Rådet for
Den Europæiske Union

Bruxelles, den 9. marts 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-PUNKTSNOTE

fra:	Generalsekretariatet for Rådet
til:	De Faste Repræsentanters Komité/Rådet
Vedr.:	Udkast til Rådets konklusioner om EU's strategi for cybersikkerhed for det digitale årti

1. Den 16. december 2020 offentliggjorde Kommissionen og Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik deres fælles meddelelse til Europa-Parlamentet og Rådet: "EU's strategi for cybersikkerhed for det digitale årti"[1] Den nye strategi for cybersikkerhed tilsigter at styrke Europas kollektive modstandsdygtighed over for cybertrusler og sikre, at alle borgere og virksomheder fuldt ud kan drage fordel af troværdige og pålidelige tjenester og digitale værktøjer.

[1] 14133/20.

2. Kommissionen og EU-Udenrigstjenesten fremlagde den fælles meddelelse på den uformelle videokonference i Den Horisontale Gruppe vedrørende Cyberspørgsmål (Cybergruppen) den 17. december 2020 og den 12. januar 2021. På Cybergruppens uformelle videokonference den 17. december 2020 meddelte det kommende portugisiske formandskab, at det agter at udarbejde et udkast til Rådets konklusioner om EU's strategi for cybersikkerhed for det digitale årti.

3. Formandskabet fremlagde et første udkast til Rådets konklusioner på Cybergruppens uformelle videokonference den 2. februar 2021. Disse konklusioner blev efterfølgende drøftet på Cybergruppens uformelle videokonference den 9. februar 2021, den 19. februar 2021, den 1. marts og den 9. marts 2021.

4. Da udkastet til konklusioner også indeholder en henvisning til EU's forsvarspolitik (punkt 30), drøftede Den Politisk-Militære Gruppe (PMG) det relevante punkt på sit møde den 10. februar 2021.

5. Diverse punkter vedrører den fælles udenrigs- og sikkerhedspolitik (punkt 1, 4, 7, 8, 9, 20, 23, 24, 26, 27, 28, 29, 30, 31, 32 og 33) og blev derfor forelagt Den Udenrigs- og Sikkerhedspolitiske Komité, som godkendte disse punkter på sit møde den 4. marts 2021.

6. På den uformelle videokonference den 9. marts 2021 nåede Cybergruppen til enighed om udkastet til Rådets konklusioner, jf. dok. 6722/21.

7. På baggrund af ovenstående opfordres De Faste Repræsentanters Komité til at forelægge Rådet udkastet til Rådets konklusioner, som det foreligger i bilaget, og henstille til Rådet, at det som A-punkt på dagsordenen vedtager udkastet til konklusioner.

BILAG

Udkast til Rådets konklusioner om EU's strategi for cybersikkerhed for det digitale årti

RÅDET FOR DEN EUROPÆISKE UNION,

SOM MINDER OM sine konklusioner om

– den fælles meddelelse af 25. juni 2013 til Europa-Parlamentet og Rådet om en EU-strategi for cybersikkerhed: "Et åbent, sikkert og beskyttet cyberspace"[2]

– internetforvaltning[3]

– den fælles meddelelse af 20. november 2017 til Europa-Parlamentet og Rådet: "Modstandsdygtighed, afskrækkelse og forsvar: opbygning af en stærk cybersikkerhed for EU"[4]

– opbygning af cybersikkerhedskapacitet i EU[5]

– betydningen af 5G for den europæiske økonomi og behovet for at afbøde de sikkerhedsrisici, der er forbundet med 5G[6]

– fremtiden for et højdigitaliseret Europa efter 2020: "Styrke den digitale og økonomiske konkurrenceevne i hele Unionen og den digitale samhørighed"[7]

– supplerende tiltag for at styrke modstandsdygtighed og imødegå hybride trusler[8]

– Europas digitale fremtid i støbeskeen[9]

---

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

– digitalt diplomati[10]

– styrkelse af modstandsdygtigheden og imødegåelse af hybride trusler, herunder desinformation i forbindelse med covid-19-pandemien[11]

– cyberdiplomati[12]

– en koordineret EU-reaktion på væsentlige cybersikkerhedshændelser og -kriser[13]

– en ramme for EU's fælles diplomatiske reaktion på ondsindede cyberaktiviteter ("cyberdiplomatisk værktøjskasse")[14]

