sektorerna för it-säkerhet och brottsbekämpning samt den diplomatiska sektorn, och genom att stärka brottsbekämpningskapaciteten när det gäller att utreda och lagföra it-brottslighet, BEKRÄFTAR sitt åtagande att informera allmänheten om cyberhot och de åtgärder som vidtagits nationellt och på EU-nivå mot dessa hot genom att involvera det civila samhället, den privata sektorn och den akademiska världen, i syfte att öka medvetenheten och uppmuntra en lämplig nivå av it-skydd och it-hygien, FRAMHÅLLER behovet av att fokusera på medborgarnas färdigheter och förmåga när det gäller cybersäkerhet på EU- och medlemsstatsnivå och behovet av att aktivt involvera användarna i deras eget skydd,

II. GÖRA KRISHANTERINGEN MER SOLIDARISK OCH HELTÄCKANDE

11. BETONAR, med utgångspunkt i de årliga cyberövningarna, andra övningar med en cyberdimension och Cyber Europe-övningen (EU CyCLES) 2022, vikten av att inrätta ett program för regelbundna EU-omfattande cyberövningar på flera nivåer i syfte att testa och utveckla EU:s interna och externa insatser vid storskaliga cyberincidenter, med deltagande av rådet, utrikestjänsten, kommissionen och relevanta aktörer såsom Enisa och den privata sektorn, vilket ska utformas så att det bidrar till EU:s allmänna övningsstrategi, FRAMHÅLLER vikten av att vidareutveckla Cyber Europe- och BlueOLEx-övningarna och kombinera insatser på olika nivåer, ÄR MEDVETET OM behovet av att utvärdera och konsolidera de befintliga övningarna och undersöka möjligheterna till ytterligare övningar inom specifika delar av cyberområdet, särskilt en militär CERT-övning eller en övning med fokus på krissamarbete mellan EU:s institutioner, organ och byråer, INSER att unionens arbete på cyberområdet kommer att stärka vår förmåga att förhindra cyberattacker genom olika åtgärder, inbegripet utbildning, och UPPMANAR därför medlemsstaterna att stärka det civil-militära samarbetet när det gäller cyberutbildning och gemensamma övningar,

12. FRAMHÄVER behovet av att ytterligare testa och förstärka det operativa samarbetet och den kollektiva situationsmedvetenheten bland medlemsstaterna, bland annat genom etablerade nätverk såsom CSIRT-nätverket och Europeiska kontaktnätverket för cyberkriser (EU CyCLONe), i syfte att öka EU:s beredskap för storskaliga cyberincidenter, UNDERSTRYKER vikten av att arbeta för att bland medlemsstaterna och med EU:s institutioner, organ och byråer utveckla ett gemensamt språk som är skräddarsytt för diskussioner på politisk nivå, och därigenom på lämpligt sätt stödja inrättandet av en konsoliderad bedömning av allvarlighetsgrad och konsekvenser när det gäller relevanta cyberincidenter samt möjliga utvecklingsscenarier och de behov som uppstår genom dessa, BETONAR i detta avseende behovet av att förbättra komplementariteten hos de gemensamma lägesbedömningsrapporterna, inbegripet EU CyCLONE:s rapporter om effekterna och allvarlighetsgraden när det gäller storskaliga cyberincidenter i EU:s medlemsstater och de hotbildsbedömningar som EU Intcen tillhandahåller inom ramen för EU:s verktygslåda för cyberdiplomati, UPPMANAR kommissionen, den höga representanten och samarbetsgruppen för nät- och informationssäkerhet att, i samordning med relevanta civila och militära organ och byråer samt etablerade nätverk, inbegripet EU CyCLONe, senast i slutet av 2022 genomföra en riskbedömning och utarbeta riskscenarier ur ett cybersäkerhetsperspektiv i en situation med hot eller möjlig attack mot medlemsstater eller partnerländer och lägga fram dem för relevanta rådsorgan, FRAMHÅLLER behovet av lämplig och samordnad offentlig kommunikation om EU:s insatser vid storskaliga cyberincidenter,

