Europeiska unionens råd

Bryssel den 9 mars 2021
(OR. en)

6722/21

CYBER 55	RECH 86
JAI 227	COMPET 151
JAIEX 23	IND 52
EJUSTICE 25	COTER 25
COSI 39	ENFOPOL 80
DATAPROTECT 54	COPS 79
COPEN 103	MI 136
TELECOM 88	IXIM 43
PROCIV 21	POLMIL 25
CSC 85	HYBRID 10
CIS 35	CSCI 34
RELEX 168	POLGEN 33

I/A-PUNKTSNOT

från:	Rådets generalsekretariat
till:	Ständiga representanternas kommitté (Coreper)/rådet
Ärende:	Utkast till rådets slutsatser om EU:s strategi för cybersäkerhet för ett digitalt decennium

1. Den 16 december 2020 offentliggjorde kommissionen och unionens höga representant för utrikes frågor och säkerhetspolitik sitt gemensamma meddelande till Europaparlamentet och rådet med titeln *EU:s strategi för cybersäkerhet för ett digitalt decennium*[1]. Målet med denna nya strategi för cybersäkerhet är att stärka Europas kollektiva resiliens mot cyberhot och säkerställa att alla medborgare och företag kan dra full nytta av säkra och tillförlitliga tjänster och digitala verktyg.

[1] Dok. 14133/20.

2. Kommissionen och utrikestjänsten lade fram det gemensamma meddelandet vid den informella videokonferensen i den övergripande arbetsgruppen för cyberfrågor (*arbetsgruppen*) den 17 december 2020 och den 12 januari 2021. Vid arbetsgruppens informella videokonferens den 17 december 2020 tillkännagav det tillträdande portugisiska ordförandeskapet sin avsikt att utarbeta ett utkast till rådets slutsatser om EU:s strategi för cybersäkerhet för ett digitalt decennium.

3. Ordförandeskapet lade fram ett första utkast till rådets slutsatser vid den informella videokonferensen i arbetsgruppen den 2 februari 2021. Dessa slutsatser diskuterades därefter vid informella videokonferenser i arbetsgruppen den 9 februari 2021, den 19 februari 2021 och den 1 och 9 mars 2021.

4. Eftersom utkastet till slutsatser också innehåller en hänvisning till EU:s försvarspolitik (punkt 30) diskuterade gruppen för politiska och militära frågor den punkten i fråga vid sitt möte den 10 februari 2021.

5. Ett antal olika punkter rör den gemensamma utrikes- och säkerhetspolitiken (punkterna 1, 4, 7, 8, 9, 20, 23, 24, 26, 27, 28, 29, 30, 31, 32 och 33) och överlämnades därför till kommittén för utrikes- och säkerhetspolitik, som godkände dessa punkter vid sitt möte den 4 mars 2021.

6. Vid sin informella videokonferens den 9 mars 2021 nådde arbetsgruppen en överenskommelse om utkastet till rådets slutsatser enligt dok. 6722/21.

7. Mot bakgrund av ovanstående uppmanas Coreper att förelägga rådet utkastet till rådets slutsatser enligt bilagan och föreslå att det som en A-punkt på dagordningen antar detta utkast till slutsatser.

BILAGA

Utkast till rådets slutsatser om EU:s strategi för cybersäkerhet för ett digitalt decennium

EUROPEISKA UNIONENS RÅD,

SOM ERINRAR OM sina 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[2],

– förvaltning av internet[3],

– det gemensamma meddelandet av den 20 november 2017 till Europaparlamentet och rådet – *Resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU*[4],

– uppbyggnad av kapacitet och förmågor på cybersäkerhetsområdet i EU[5],

– 5G:s betydelse för den europeiska ekonomin och behovet av att minska säkerhetsriskerna i samband med 5G[6],

– framtiden för ett starkt digitaliserat Europa efter 2020: främjande av digital och ekonomisk konkurrenskraft i unionen och digital sammanhållning[7],

– kompletterande insatser för förstärkning av motståndskraft och motverkande av hybridhot[8],

– att forma Europas digitala framtid[9],

---

2 Dok. 12109/13.
3 Dok. 16200/14.
4 Dok. 14435/17 + COR 1.
5 Dok. 7737/19.
6 Dok. 14517/19.
7 Dok. 9596/19.
8 Dok. 14972/19.
9 Dok. 8711/20.

