Europeiska unionens råd

Bryssel den 20 oktober 2021
(OR. en)

13048/21

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

LÄGESRAPPORT

från:	Rådets generalsekretariat
av den:	19 oktober 2021
till:	Delegationerna
Föreg. dok. nr:	12534/21
Ärende:	Rådets slutsatser om att undersöka potentialen hos initiativet för den gemensamma cyberenheten – en komplettering av EU:s samordnade insatser vid storskaliga cyberincidenter och cyberkriser – Rådets slutsatser (den 19 oktober 2021)

För delegationerna bifogas rådets slutsatser om att undersöka potentialen hos initiativet för den gemensamma cyberenheten – en komplettering av EU:s samordnade insatser vid storskaliga cyberincidenter och cyberkriser, som antogs av rådet vid mötet den 19 oktober 2021.

BILAGA

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

EUROPEISKA UNIONENS RÅD,

SOM ERINRAR OM sina slutsatser om

– EU:s strategi för cybersäkerhet för ett digitalt decennium[1],

– EU:s samordnade insatser vid storskaliga cyberincidenter och cyberkriser[2],

– cyberdiplomati[3],

– en ram för en gemensam diplomatisk respons från EU mot skadlig it-verksamhet (”verktygslåda för cyberdiplomati”)[4],

– säkerhet och försvar[5],

– ramen för EU:s politik för it-försvar[6],

– att forma Europas digitala framtid[7], och erinrar om

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

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

– Gemensamt meddelande till Europaparlamentet och rådet – *Resiliens, avskräckning och försvar: stärkt cybersäkerhet i EU*[8], liksom om sina slutsatser om

– uppbyggnad av kapacitet och förmågor på cybersäkerhetsområdet i EU[9],

1. UNDERSTRYKER att cybersäkerhet är avgörande för att bygga ett motståndskraftigt, grönt och digitalt Europa, BETONAR att cybersäkerhet är oumbärligt för välståndet och säkerheten i EU och dess medlemsstater, och bland dess befolkning, företag och institutioner, samt för att bevara våra fria och demokratiska samhällens integritet,

2. ÄR MEDVETET om många cybersäkerhetshots gränsöverskridande och sektorsövergripande karaktär samt riskerna med och de potentiella följderna av fortlöpande kampanjer av mer verkningsfull, sofistikerad, riktad, komplicerad, ihållande och/eller genomgripande skadlig cyberverksamhet[10]; covid-19-pandemin har ytterligare blottlagt våra samhällens sårbarhet och risken för storskaliga cyberincidenters skador på ekonomin, demokratin, samhällsviktiga tjänster och kritisk infrastruktur, framför allt inom hälso- och sjukvårdssektorn; den har också ökat betydelsen av konnektivitet och samhällets beroende av tillförlitliga, pålitliga och säkra nät och informationssystem; slutligen har den understrukit att det behövs ett globalt, öppet, fritt, stabilt och säkert internet och förtroende för produkterna, processerna och tjänsterna på området för informations- och kommunikationsteknik (IKT) och deras säkerhet, inbegripet behovet av att säkerställa en motståndskraftig leveranskedja,

---

8 14435/17 + COR 1.
9 7737/19.
10 Enisas hotbildsrapport 2020.

3. UPPREPAR vikten av cyberresiliens och av att EU:s ram för hantering av cyberkriser[11] för effektiva och snabba insatser på EU-nivå vid storskaliga cyberincidenter och cyberkriser vidareutvecklas och ytterligare integreras i de befintliga horisontella och sektoriella EU-krishanteringsmekanismerna, BETONAR den roll som rådet och EU-arrangemangen för integrerad politisk krishantering (IPCR) har när det gäller att säkerställa snabb samordning och reaktion på unionens politiska nivå vid kriser med ursprung i eller utanför unionen som har omfattande konsekvenser eller politisk betydelse, FRAMHÅLLER att det är viktigt att testa dessa ramar och mekanismer vid regelbundna övningar,

4. ERINRAR om att verksamhet på EU-nivå vad gäller storskaliga cyberincidenter och cyberkriser äger rum i enlighet i enlighet med subsidiaritets-, proportionalitets-, komplementaritets- och konfidentalitetsprincipen samt principen om att undvika dubbelarbete, UPPREPAR att medlemsstaterna har huvudansvaret för hanteringen av de storskaliga cyberincidenter och cyberkriser som drabbar dem, ERINRAR om att det är viktigt att respektera medlemsstaternas befogenheter och respektera att den nationella säkerheten, i enlighet med artikel 4.2 i fördraget om Europeiska unionen, är varje medlemsstats eget ansvar, även inom cybersäkerhet,

5. ERINRAR samtidigt om att det är viktigt att respektera EU-institutionernas, EU-organens och EU-byråernas befogenheter och mandat; även den höga representanten, kommissionen och andra av EU:s institutioner, organ och byråer har en väsentlig roll grundad på unionsrätten, bland annat på grund av de eventuella konsekvenserna av storskaliga cyberincidenter och cyberkriser för den inre marknaden och för EU-institutionernas, EU-organens och EU-byråernas funktion,

---

[11] 10086/18.