– EU's retningslinjer for opbygning af ekstern cyberkapacitet[15]

– en genopretning, der fremmer omstillingen til en mere dynamisk, modstandsdygtig og konkurrencedygtig europæisk industri[16]

– cybersikkerheden ved forbundet udstyr[17]

– styrkelse af Europas system for modstandsdygtighed over for cyberangreb og fremme af en konkurrencedygtig og innovativ cybersikkerhedsindustri[18]

– og Rådets resolution om kryptering – Sikkerhed ved hjælp af kryptering og på trods heraf[19]

---

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

– og medlemsstaternes erklæring af 15. oktober 2020 om opbygning af den næste generation af clouds til virksomheder og den offentlige sektor i EU,

SOM MINDER OM Det Europæiske Råds konklusioner af 1.-2. oktober 2020 om covid-19, det indre marked, industripolitik og det digitale samt eksterne forbindelser[20] og konklusionerne af 20. juni 2019 om desinformation og hybride trusler og om en ny strategisk dagsorden 2019-2024[21],

SOM MINDER OM den globale strategi for Den Europæiske Unions udenrigs- og sikkerhedspolitik af 28. juni 2016 – Fælles vision, fælles handling: et stærkere Europa,

SOM MINDER OM Europa-Kommissionens meddelelse af 19. december 2020 om Europas digitale fremtid i støbeskeen[22] og af 24. juli 2020 om strategien for EU's sikkerhedsunion[23],

SOM MINDER OM den fælles meddelelse af 2. december 2020 fra Europa-Kommissionen og den højtstående repræsentant om en ny dagsorden for EU og USA om globale forandringer[24],

1. FREMHÆVER, at cybersikkerhed er afgørende for opbygningen af et modstandsdygtigt, grønt og digitalt Europa, og SER MED TILFREDSHED PÅ den fælles meddelelse til Europa-Parlamentet og Rådet med titlen "EU's strategi for cybersikkerhed for det digitale årti", som skitserer den nye ramme for EU's indsats på området "modstandsdygtighed, teknologisk suverænitet og lederskab", og for at beskytte sine borgere, virksomheder og institutioner mod cyberhændelser og -trusler og samtidig styrke enkeltpersoners og organisationers tillid til EU's evne til at fremme sikre og pålidelige net- og informationssystemer, infrastruktur og konnektivitet og til at fremme og beskytte et globalt, åbent, frit, stabilt og sikkert cyberspace baseret på menneskerettigheder, grundlæggende frihedsrettigheder, demokrati og retsstatsprincippet.

---

20 EUCO 13/20.
21 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. ANERKENDER, at covid-19-pandemien har betydet, at det øgede behov for tillid til informations- og kommunikationsteknologiske (IKT) værktøjer og systemer og deres sikkerhed er i forreste linje i vores dagligdag. UNDERSTREGER, at cybersikkerhed og et globalt og åbent internet er afgørende for en velfungerende offentlig forvaltning og velfungerende offentlige institutioner på både nationalt plan og EU-plan og for vores samfund og økonomi som helhed,

3. UNDERSTREGER behovet for at øge bevidstheden om cyberspørgsmål på det politiske og strategiske beslutningsniveau ved at give beslutningstagerne relevant viden og information og UNDERSTREGER behovet for at øge bevidstheden i offentligheden og fremme cyberhygiejne.