– digital diplomati[10],

– stärkande av motståndskraften och motverkande av hybridhot, inbegripet desinformation i samband med covid-19-pandemin[11],

– cyberdiplomati[12],

– EU:s samordnade insatser vid storskaliga cyberincidenter och cyberkriser[13],

– en ram för en gemensam diplomatisk respons från EU mot skadlig it-verksamhet (”verktygslåda för cyberdiplomati”)[14],

– EU-riktlinjer för extern kapacitetsuppbyggnad på cyberområdet[15],

– en återhämtning som främjar omställningen till en mer dynamisk, motståndskraftig och konkurrenskraftig europeisk industri[16],

– cybersäkerheten för uppkopplade enheter[17],

– att stärka Europas system för cyberresiliens och främja en konkurrenskraftig och innovativ cybersäkerhetsbransch[18],

och om rådets resolution om kryptering: Säkerhet genom kryptering och säkerhet trots kryptering[19],

---

10 Dok. 12804/20.
11 Dok. 14064/20.
12 Dok. 6122/15 + COR 1.
13 Dok. 10086/18.
14 Dok. 10474/17.
15 Dok. 10496/18.
16 Dok. 13004/20.
17 Dok. 13629/20.
18 Dok. 14540/16.
19 Dok. 13084/1/20 REV 1.

– samt medlemsstaternas gemensamma förklaring av den 15 oktober 2020 om inrättandet av nästa generations molntjänster för företag och den offentliga sektorn i EU,

SOM ERINRAR OM Europeiska rådets slutsatser av den 1–2 oktober 2020 om covid-19, den inre marknaden, industripolitik, digitala frågor och yttre förbindelser[20] samt om Europeiska rådets slutsatser av den 20 juni 2019 om desinformation och hybridhot och en ny strategisk agenda 2019–2024[21],

SOM ERINRAR OM den globala strategin för Europeiska unionens utrikes- och säkerhetspolitik med titeln *Delade visioner, gemensamma åtgärder: Ett starkare Europa*av den 28 juni 2016,

SOM ERINRAR OM Europeiska kommissionens meddelanden om att forma Europas digitala framtid av den 19 december 2020[22] och om strategin för EU:s säkerhetsunion av den 24 juli 2020[23],

SOM ERINRAR OM det gemensamma meddelandet från Europeiska kommissionen och den höga representanten av den 2 december 2020 om en ny agenda mellan EU och USA för globala förändringar[24],

1. FRAMHÅLLER att cybersäkerhet är avgörande för att bygga ett motståndskraftigt, grönt och digitalt Europa och VÄLKOMNAR det gemensamma meddelandet till Europaparlamentet och rådet med titeln *EU:s strategi för cybersäkerhet för ett digitalt decennium*, som beskriver den nya ramen för EU:s åtgärder på området ”resiliens, teknisk suveränitet och ledarskap” och hur unionens medborgare, företag och institutioner ska skyddas från cyberincidenter och cyberhot, samtidigt som man stärker enskilda personers och organisationers förtroende för EU:s förmåga att främja säkra och tillförlitliga nätverks- och informationssystem, infrastruktur och konnektivitet, samt till att främja och skydda en global, öppen, fri, stabil och säker cyberrymd som bygger på mänskliga rättigheter, grundläggande friheter, demokrati och rättsstatsprincipen,

---

20 Dok. EUCO 13/20.
21 Dok. EUCO 9/19.
22 19.2.2020, COM(2020) 67 final.
23 24.7.2020, COM(2020) 605 final.
24 2.12.2020, JOIN(2020) 22 final.

2. ÄR MEDVETET OM att covid-19-pandemin har gjort att det ökade behovet av förtroende för verktyg och system för informations- och kommunikationsteknik (IKT) och deras säkerhet har hamnat i framkant i vårt dagliga liv, BETONAR att cybersäkerhet och ett globalt och öppet internet är avgörande för den offentliga förvaltningens och institutionernas funktion på både nationell nivå och EU-nivå och för vårt samhälle och ekonomin som helhet,

3. BETONAR behovet av att öka medvetenheten om cyberfrågor på politisk och strategisk beslutsnivå genom att förse beslutsfattarna med relevant kunskap och information och UNDERSTRYKER behovet av att öka allmänhetens medvetenhet och främja cyberhygien,