13. BETONAR behovet av att, i händelse av en storskalig cyberincident, stärka samordningen och, när så är lämpligt, bygga vidare på de framsteg som gjorts och det arbete som utförts av snabbinsatsteam för cybersäkerhet inom ramen för Pesco och på det arbete som utförts av CSIRT-nätverket och EU CyCLONe, för en frivillig sammanslagning av medlemsstaternas resurser att hantera incidenter, KONSTATERAR att en utveckling av förbindelser med den privata sektorn skulle kunna stärka den offentliga kapaciteten, särskilt mot bakgrund av kompetensbristerna i EU, och att en identifiering och samordning av dessa privata aktörer skulle kunna göra skillnad i händelse av storskaliga incidenter, UPPMANAR kommissionen att lägga fram ett förslag om en ny fond för hantering av cybersäkerhetsincidenter före utgången av tredje kvartalet 2022, som ett led i en fullständig förberedelse för storskaliga cyberincidenter,

14. ERINRAR OM behovet av att, i linje med den strategiska kompassen, investera i ömsesidigt bistånd i enlighet med artikel 42.7 i fördraget om Europeiska unionen och solidaritet i enlighet med artikel 222 i fördraget om Europeiska unionens funktionssätt, särskilt genom att ofta anordna övningar, BETONAR i detta sammanhang behovet av att fortsätta arbetet med att tillhandahålla och samordna bilateralt civilt och militärt stöd, bland annat genom att undersöka möjligheterna till stöd från EU på medlemsstaternas uttryckliga begäran, och med att identifiera lämpliga motåtgärder, bland annat genom att utforma en samordnad kommunikationsstrategi, i samband med genomförandet av artikel 42.7, NOTERAR att detta även bör inbegripa en undersökning av kopplingarna till EU:s befintliga krishanteringsmekanismer och EU:s civilskyddsmekanism,

15. FRAMHÅLLER att ett förstärkt arbete på cyberområdet i EU kommer att kräva förbättrade säkra kommunikationer, ERINRAR i detta syfte OM den strategiska kompassens riktlinjer i detta avseende och UPPMANAR kommissionen och andra berörda institutioner, organ och byråer att senast i slutet av 2022 göra en kartläggning av de befintliga verktygen för säker kommunikation på cyberområdet, för diskussion i relevanta rådsorgan och med relevanta samarbetsgrupper, t.ex. CSIRT-nätverket och EU CyCLONe,

III. FRÄMJA VÅR VISION FÖR CYBERRYMDEN

16. ERINRAR OM att den gemensamma och övergripande EU-strategin för cyberdiplomati syftar till att bidra till konfliktförebyggande, begränsning av cybersäkerhetshot och ökad stabilitet i internationella förbindelser, BEKRÄFTAR i detta sammanhang EU:s åtagande att lösa internationella tvister i cyberrymden med fredliga medel och att internationell rätt, inbegripet internationell människorättslagstiftning och internationell humanitär rätt, ska tillämpas på staternas agerande i cyberrymden, FRAMHÅLLER EU:s och dess medlemsstaters åtagande att agera i enlighet med de frivilliga, icke-bindande normer för ansvarsfullt statligt agerande i cyberrymden som alla FN:s medlemsstater har enats om, BETONAR vikten av en öppen, fri, global, stabil och säker cyberrymd där mänskliga rättigheter, grundläggande friheter och rättsstatsprincipen tillämpas fullt ut till stöd för socialt välbefinnande, ekonomisk tillväxt, välstånd och integritet i våra fria och demokratiska samhällen och BEKRÄFTAR EU:s och dess medlemsstaters åtagande att fortsätta att främja dessa värden och principer, BETONAR, i syfte att utveckla kanaler för en konstruktiv, uppriktig och öppen dialog med viktiga intressenter på cyberområdet, vikten av att cyberfrågor, inbegripet EU:s verktygslåda för cyberdiplomati, blir en integrerad del av unionens anslutningsförhandlingar och EU:s strategiska och politiska dialoger med både internationella partner och konkurrenter och UPPMANAR samtidigt den höga representanten att se över befintliga bilaterala cyberdialoger och vid behov föreslå att liknande samarbete inleds med ytterligare länder eller relevanta internationella organisationer,