6. POÄNGTERAR att det är nödvändigt att undvika onödigt dubbelarbete och eftersträva komplementaritet och mervärde vid den fortsatta utvecklingen av EU:s ram för hantering av cyberkriser samt att säkerställa anpassning till befintliga mekanismer, initiativ, nätverk, processer och förfaranden på nationell och europeisk nivå, UNDERSTRYKER betydelsen av att rationalisera befintliga processer och strukturer för att minska komplexiteten samt av att i unionssammanhållningens intresse förbättra tillgängligheten och lyhördheten för dem som söker hjälp och solidaritet,

7. ÄR MEDVETET om att internationell rätt, inbegripet Förenta nationernas stadga i dess helhet, internationell humanitär rätt och människorättslagstiftning, är tillämplig i cyberrymden och FÖRESPRÅKAR efterlevnad av de frivilliga, icke-bindande normer, regler och principer för staters ansvarsfulla agerande i cyberrymden, som alla FN-medlemsstater ställt sig bakom,

8. VÄLKOMNAR de framsteg som gjorts de senaste åren i rådet, framför allt i övergripande arbetsgruppen för cyberfrågor och andra berörda arbetsgrupper i rådet, samt vid inrättande av andra initiativ, nätverk och mekanismer för samarbete och informationsutbyte mellan medlemsstaterna, i synnerhet samarbetsgruppen för nät- och informationssäkerhet och CSIRT-nätverket, som inrättats genom Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016, Europeiska kontaktnätverket för cyberkriser (EU CyCLONe) samt relevanta cyberförsvarsrelaterade projekt som inletts inom ramen för det permanenta strukturerade samarbetet (Pesco)[12], den gemensamma arbetsgruppen mot it-brottslighet (J-CAT), det europeiska rättsliga nätverket mot it-brottslighet (EJCN), medlemsstaternas frivilliga bidrag till EU:s underrättelse- och lägescentral (EU Intcen) liksom samordning och samarbete i samband med verktygslådan för cyberdiplomati,

---

[12] Särskilt *Snabbinsatsteam och ömsesidigt bistånd på området för cybersäkerhet*, som samordnas av Litauen, *Samordningscentrumet för cyber- och informationsområdet*, som samordnas av Tyskland, och *Plattform för utbyte av information om hantering av cyberhot och cyberincidenter*, som samordnas av Grekland.

9. ERINRAR om de befintliga nätverken för samarbete mellan EU:s institutioner, organ och byråer, till exempel det strukturerade samarbetet mellan Enisa och incidenthanteringsorganisationen för EU:s institutioner och byråer (CERT-EU), och samförståndsavtalet mellan Enisa, Europeiska försvarsbyrån (EDA), Europeiska it-brottscentrumet (EC3) vid Europol och CERT-EU, BETONAR vikten av fortsatt regelbundet informationsutbyte med rådet om den ytterligare utvecklingen inom dessa samarbetsramar,

10. FRAMHÅLLER vikten av att förbättra samarbetet och informationsutbytet mellan olika cybergrupper inom EU och dess medlemsstater på alla nödvändiga nivåer – teknisk, operativ och strategisk/politisk nivå – och att koppla samman befintliga mekanismer, nätverk, strukturer, processer och förfaranden för krishantering, om detta stöder och förbättrar hanteringen av storskaliga och gränsöverskridande cyberincidenter och cyberhot,

11. VÄRDESÄTTER de framsteg som gjorts inom ramen för Pesco av en grupp av medlemsstater vid inrättandet av en gemensam operativ cyberförmåga, s.k. snabbinsatsteam för cybersäkerhet, i syfte att fördjupa det frivilliga samarbetet på cyberområdet genom ömsesidigt bistånd, bland annat som svar på storskaliga cyberincidenter och cyberkriser,

12. ÄR MEDVETET om de brottsbekämpande myndigheternas erfarenheter av och dygnet runt-förmåga till operativt samarbete och säkert informationsutbyte när det gäller större gränsöverskridande cyberattacker genom beredskapsprotokollet för EU:s brottsbekämpningsinsatser,