4. EFTERLYSER främjande och skydd av EU:s grundläggande värden demokrati, rättsstatsprincipen, mänskliga rättigheter och grundläggande friheter, inbegripet rätten till yttrande- och informationsfrihet, mötes- och föreningsfrihet och rätten till integritet i cyberrymden, VÄLKOMNAR i detta avseende ytterligare uthålliga ansträngningar för att skydda människorättsförsvarare, civilsamhället och personer inom den akademiska världen som arbetar med sådana frågor som cybersäkerhet, dataskydd, övervakning och censur online genom utarbetande av ytterligare praktiska vägledningar, främjande av bästa praxis och intensifiering av EU:s insatser för att förhindra missbruk av ny teknik, bland annat genom diplomatiska åtgärder, vid behov, liksom exportkontroll av sådan teknik, BETONAR i detta sammanhang vikten av EU:s handlingsplan för mänskliga rättigheter och demokrati 2020–2024 och dess riktlinjer om mänskliga rättigheter vad gäller yttrandefrihet online och offline,

5. FRAMHÅLLER att uppnåendet av strategiskt oberoende, samtidigt som man bevarar en öppen ekonomi, är ett centralt mål för unionen för att unionen själv ska kunna bestämma sin ekonomiska bana och sina ekonomiska intressen; detta inbegriper att stärka förmågan att göra självständiga val på cybersäkerhetsområdet i syfte att stärka EU:s digitala ledarskap och strategiska kapacitet, ERINRAR OM att detta inbegriper att kartlägga och minska strategiska beroendeförhållanden och öka resiliensen i de känsligaste industriella ekosystemen och specifika områden, UNDERSTRYKER att detta kan innebära att produktions- och leveranskedjorna diversifieras, att investeringar och produktion i Europa främjas och lockas hit, och att man undersöker alternativa lösningar och cirkulära modeller samt främjar ett brett industriellt samarbete mellan medlemsstaterna,

6. BETONAR, med tanke på bristen på digitala färdigheter och cybersäkerhetskompetens hos arbetskraften, vikten av att tillgodose efterfrågan på utbildad arbetskraft på området för digital teknik och cybersäkerhet, särskilt genom att utveckla, behålla och locka till sig de största begåvningarna, till exempel genom utbildning för att kunna digitalisera vårt samhälle på ett cybersäkert sätt, UPPMUNTRAR kvinnors och flickors ökade deltagande i utbildning inom naturvetenskap, teknik, ingenjörsvetenskap, matematik samt i kompetensutveckling och omskolning inom IKT-jobb vad gäller digitala färdigheter som ett sätt att överbrygga den digitala klyftan mellan könen,

7. 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 sitt åtagande att lösa internationella tvister i cyberrymden med fredliga medel och att alla EU:s diplomatiska insatser som en prioritering bör inriktas på att främja säkerhet och stabilitet i cyberrymden genom ökat internationellt samarbete och att minska risken för missförstånd, upptrappning och konflikter till följd av IKT-incidenter och STÖDER ytterligare utveckling och operationalisering av förtroendeskapande åtgärder på regional och internationell nivå, UPPREPAR FN:s generalförsamlings uppmaning, som antogs enhälligt, att FN:s medlemsstater när de använder IKT ska vägledas av rekommendationerna i rapporterna från FN:s grupp med regeringsexperter på informations- och telekommunikationsområdet och BEKRÄFTAR tillämpningen av internationell rätt, särskilt FN-stadgan i dess helhet, i cyberrymden,

8. BEKRÄFTAR att ytterligare utveckling av normer och standarder inom unionen genom en flerpartsstrategi är avgörande för att i grunden forma internationella normer och standarder på områdena för ny teknik och den tekniska och logiska infrastruktur som är nödvändig för den allmänna tillgängligheten och integriteten hos den offentliga kärnan i Internet, så att dessa överensstämmer med universella värden och EU:s värden; detta kommer att säkerställa att internet förblir globalt, öppet, fritt, stabilt och säkert och att användningen och utvecklingen av digital teknik respekterar de mänskliga rättigheterna och att användningen av denna teknik är laglig, säker och etisk, NOTERAR den kommande standardiseringsstrategin och ÅTAR sig att bedriva ett aktivt och samordnat utåtriktat arbete för att främja EU:s ledarskap och EU:s mål på internationell nivå, inbegripet i olika internationella standardiseringsorgan och genom samarbete med likasinnade partner, civilsamhället, den akademiska världen och den privata sektorn,

9. STÖDER HELHJÄRTAT flerpartsmodellen för förvaltning av internet och cybersäkerhet och åtar sig att stärka de regelbundna och strukturerade kontakterna med berörda parter, inbegripet den privata sektorn, en akademiska världen och civilsamhället, bland annat inom ramen för Paris Call for Trust and Security in Cyberspace (”Parisuppropet för tillit och säkerhet i cyberrymden”), FRÄMJAR en samhällsomfattande och lika tillgång till internet till rimliga kostnader som överbryggar de digitala klyftorna och, i synnerhet, egenmakt för kvinnor och flickor och personer i utsatta eller marginaliserade situationer, både när det gäller utarbetande av politik och användning av internet,