17. ERINRAR OM vikten av samarbete med flera parter eftersom andra intressenter också är ansvariga för cybersäkerheten, särskilt när det gäller att genomföra de rekommendationer och beslut som fattas i internationella och regionala forum, UPPMANAR EU och dess medlemsstater att ytterligare främja vår modell för cyberrymden och internet på grundval av flerpartsstrategin och genom initiativ såsom Paris Call for Trust and Security in Cyberspace (”Parisuppropet för tillit och säkerhet i cyberrymden”) och förklaringen om internets framtid, för att betona de gemensamma fördelarna med stabilitet i cyberrymden och öka medvetenheten globalt om farorna med en statscentrerad och auktoritär syn på internet, och UPPMANAR EU och dess medlemsstater att ytterligare stärka samarbetet med flerpartssamhället, bland annat genom att utnyttja relevanta projekt såsom initiativet för cyberdiplomati som ingår i EU:s utrikespolitiska instrument,

18. ÅTAR SIG att kontinuerligt engagera sig i relevanta internationella organisationer, särskilt inom ramen för processer med anknytning till FN:s första och tredje utskott, samtidigt som det betonas att gällande internationell rätt ska tillämpas, utan förbehåll, i och med avseende på cyberrymden, BETONAR vikten av fortsatta ansträngningar för att upprätthålla och främja FN:s ram för ansvarsfullt statligt agerande, och UNDERSTRYKER att EU och dess medlemsstater aktivt kommer att arbeta för att stärka dess genomförande, bland annat genom att inrätta ett handlingsprogram för att främja ett ansvarsfullt statligt agerande i cyberrymden, BETONAR att EU och dess medlemsstater kommer att delta aktivt i förhandlingarna om en framtida FN-konvention som ska fungera som ett effektivt instrument för brottsbekämpande och rättsliga myndigheter i den globala kampen mot it-relaterad brottslighet, med fullt beaktande av den befintliga ramen med internationella och regionala instrument på detta område, särskilt Budapestkonventionen om it-relaterad brottslighet, FRAMHÅLLER vikten av att ytterligare stödja utvecklingen och operationaliseringen av förtroendeskapande åtgärder på regional och internationell nivå och ytterligare uppmuntra till användning av befintliga förtroendeskapande åtgärder inom cyberområdet i OSSE, även i tider av internationella spänningar,

19. ERINRAR OM att en proaktiv människorättsbaserad strategi för att säkerställa internationella standarder på områdena ny teknik och grundläggande internetstruktur som följer demokratiska värden och principer är avgörande för att garantera att internet förblir ett enda globalt och öppet nätverk, och STÖDER principen om att användningen och utvecklingen av teknik ska respektera mänskliga rättigheter och vara integritetsinriktad samt att teknikens användning ska vara laglig, säker och etisk, UPPMANAR den höga representanten och kommissionen att utarbeta en strategisk vision för tekniska frågor på det digitala området som har utrikespolitiska konsekvenser och skulle kunna påverka cyberrymdens och i synnerhet internets stabilitet, inbegripet i relevanta specialiserade internationella organisationer (Internationella teleunionen osv.),

IV. STÄRKA VÅRT SAMARBETE MED PARTNERLÄNDER OCH INTERNATIONELLA ORGANISATIONER

20. BETONAR behovet av att bättre koppla samman EU:s strategi för kapacitetsuppbyggnad på cyberområdet till FN:s normer för ansvarsfullt statligt agerande i cyberrymden, bland annat genom att utveckla skräddarsydda samarbets- och kapacitetsuppbyggnadsprogram för att stödja tredjeländer i deras genomförandearbete, och därigenom fortsätta och utöka våra insatser för att främja FN:s handlingsprogram för att främja ansvarsfullt statligt agerande i cyberrymden, BETONAR vikten av att fullt ut integrera uppbyggnad av cyberkapacitet som en del av EU:s utbud i dess egenskap av säkerhetsgarant, med lämplig samordning av insatserna mellan medlemsstaterna och EU:s institutioner, organ och byråer, och VÄLKOMNAR särskilt samarbete mellan medlemsstaterna samt med partner inom den offentliga och den privata sektorn, särskilt genom EU CyberNet (EU:s nätverk för kapacitetsuppbyggnad på cyberområdet) och det globala forumet för it-expertis (GFCE), för att säkerställa samordning och undvika dubbelarbete,