13. ÄR MEDVETET om det fortsatta genomförandet av ramen för en gemensam diplomatisk respons från EU mot skadlig it-verksamhet (”verktygslåda för cyberdiplomati”), ERINRAR om att varje medlemsstat från fall till fall fritt kan fatta sina egna suveräna beslut vad gäller attribuering av skadlig cyberverksamhet, ERINRAR om att de åtgärder som vidtas inom ramen för den gemensamma diplomatiska responsen från EU mot skadlig cyberverksamhet bör grundas på en gemensam situationsmedvetenhet som medlemsstaterna har kommit överens om; EU Intcen spelar en central roll som nav för tillhandahållande av situationsmedvetenhet och hotbildsbedömning i cyberfrågor till EU på grundval av frivilliga underrättelsebidrag från medlemsstaterna och utan att det påverkar deras befogenheter,

14. ERINRAR om vikten av ömsesidigt bistånd och solidaritet, i enlighet med artikel 42.7 i fördraget om Europeiska unionen och artikel 222 i fördraget om Europeiska unionens funktionssätt, och EFTERLYSER ytterligare övningar med en cyberdimension, ERINRAR om behovet av att reflektera över kopplingen mellan EU:s ram för hantering av cyberkriser, verktygslådan för cyberdiplomati och bestämmelserna i de ovannämnda artiklarna i fall av storskaliga cyberincidenter eller cyberkriser, ERINRAR vidare om att medlemsstaternas skyldigheter som följer av artikel 42.7 i fördraget om Europeiska unionen inte påverkar den särskilda karaktären hos vissa medlemsstaters säkerhets- och försvarspolitik, ERINRAR även om att Nato förblir grundvalen för det kollektiva försvaret av de stater som är medlemmar i den organisationen,

15. VÄRDESÄTTER samarbetet mellan EU och Nato om cybersäkerhet och cyberförsvar, inbegripet informationsutbytet mellan CERT-EU och Natos *Computer Incident Response Capability* (NCIRC), med full respekt för principerna om öppenhet, ömsesidighet och delaktighet samt de båda organisationernas beslutsautonomi,

16. ÄR MEDVETET om vikten av samarbete, när så är lämpligt, med den privata sektorn när det gäller övningar för informationsutbyte, och tillhandahållande av relevant expertis, samt betrodda lösningar och tjänster, till exempel när det gäller att stödja incidentinsatser och stärka situationsmedvetenheten mellan olika cybergrupper,

17. BETONAR vikten av säkra kommunikationskanaler för utbyte av säkerhetsskyddsklassificerad och känslig information, FRAMHÅLLER att det krävs ytterligare framsteg.

I detta avseende, och med beaktande av ovanstående, gäller följande:
Rådet

18. VÄRDESÄTTER kommissionens rekommendation om att bygga en gemensam cyberenhet som ett initiativ som måste övervägas vid vidareutvecklingen av EU:s ram för hantering av cyberkriser[13],

19. UPPMANAR EU och dess medlemsstater att fortsätta sina insatser för en mer heltäckande och effektiv EU-ram för hantering av cyberkriser, med utgångspunkt i befintliga mekanismer och de framsteg som redan gjorts, och att beakta potentialen hos initiativet för den gemensamma cyberenheten att komplettera dessa mekanismer genom en stegvis strategi, BETONAR att en stegvis, transparent och inkluderande process är avgörande för att öka förtroendet och att den därför är avgörande för den fortsatta utvecklingen av EU:s ram för hantering av cyberkriser; denna process bör respektera de befintliga rollerna, befogenheterna och mandaten för medlemsstaterna och EU:s institutioner, organ och byråer samt de principer som anges i dessa slutsatser, inbegripet proportionalitet, subsidiaritet, inkludering, komplementaritet, undvikande av dubbelarbete och konfidentialitet när det gäller information, BETONAR samtidigt att varje eventuellt deltagande i eller bidrag från medlemsstaterna till en potentiell gemensam cyberenhet är av frivillig karaktär,

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

20. BETONAR behovet av att fastställa lämpliga arbetsmetoder och lämplig styrning, i syfte att göra det möjligt för alla medlemsstater att delta i överläggningarna, utvecklingen och effektiva beslutsprocesser om EU:s ram för hantering av cyberkriser, inbegripet om det potentiella initiativet om en gemensam cyberenhet, MANAR till respekt av rådets befogenheter enligt fördragen och principen om lojalt samarbete,