10. FRAMHÅLLER behovet av att inkludera cybersäkerhet i digitala investeringar och initiativ under de kommande åren och behovet av att successivt bidra till lika villkor inom cybersäkerhet samt NOTERAR kommissionens plan att öka de offentliga utgifterna och stimulera privata investeringar på cybersäkerhetsområdet, UNDERSTRYKER vikten av små och medelstora företag i cybersäkerhetsekosystemet och ÄR MEDVETET OM de relevanta finansiella instrument som finns tillgängliga för att stödja ett starkt fokus på cybersäkerhet inom den digitala omvandlingen under den fleråriga budgetramen 2021–2027 samt inom faciliteten för återhämtning och resiliens,

11. SER FRAM EMOT ett snabbt genomförande av förordningen om Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och nätverket av nationella samordningscentrum, inbegripet ett snabbt inrättande och idrifttagande av Europeiska kompetenscentrumet för cybersäkerhet i Bukarest; ett snabbt antagande av dess agenda kommer att bidra till att maximera effekterna av investeringar för att stärka unionens ledarskap och strategiska oberoende på området cybersäkerhet och stödja teknisk kapacitet och kompetens samt öka unionens globala konkurrenskraft med bidrag från näringslivet och den akademiska världen inom cybersäkerhetsområdet, inbegripet små och medelstora företag och forskningscentrum, som kommer att gynnas av ett mer systematiskt, inkluderande och strategiskt samarbete, med beaktande av sammanhållningen i unionen och alla dess medlemsstater,

12. VÄLKOMNAR det pågående arbete som leds av Enisa, tillsammans med medlemsstaterna och berörda parter, för att förse EU med certifieringssystem för IKT-produkter, IKT-tjänster och IKT-processer, vilket bör bidra till att höja den övergripande cybersäkerhetsnivån på den digitala inre marknaden, SER i detta sammanhang FRAM EMOT unionens löpande arbetsprogram i syfte att utveckla EU:s system för cybersäkerhetscertifiering inom ramen för cybersäkerhetsakten, KONSTATERAR i detta sammanhang EU:s centrala roll när det gäller att utarbeta standarder som kan forma cybersäkerhetsområdet och som bidrar till att säkerställa rättvis konkurrens inom EU och på den globala arenan, främja marknadstillträde och hantera säkerhetsrisker samtidigt som man säkerställer att EU:s rättsliga ram är tillämplig,

13. UPPREPAR vikten av att bedöma behovet på lång sikt av en övergripande lagstiftning, som också specificerar de nödvändiga villkoren för utsläppande på marknaden, för att hantera alla relevanta aspekter av cybersäkerheten för uppkopplade enheter, till exempel tillgänglighet, integritet och konfidentialitet, VÄLKOMNAR i detta avseende en diskussion för att undersöka tillämpningsområdet för sådan lagstiftning och dess kopplingar till ramverket för cybersäkerhetscertifiering enligt cybersäkerhetsakten i syfte att höja säkerhetsnivån på den digitala inre marknaden, UNDERSTRYKER att cybersäkerhetskrav bör fastställas i enlighet med relevant unionslagstiftning, inbegripet cybersäkerhetsakten, den nya lagstiftningsramen, förordningen om europeisk standardisering och en eventuell framtida övergripande lagstiftning, för att undvika tvetydighet och fragmentering i lagstiftningen,

14. ÄR MEDVETET OM vikten av en övergripande och horisontell strategi för cybersäkerhet i unionen, samtidigt som medlemsstaternas befogenheter och behov respekteras fullt ut, samt av vikten av kontinuerligt stöd till tekniskt bistånd och samarbete för att bygga upp medlemsstaternas kapacitet, NOTERAR, med beaktande av cyberhotbildens utveckling, det nya förslaget till direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen som bygger på NIS-direktivet och upprepar sitt stöd för att stärka och harmonisera nationella cybersäkerhetsramar samt för kontinuerligt samarbete mellan medlemsstaterna, BETONAR dessutom behovet av anpassning och harmonisering av sektorsspecifik lagstiftning på detta område,