UPPMANAR den höga representanten och kommissionen att senast tredje kvartalet 2022 inrätta en *nämnd för kapacitetsuppbyggnad på cyberområdet* och att hålla regelbundna diskussioner i den övergripande arbetsgruppen för cyberfrågor, UPPMANAR kommissionen och den höga representanten att ytterligare mobilisera instrumentet för grannskapet, utvecklingssamarbete och internationellt samarbete (NDICI), instrumentet för stöd inför anslutningen (IPA III) och andra finansiella verktyg, såsom den europeiska fredsfaciliteten och initiativet Global Gateway, för att stödja stärkandet av våra partners motståndskraft, deras

förmåga att identifiera och ta itu med cyberhot och att utreda och lagföra it-brottslighet samt ta fram samarbetsprojekt, inbegripet och i synnerhet i samband med kriser, UPPMANAR till samarbete med partner på västra Balkan och i EU:s östra och södra grannskap samt utstationering av experter från EU och medlemsstaterna för att erbjuda stöd vid cyberkriser, med beaktande av befintliga rättsliga mandat,

21. FRAMHÅLLER behovet av att intensifiera ansträngningarna för att utarbeta en strukturerad, öppen och utåtriktad EU-strategi för hur man ska kunna främja en global samsyn om tillämpningen av internationell rätt i cyberrymden, FN:s ram för ansvarsfullt statligt agerande i cyberrymden, inbegripet initiativet till ett handlingsprogram för att främja ett ansvarsfullt statligt agerande i cyberrymden, samt vad gäller EU:s och dess medlemsstaters ståndpunkt i de pågående förhandlingarna om en FN-konvention om it-brottslighet, och UPPMANAR den höga representanten att, som ett led i dessa insatser, senast i slutet av 2022 förelägga rådet en plan för utåtriktad verksamhet, UPPMANAR den höga representanten och kommissionens avdelningar att fullt ut och systematiskt utnyttja de 145 delegationerna och utveckla ett regelbundet och givande samarbete mellan dem och medlemsstaternas ambassader i tredjeländer, under överinseende av EU:s planerade nätverk för cyberdiplomati, UPPMANAR den höga representanten att senast under tredje kvartalet 2022 inrätta EU-nätverket för cyberdiplomati, som ska bidra till informationsutbyte, gemensam utbildningsverksamhet för EU-personal och personal från medlemsstaterna, samstämmiga insatser för kapacitetsuppbyggnad och stärkande av genomförandet av FN:s ram för ansvarsfullt statligt agerande samt förtroendeskapande åtgärder mellan stater,

22. BETONAR sitt åtagande om att utöka sitt samarbete med internationella organisationer och partnerländer för att främja den gemensamma förståelsen av cyberhotbilden, utveckla samarbetsmekanismer och proaktivt identifiera samarbetsinriktade diplomatiska insatser, ERINRAR OM de viktigaste resultaten av samarbetet mellan EU och Nato på området cybersäkerhet inom ramen för genomförandet av de gemensamma förklaringarna från Warszawa 2016 och Bryssel 2018, med full respekt för båda organisationernas beslutsautonomi och förfaranden och på grundval av principerna om öppenhet, ömsesidighet och delaktighet, BETONAR behovet av att ytterligare stärka it-samarbetet med Nato genom övningar, informationsutbyte och utbyte mellan experter, inbegripet om förmågeutveckling, kapacitetsuppbyggnad för partner och uppdrag och insatser, samt om tillämpligheten av internationell rätt och FN:s normer för ansvarsfullt statligt agerande i cyberrymden, och möjlig samordnad respons mot skadlig cyberverksamhet,