21. UNDERSTRYKER att det är viktigt att identifiera och involvera alla relevanta cybergrupper inom EU och dess medlemsstater och samtidigt ta hänsyn till deras olika roller och ansvarsområden vid olika typer av storskaliga cyberincidenter och cyberkriser, UNDERSTRYKER att rådet har en avgörande roll, särskilt genom den övergripande arbetsgruppen för cyberfrågor, inom besluts- och samordningsfunktionen när det gäller den fortsatta utvecklingen av EU:s ram för hantering av cyberkriser, UPPMANAR därför medlemsstaterna, kommissionen, Europeiska utrikestjänsten, EU Intcen, CERT-EU, Enisa, Europol (EC3), Eurojust (EJCN), Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning samt företrädare för CSIRT-nätverket, EU CyCLONe, samarbetsgruppen för nät- och informationssäkerhet, Europeiska försvarsbyrån och relevanta Pesco-projekt samt andra möjliga intressenter att delta i denna process; frågan om en eventuell arbetsgrupp, som föreslås i kommissionens rekommendation, skulle kunna undersökas ytterligare genom att man säkerställer en lämplig representation av alla medlemsstater och agerar med politisk vägledning från rådet; den skulle fungera som ett tillfälligt forum som sammanför företrädare för alla relevanta cybergrupper i medlemsstaterna och inom EU; en sådan arbetsgrupp bör regelbundet rapportera om sin verksamhet och förelägga rådet eventuella förslag för diskussion, godkännande och ytterligare vägledning; dessutom skulle andra former av dialog inom och mellan olika grupper kunna inrättas, bland annat genom workshoppar, seminarier, gemensam utbildning och övningar,

22. UNDERSTRYKER den roll som Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning samt nätverket av nationella samordningscentrum har för den potentiella gemensamma cyberenheten, särskilt med tanke på dess roll för att avsevärt öka unionens tekniska kapacitet, tekniska lösningar, förmågor och kompetens på området cybersäkerhet,

23. UPPMANAR EU och dess medlemsstater att engagera sig i den fortsatta utvecklingen av EU:s ram för hantering av cyberkriser, bland annat genom att undersöka potentialen hos initiativet för en gemensam cyberenhet, genom att fastställa och definiera processen, inbegripet milstolpar och en tidsplan, samt klargöra målen och eventuella roller och ansvarsområden, FRAMHÅLLER behovet av att som en prioriterad fråga konsolidera befintliga nätverk och samspel inom varje grupp, samt att göra en grundlig kartläggning av eventuella luckor och behov vad gäller informationsutbytet inom och mellan cybergrupper liksom inom och mellan EU:s institutioner, organ och byråer, och därefter enas om eventuella primära mål och prioriteringar för en potentiell gemensam cyberenhet, BETONAR, utan att föregripa resultatet, behovet av att fokusera på att identifiera informationsutbytesbehoven för att skapa en gemensam situationsmedvetenhet bland alla berörda grupper; vid fastställandet av luckor och behov vad gäller informationsutbytet, inbegripet eventuell användning av virtuella plattformar, bör vederbörlig uppmärksamhet även fortsättningsvis ägnas åt säkra kommunikationskanaler för utbyte av säkerhetsskyddsklassificerade och känsliga uppgifter, och rådet BETONAR samtidigt vikten av att använda redan befintlig infrastruktur; införandet av en stegvis strategi är tänkt att bygga upp förtroendet och lägga grunden till eventuella ytterligare åtgärder för att förbättra beredskapen och det operativa samarbetet, KONSTATERAR att olika mål kan motivera olika lösningar och engagemang från olika företrädare för relevanta cybergrupper i EU och dess medlemsstater,

24. EFTERLYSER ytterligare överväganden om rättslig grund för den potentiella gemensamma cyberenheten under hela processen, inbegripet en bedömning av uppgifterna och rollerna i förhållande till Enisas uppgifter och roller i rekommendationen mot bakgrund av artikel 7 i Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019, EFTERLYSER ytterligare diskussion om enskilda delar av rekommendationen om den gemensamma cyberenheten, bland annat när det gäller idén om EU:s snabbinsatsteam för cybersäkerhet och EU:s incident- och krishanteringsplan för cybersäkerhet, BETONAR att en potentiell gemensam cyberenhet måste respektera de eventuella framtida deltagarnas befogenheter, mandat och rättsliga befogenheter,

25. UPPMANAR EU och dess medlemsstater att beakta potentialen hos ett initiativ för en gemensam cyberenhet, även ur EU:s institutioners, organs och byråers perspektiv, för att komplettera de pågående insatserna på medlemsstatsnivå, VÄLKOMNAR kommissionens avsikt att stärka resiliensen hos EU:s relevanta institutioner, organ och byråer genom sitt kommande förslag till förordning om gemensamma bindande regler för cybersäkerhet för EU:s institutioner, organ och byråer, och

26. UPPREPAR slutligen sitt åtagande att stärka cyberresiliensen och vidareutveckla EU:s ram för hantering av cyberkriser och KOMMER REGELBUNDET ATT FÖLJA framstegen och ge ytterligare vägledning om komplettering av EU:s ram för hantering av cyberkriser.