15. NOTERAR kommissionens förslag om att stödja medlemsstaterna i deras arbete med att inrätta och stärka säkerhetscentrum i syfte att bygga upp ett nätverk av sådana centrum omfattande hela EU, för att ytterligare övervaka och förutse signaler som tyder på möjliga angrepp på nätverk, SER i detta sammanhang FRAM EMOT kommissionens detaljerade planer för nätverket av säkerhetscentrum, och respekterar samtidigt medlemsstaternas befogenheter, ERINRAR OM de insatser som gjorts av medlemsstaterna, med stöd av EU, för att inrätta sektoriella, nationella och regionala CSIRT-enheter och nationella eller europeiska informations- och analyscentraler som en del av ett effektivt nätverk av cybersäkerhetspartnerskap i unionen, SER FRAM EMOT att utforska detta nätverks potential att stärka säkerhetscentrumen samt deras komplementaritet och samordning med befintliga nätverk och aktörer (framför allt CSIRT-nätverket) i syfte att främja en effektiv, säker och tillförlitlig informationsutbyteskultur, BETONAR att denna process kommer att bygga på det arbete som utförts inom ramen för initiativ för artificiell intelligens och högpresterande datorsystem och av europeiska digitala innovationsknutpunkter,

16. NOTERAR den möjliga utvecklingen av ett säkert system för konnektivitet som bygger på den europeiska kvantkommunikationsinfrastrukturen (EuroQCI) och Europeiska unionens statliga satellitkommunikation (Govsatcom) och KONSTATERAR att all framtida utveckling bör baseras på en robust cybersäkerhetsram och ta hänsyn till hela infrastrukturen för elektronisk kommunikation såsom nätverkssystem för rymd-, land- och undervattenskommunikation,

17. SER FRAM EMOT diskussionerna med kommissionen, Enisa, EU:s två DNS-rotserveroperatörer och flerpartssamhället för att bedöma de två rotserveroperatörernas roll när det gäller att garantera att internet förblir globalt tillgängligt och icke-fragmenterat, VÄLKOMNAR ytterligare diskussioner om kommissionens avsikt att utveckla en alternativ tjänst på EU-nivå för tillgång till det globala internet (DNS4EU-initiativet), baserad på en transparent modell som följer de senaste standarderna och reglerna för säkerhet, dataskydd och integritetsskydd, inbyggt och som standard, i syfte att bidra till ökad resiliens och samtidigt upprätthålla och förbättra den internationella konnektiviteten för alla medlemsstater,

18. ERKÄNNER behovet av en gemensam insats från kommissionen och medlemsstaterna för att påskynda införandet av centrala internetstandarder, inklusive IPv6, och väletablerade internetsäkerhetsstandarder, eftersom dessa bidrar till att höja den övergripande nivån av säkerhet, resiliens, öppenhet och interoperabilitet för det globala internet, och samtidigt ökar konkurrenskraften hos EU:s industri, i synnerhet hos internetinfrastrukturförvaltarna,

19. BETONAR vikten av en samordnad strategi samt utveckling och genomförande av effektiva åtgärder på nationell nivå för att stärka cybersäkerheten i 5G-nät, STÖDER nästa steg i fråga om cybersäkerhet i 5G-nät, som presenteras i bilagan till EU:s strategi för cybersäkerhet och som bygger på resultaten av rapporten om konsekvenserna av kommissionens rekommendation om säkerheten i 5G-nät,till exempel när det gäller fastställandet av en långsiktig och övergripande strategi som omfattar hela värdekedjan och ekosystemet för 5G, UPPMANAR ENTRÄGET medlemsstaterna, EU-institutionerna och andra berörda aktörer att fortsätta med sin periodiska inventering, tillsammans med utbytet av information och bästa praxis inom ramen för NIS-samarbetsgruppens särskilda arbete med 5G-cybersäkerhet, och regelbundet rapportera till rådet om de framsteg som gjorts, i syfte att ytterligare stärka den samordnade strategin för säkerheten i 5G-nät, FRAMHÅLLER sitt starka engagemang när det gäller att tillämpa och snabbt slutföra genomförandet av åtgärderna i EU:s 5G-verktygslåda och att fortsätta insatserna för att garantera 5G-nätens säkerhet och utvecklingen av framtida generationer av nätverk, och betonar samtidigt medlemsstaternas ansvar för skyddet av den nationella säkerheten; det nära samarbetet mellan medlemsstaterna, kommissionen och Enisa om säkerheten i 5G-nät skulle kunna tjäna som ett exempel för andra frågor på cybersäkerhetsområdet, samtidigt som medlemsstaternas befogenheter och subsidiaritets- och proportionalitetsprinciperna respekteras,