V. FÖREBYGGA, FÖRSVARA SIG MOT OCH BEMÖTA CYBERATTACKER,

23. INSER att cyberrymden har blivit en arena för geopolitisk konkurrens och UPPREPAR därför att EU måste ha förmåga att snabbt och kraftfullt svara på cyberattacker, däribland statsstödd skadlig cyberverksamhet riktad mot EU och dess medlemsstater, och därför måste stärka EU:s verktygslåda för cyberdiplomati och fullt ut utnyttja alla dess instrument, inbegripet tillgängliga politiska, ekonomiska, diplomatiska, rättsliga och strategiska kommunikationsverktyg för att förebygga, avskräcka, motverka och bemöta skadlig cyberverksamhet, UNDERSTRYKER att fientliga aktörer måste vara medvetna om att cyberangrepp mot medlemsstater och EU-institutioner kommer att upptäckas på ett tidigt stadium, identifieras omgående och bemötas med alla nödvändiga verktyg och strategier, UPPMANAR medlemsstaterna och den höga representanten att med kommissionens stöd och med utgångspunkt i de lärdomar som dragits av genomförandet av verktygslådan för cyberdiplomati sedan dess start och av EU CyCLES-övningen, och främst de delar av cyberarbetet som ingår i däri, arbeta för att senast före utgången av första kvartalet 2023 ta fram en reviderad version av riktlinjerna för genomförandet av EU:s verktygslåda för cyberdiplomati, särskilt genom att undersöka ytterligare motåtgärder,

24. UNDERSTRYKER behovet av att hålla regelbundna diskussioner om cyberhotbilden i rådets relevanta organ och kommittéer, samtidigt som man regelbundet samarbetar med den privata sektorn och utgår från bedömningen av de senaste incidenternas konsekvenser och allvarlighetsgrad, för att öka den allmänna medvetenheten om och beredskapen för ytterligare tillämpningar av EU:s verktygslåda för cyberdiplomati och utveckla fler verktyg till stöd för dess genomförande; konstaterar att den nationella säkerheten förblir varje medlemsstats eget ansvar, men NOTERAR behovet av att stärka utbytet och samarbetet vad avser underrättelser och information mellan medlemsstaterna samt med EU Intcen för att kunna utbyta underrättelser i början av beslutsprocessen, bland annat när det gäller frågan om attribuering, och därigenom möjliggöra en snabb, effektiv och välgrundad reaktion på skadlig cyberverksamhet riktad mot EU och dess partner, UPPREPAR vikten av att stärka EU Intcens kapacitet på cyberområdet, på grundval av frivilliga underrättelsebidrag från medlemsstaterna och utan att det påverkar deras befogenheter, och av att utreda förslaget om ett eventuellt inrättande av en medlemsstaternas arbetsgrupp för cyberunderrättelser,

25. KONSTATERAR att EU:s förklaringar och de restriktiva åtgärder som antagits inom ramen för EU:s verktygslåda för cyberdiplomati har sänt ett starkt budskap om att skadlig cyberverksamhet som utgör ett yttre hot mot EU, dess medlemsstater och partner är oacceptabel och att de därmed bidrar till att förebygga, avskräcka, motverka och bemöta skadlig cyberverksamhet, UPPREPAR sitt åtagande att använda dessa åtgärder i syfte att erinra om de skyldigheter som gäller för cyberrymden enligt internationell rätt, inbegripet FN-stadgan i dess helhet, och främja FN:s ram för ansvarsfullt statligt agerande i cyberrymden, inbegripet kravet på tillbörlig aktsamhet för alla stater att inte medvetet tillåta att deras territorium används för internationellt rättsstridiga handlingar med användning av IKT, i syfte att ytterligare utveckla och främja EU:s gemensamma syn på tillämpningen av internationell rätt i cyberrymden, NOTERAR att lämpliga och snabba budskap minskar risken för upptrappning och kan avskräcka angripare som riktar sig mot europeiska intressen och UPPMANAR den höga representanten att utveckla och förelägga medlemsstaterna en enhetlig kommunikationsstrategi om användningen av EU:s verktygslåda för cyberdiplomati,