20. INSER betydelsen av att ytterligare integrera cybersäkerhet i EU:s krishanteringsmekanismer och testa dessa genom relevanta övningar och FRAMHÅLLER vikten av att förbättra samarbetet och informationsutbytet mellan olika cybergrupper inom EU och av att koppla samman befintliga initiativ, strukturer och förfaranden (däribland IPCR, CSIRT-nätverket, NIS-samarbetsgruppen, CyCLONe, Europeiska it-brottscentrumet, EU Intcen och andra relevanta EU-organ) vid storskaliga och gränsöverskridande cyberincidenter och cyberhot, BEAKTAR de framsteg som redan gjorts på detta område och SER FRAM EMOT kommissionens förslag om processen, etappmålen och tidsplanen för att fastställa den gemensamma cyberenheten i syfte att rationalisera EU:s ram för hantering av cyberkriser, ge den mervärde och ett tydligt fokus, bland annat genom beredskap, kollektiv situationsmedvetenhet, förstärkning av den samordnade responsen och övningar, på ett transparent och successivt sätt, samtidigt som dubbelarbete och överlappningar undviks och medlemsstaternas befogenheter respekteras,

21. BETONAR såväl vikten av att främja samarbete och informationsutbyte mellan relevanta cybersäkerhetsaktörer och behöriga myndigheter på området säkerhet och straffrätt, t.ex. brottsbekämpande och rättsliga myndigheter, som behovet av att utöka och förbättra dessa myndigheters kapacitet att utreda och lagföra it-brottslighet och att främja internationella förhandlingar och EU-regler om gränsöverskridande tillgång till elektroniska bevis; oberoende av dagens tekniska miljö är det viktigt att bevara de behöriga myndigheternas befogenheter på området säkerhet och straffrätt genom laglig tillgång, som gör att de kan utföra sina uppgifter i enlighet med vad som föreskrivs och är tillåtet enligt lag; sådana lagar som föreskriver brottsbekämpande befogenheter måste alltid fullt ut respektera vederbörliga förfaranden och andra skyddsåtgärder samt grundläggande rättigheter, särskilt rätten till respekt för privatlivet och kommunikation och rätten till skydd av personuppgifter,

22. BEKRÄFTAR sitt stöd för utveckling, genomförande och användning av stark kryptering som ett nödvändigt medel för att skydda de grundläggande rättigheterna och den digitala säkerheten för enskilda, regeringar, industrin och samhället och ERKÄNNER samtidigt behovet av att säkerställa att de behöriga myndigheterna på området säkerhet och straffrätt, däribland brottsbekämpande och rättsliga myndigheter, kan utöva sina lagliga befogenheter, både online och offline, för att skydda våra samhällen och medborgare; behöriga myndigheter måste kunna få tillgång till uppgifter på ett lagligt och målinriktat sätt, med full respekt för grundläggande rättigheter och relevant dataskyddslagstiftning, samtidigt som cybersäkerheten upprätthålls. BETONAR att man i alla de åtgärder som vidtas noga måste väga dessa intressen mot principerna om nödvändighet, proportionalitet och subsidiaritet,

23. STÖDJER och FRÄMJAR konventionen om it-brottslighet (Budapestkonventionen) och det pågående arbetet med det andra tilläggsprotokollet till konventionen; rådet fortsätter dessutom att delta i multilaterala utbyten om cyberbrottslighet, inbegripet i processer som rör Europarådet, FN:s drog- och brottsbekämpningsbyrå (UNODC) och FN:s kommission för brottsförebyggande arbete och straffrätt, i syfte att säkerställa ett förstärkt internationellt samarbete för bekämpning av it-brottslighet, inbegripet utbyte av bästa praxis och teknisk kunskap samt stöd till kapacitetsuppbyggnad, samtidigt som mänskliga rättigheter och grundläggande friheter respekteras, främjas och skyddas,

24. ÄR MEDVETET OM vikten av strategiskt underrättelsesamarbete om cyberhot och cyberverksamheter, även om den nationella säkerheten också i fortsättningen förblir varje medlemsstats eget ansvar, och UPPMANAR medlemsstaterna att genom sina behöriga myndigheter fortsätta att bidra till det arbete som utförs av EU Intcen i egenskap av EU:s nav för situationsmedvetenhet och hotbildsbedömningar i cyberfrågor, och att undersöka förslaget om ett eventuellt inrättande av medlemsstaternas arbetsgrupp för cyberunderrättelser i syfte att stärka Intcens särskilda kapacitet på detta område, på grundval av frivilliga underrättelsebidrag från medlemsstaterna och utan att det påverkar deras befogenheter,

25. FRAMHÅLLER vikten av en robust och konsekvent säkerhetsram för att skydda all EU-personal, EU:s samtliga uppgifter, kommunikationsnätverk och beslutsprocesser på grundval av övergripande, konsekventa och enhetliga regler; detta bör i synnerhet ske genom att man stärker resiliensen och EU:s säkerhetskultur vad avser cyberhot samt säkerheten för säkerhetsskyddsklassificerade och icke-sekretessbelagda EU-nätverk samtidigt som man säkerställer en adekvat styrning och att tillräckliga resurser och tillräcklig kapacitet ställs till förfogande, bland annat i samband med förstärkningen av CERT-EU:s mandat, VÄLKOMNAR i detta sammanhang de pågående diskussionerna om fastställandet av gemensamma regler för informationssäkerhet med vederbörlig hänsyn till rådets säkerhetsbestämmelser om skydd av säkerhetsskyddsklassificerade EU-uppgifter samt fastställandet av gemensamma bindande regler om cybersäkerhet för alla EU:s institutioner, organ och byråer,

26. ÅTAR SIG att MED UTGÅNGSPUNKT i EU:s insatser inom cyberdiplomati öka ändamålsenligheten och effektiviteten hos verktygslådan för cyberdiplomati, och SER FRAM EMOT att fördjupa diskussionerna om dess tillämpningsområde och användning utifrån de lärdomar som dragits av tillämpningen av detta instrument till dags dato; dessa diskussioner bör bidra till att främja säkerhet på internationell nivå genom att främja dialog och en gemensam syn på cybersäkerhetsfrågor, stärka förebyggande, stabilitet och samarbete samt främja förtroende och kapacitetsuppbyggnad, och vid behov tillämpa restriktiva åtgärder, i syfte att förebygga, avskräcka, motverka och bemöta skadlig cyberverksamhet inriktad på EU:s och dess medlemsstaters integritet och säkerhet, och därigenom bidra till internationell säkerhet och stabilitet och befästa EU:s arbete på cyberområdet, med full respekt för nationella befogenheter och rättigheter; särskild uppmärksamhet bör ägnas åt att förebygga och motverka cyberattacker med systemiska effekter som kan påverka våra leveranskedjor, vår kritiska infrastruktur och våra samhällsviktiga tjänster, demokratiska institutioner och processer och undergräva vår ekonomiska säkerhet, inbegripet cyberbaserade stölder av immateriella rättigheter; medlemsstaterna och EU-institutionerna bör också ytterligare reflektera över kopplingen mellan EU:s ram för hantering av cyberkriser, verktygslådan för cyberdiplomati och bestämmelserna i artikel 42.7 i EU-fördraget och artikel 222 i EUF-fördraget, särskilt genom scenariebaserat arbete för att skapa en samsyn om de praktiska formerna för genomförandet av artikel 42.7 i EU-fördraget,

27. ÄR MEDVETET OM vikten av att stärka samarbetet med internationella organisationer och partnerländer för att främja en gemensam förståelse av cyberhotbilden, utveckla dialoger och samarbetsmekanismer, vid behov identifiera samarbetsinriktade diplomatiska insatser samt förbättra informationsutbytet, bland annat genom utbildning och övningar, FRAMHÅLLER särskilt att ett starkt transatlantiskt partnerskap på cybersäkerhetsområdet bidrar till vår gemensamma säkerhet och stabilitet och vårt välstånd och NOTERAR bestämmelserna om cybersäkerhetssamarbete i handels- och samarbetsavtalet mellan EU och Förenade kungariket, 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 och upprepar vikten av ett utökat, ömsesidigt stärkande och gynnsamt samarbete genom utbildning, övningar och samordnade insatser mot skadlig cyberverksamhet, med full respekt för de båda organisationernas beslutsautonomi och förfaranden och på grundval av principerna om öppenhet, ömsesidighet och delaktighet,

28. ÅTAR SIG, i syfte att bidra till en global, öppen, fri, stabil och säker cyberrymd, som är av allt större betydelse för vårt samhälles fortsatta välstånd, tillväxt, säkerhet, välfärd, konnektivitet och integritet, att kontinuerligt engagera sig i normgivningsprocesser i internationella organisationer, särskilt inom ramen för processer med anknytning till FN:s första utskott, främja och bidra till erkännandet av tillämpningen av internationell rätt i cyberrymden och ansluta sig till normer, regler och principer för ett ansvarsfullt statligt agerande i cyberrymden, inbegripet genom att främja ett snabbt införande av ett handlingsprogram för staters ansvarsfulla agerande i cyberrymden som en konstruktiv, inkluderande och konsensusbaserad uppföljning av de båda pågående processerna inom ramen för FN:s grupp med regeringsexperter på informations- och telekommunikationsområdet och den öppna arbetsgruppen,