26. UPPMUNTRAR utvecklingen av gradvisa, riktade och hållbara strategier och reaktioner på skadlig cyberverksamhet, med användning av de många olika verktyg som tillhandahålls genom EU:s verktygslåda för cyberdiplomati, inbegripet EU:s cybersanktionssystem, och med planering för ytterligare åtgärder, BETONAR behovet av att öka möjligheten att från fall till fall mobilisera alla tillgängliga verktyg, både interna och externa, för att förebygga, avskräcka, motverka, och bemöta cyberattacker, och genomföra dessa verktyg i en snabb, effektiv, gradvis, riktad och varaktig strategi som bygger på ett långsiktigt strategiskt engagemang, UPPMANAR den höga representanten att i samarbete med kommissionen identifiera möjliga gemensamma EU-insatser mot cyberattacker, inbegripet olika sanktionsalternativ, över hela spektrumet, för att vara redo att vid behov vidta snabba och effektiva åtgärder, och presentera dem för rådet före utgången av första kvartalet 2023,

27. NOTERAR att cyberförsvar i första hand är ett nationellt ansvar och UPPMANAR medlemsstaterna att vidareutveckla sin egen förmåga att genomföra cyberförsvarsinsatser, inbegripet proaktiva åtgärder för att skydda, upptäcka, försvara sig mot och avskräcka från cyberattacker, och eventuellt stödja andra medlemsstater och EU; varje medlemsstat uppmuntras att vid behov förbättra sin egen förmåga att tillhandahålla och ta emot stöd och bistånd, BETONAR att ytterligare utveckling av denna förmåga bör vara ett av de viktigaste målen för EU:s kommande politik för cyberförsvar, NOTERAR att EU:s politik för cyberförsvar i högre grad bör beakta hur relevanta EU-institutioner och EU-organ kan medverka till att öka samarbetet mellan EU:s och medlemsstaternas relevanta cyberförsvarsaktörer och utveckla deras egen förmåga, i enlighet med sina respektive mandat, UPPMANAR den höga representanten att tillsammans med kommissionen komplettera utvecklingen av EU:s arbete på cyberområdet genom att lägga fram ett långtgående förslag till en EU-politik för cyberförsvar under 2022, vilket ska bana väg för rådets vidareutveckling av EU:s cyberarbete,

28. FRAMHÅLLER behovet av att öka interoperabiliteten och informationsutbytet genom samarbete mellan militära snabbinsatsteam för cyberincidentshantering (MilCERT), UPPMANAR medlemsstaterna att på grundval av EDA:s arbete inrätta ett MilCERT-nätverk för att utveckla samarbetet och underlätta informationsutbytet, vilket också skulle bidra till att främja samordning med andra cybergrupper, samt ett nätverk av militära cyberbefälhavare för att stärka det strategiska samarbetet mellan EU-medlemsstaternas cyberkommandon eller andra motsvarande myndigheter; inrättandet av dessa nätverk, tillsammans med cyberprojekt inom ramen för Pesco, skulle bidra till ett stärkt cyberförsvar på EU-nivå, BETONAR vikten av samarbete mellan det föreslagna MilCERT-nätverket och det redan befintliga civila nätverket (CSIRT) för att förbättra informationsutbytet och förbättra situationsmedvetenheten,

29. UPPREPAR, på grundval av EU:s militära vision och strategi för cyberrymden som operativt område (Military Vision and Strategy on Cyberspace as a Domain of Operations) och med beaktande av den pågående utvecklingen av det militära konceptet för cyberförsvar för EU-ledda militära insatser och uppdrag, behovet av att integrera cyberdimensionen i planeringen och genomförandet av GSFP-uppdrag och GSFP-insatser, bland annat genom att förbättra deras cyberkapacitet, och BETONAR att detta kommer att bidra till bättre cybersituationsmedvetenhet på EU-nivå,

30. NOTERAR avslutningsvis att cyberarbetet är ett steg mot inrättandet av en EU-doktrin för åtgärder i cyberrymden, baserad på stärkt resiliens, ökad förmåga och fler reaktionsalternativ, samt en gemensam ståndpunkt om tillämpningen av internationell rätt i cyberrymden. Rådet KOMMER ATT UTVÄRDERA de framsteg som gjorts med genomförandet av dessa slutsatser under 2023 för att säkerställa den fortsatta utvecklingen av EU:s cyberarbete.