29. ERINRAR OM sitt starka engagemang för effektiv multilateralism och en regelbaserad världsordning med FN i centrum och sin beslutsamhet att stärka samarbetet och samordningen med internationella och regionala organisationer, närmare bestämt FN-systemet, Nato, Europarådet, OSSE, OECD, AU, OAS, Asean, ARF, GCC och Arabförbundet, när det gäller diskussioner om cyberrelaterade frågor samt en fortsättning på och utvidgning av strukturerade EU-dialoger och samråd på cyberområdet med tredjeländer, BETONAR sitt aktiva stöd till FN, särskilt när det gäller dess Agenda 2030, inbegripet målen för hållbar utveckling, och VÄLKOMNAR FN:s generalsekreterares färdplan för digitalt samarbete och FN:s generalsekreterares agenda för nedrustning som främjar ansvarsskyldighet och anslutning till normer i cyberrymden och bidrar till förebyggande och fredlig lösning av konflikter som härrör från skadlig verksamhet i cyberrymden, VÄLKOMNAR förslaget från den höga representanten för utrikes frågor och säkerhetspolitik om att inrätta ett informellt EU-nätverk för cyberdiplomati för att utveckla både EU:s och medlemsstaternas engagemang och sakkunskap i internationella cyberfrågor i syfte att stärka den samordnade uppsökande verksamheten,

30. SER FRAM EMOT det kommande förslaget till en översyn av ramen för politiken för cyberförsvar och ÅTAR SIG att fortsätta ansträngningarna för att stärka cybersäkerhets- och cyberförsvarsdimensionerna i syfte att säkerställa att dessa fullt ut integreras i det bredare säkerhets- och försvarsområdet, särskilt inom ramen för arbetet med den strategiska kompassen, ANSER att det kommande dokumentet *Military Vision and Strategy on Cyberspace as a Domain of Operations* (militär vision och strategi för cyberrymden som operativt område) kommer att bidra till att främja dessa diskussioner, VÄLKOMNAR Europeiska försvarsbyråns initiativ att främja samarbete mellan militära incidenthanteringsorganisationer och STÖDER de insatser som gjorts för att stärka civil-militära synergier och civil-militär samordning när det gäller cyberförsvar och cybersäkerhet, inbegripet rymdrelaterade aspekter, bland annat genom de särskilda Pesco-projekten,

31. VÄLKOMNAR förslaget om att utarbeta en EU-agenda för extern kapacitetsuppbyggnad på cyberområdet, förslaget om att inrätta en EU-nämnd för kapacitetsuppbyggnad på cyberområdet och inrättandet och genomförandet av EU CyberNet (EU:s nätverk för kapacitetsuppbyggnad på cyberområdet) i syfte att öka den globala cyberresiliensen och cyberkapaciteten, VÄLKOMNAR i detta sammanhang samarbetet med medlemsstaterna samt med partner inom den offentliga och privata sektorn, särskilt det globala forumet för it-expertis (GFCE) och andra relevanta internationella organ, för att säkerställa samordning och undvika dubbelarbete, UPPMANAR särskilt till samarbete med partner på västra Balkan och i EU:s östra och södra grannskap,

32. ÅTAR SIG att hjälpa partnerländer att ta itu med den växande utmaningen med skadlig cyberverksamhet, särskilt sådan som skadar utvecklingen av deras ekonomier, samhällen och de demokratiska systemens integritet och säkerhet, bland annat i linje med insatserna inom ramen för den europeiska handlingsplanen för demokrati, för att säkerställa att alla länder kan dra nytta av de sociala, ekonomiska och politiska fördelarna med internet och användningen av teknik,

33. UPPMANAR kommissionen och den höga representanten för utrikes frågor och säkerhetspolitik att upprätta en detaljerad genomförandeplan där prioriteringarna och tidsplanen för planerade åtgärder fastställs, i syfte att säkerställa utarbetandet, genomförandet och övervakningen av förslag som läggs fram inom ramen för EU:s strategi för cybersäkerhet, och med beaktande av att vissa initiativ är fleråriga, kommer ATT ÖVERVAKA framstegen med genomförandet av dessa slutsatser genom en handlingsplan som regelbundet kommer att ses över och uppdateras av rådet i nära samarbete med Europeiska kommissionen och den höga representanten.