4. OPFORDRER TIL fremme og beskyttelse af EU's centrale værdier demokrati, retsstatsprincippet, menneskerettigheder og grundlæggende frihedsrettigheder, herunder ytrings- og informationsfrihed, forsamlings- og foreningsfrihed og retten til privatlivets fred i cyberspace. SER i denne henseende MED TILFREDSHED på en yderligere vedvarende indsats for at beskytte menneskerettighedsforkæmpere, civilsamfundet og akademikere, der arbejder med emner som cybersikkerhed, databeskyttelse, overvågning og onlinecensur ved at give yderligere praktisk vejledning, fremme bedste praksis og optrappe EU's indsats for at forebygge krænkelser og overtrædelser af menneskerettighederne og misbrug af nye teknologier, navnlig ved anvendelse af diplomatiske foranstaltninger, hvor det er nødvendigt, samt eksportkontrol med sådanne teknologier. FREMHÆVER i denne forbindelse betydningen af EU-handlingsplanen om menneskerettigheder og demokrati 2020-2024 og EU's retningslinjer vedrørende menneskerettighederne hvad angår ytringsfrihed online og offline.
5. FREMHÆVER, at det at opnå strategisk autonomi og samtidig bevare en åben økonomi er et centralt mål for Unionen med henblik på selv at bestemme dens økonomiske kurs og interesser. Dette omfatter styrkelse af evnen til at træffe selvstændige valg på cybersikkerhedsområdet med det formål at styrke EU's digitale lederskab og strategiske kapacitet. MINDER OM, at dette omfatter at identificere og begrænse strategisk afhængighed og øge modstandsdygtigheden i de mest følsomme industrielle økosystemer og på specifikke områder. UNDERSTREGER, at dette kan omfatte diversificering af produktions- og forsyningskæderne, fremme og tiltrækning af investeringer og produktion i Europa, undersøgelse af alternative løsninger og cirkulære modeller og fremme af et bredt industrielt samarbejde på tværs af medlemsstaterne.

6. UNDERSTREGER i betragtning af manglen på digitale færdigheder og færdigheder inden for cybersikkerhed i arbejdsstyrken betydningen af at imødekomme efterspørgslen efter en uddannet arbejdsstyrke inden for det digitale og cybersikkerhed, navnlig ved at udvikle, fastholde og tiltrække de bedste talenter, f.eks. gennem uddannelse, for at kunne digitalisere vores samfund på en cybersikker måde. TILSKYNDER flere kvinder og piger til at uddanne sig inden for naturvidenskab, teknologi, ingeniørteknik og matematik ("STEM") og til at beskæftige sig med IKT og opkvalificere og omkvalificere sig inden for det digitale område som en måde at bygge bro over den kønsbestemte digitale kløft.

7. MINDER OM, at den fælles og samlede EU-tilgang til cyberdiplomati har til formål at bidrage til konfliktforebyggelse, afbødning af cybersikkerhedstrusler og større stabilitet i internationale forbindelser. BEKRÆFTER i den forbindelse PÅ NY sit tilsagn om at bilægge internationale tvister i cyberspace med fredelige midler, og at alle EU's diplomatiske bestræbelser bør prioritere at fremme sikkerhed og stabilitet i cyberspace gennem øget internationalt samarbejde og mindske risikoen for fejlagtige opfattelser, eskalering og konflikter, der kan hidrøre fra IKT-hændelser, og STØTTER yderligere udvikling og operationalisering af tillidsskabende foranstaltninger på regionalt og internationalt plan. GENTAGER De Forenede Nationers Generalforsamlings opfordring, der blev vedtaget ved konsensus, om, at FN's medlemsstater lader sig vejlede af henstillingerne i rapporterne fra FN's gruppe af regeringseksperter i forbindelse med deres brug af IKT og BEKRÆFTER PÅ NY anvendelsen af folkeretten, navnlig FN-pagten i sin helhed, i cyberspace.

8. BEKRÆFTER PÅ NY, at det med henblik på i væsentlig grad at udforme internationale normer og standarder inden for nye teknologier og den tekniske og logiske infrastruktur, der er afgørende for den generelle tilgængelighed og integritet af den offentligt tilgængelige kerne af internettet, således at disse er i overensstemmelse med universelle værdier og EU-værdier og gennem en multiinteressenttilgang, er afgørende at videreudvikle normer og standarder i Unionen. Dette vil sikre, at internettet forbliver globalt, åbent, frit, stabilt og sikkert, og at anvendelsen og udviklingen af digitale teknologier respekterer menneskerettighederne, og at brugen heraf er lovlig, sikker og etisk. NOTERER SIG den kommende standardiseringsstrategi og FORPLIGTER sig til proaktive og koordinerede oplysningskampagner for at fremme EU's lederskab og EU's mål på internationalt plan, herunder i forskellige internationale standardiseringsorganer og gennem samarbejde med ligesindede partnere, civilsamfundet, den akademiske verden og den private sektor.

9. STØTTER KRAFTIGT multiinteressentmodellen for internetforvaltning og cybersikkerhed og forpligter sig til at styrke regelmæssige og strukturerede udvekslinger med interessenterne, herunder den private sektor, den akademiske verden og civilsamfundet i internationale fora, herunder i forbindelse med Parisopfordringen om tillid og sikkerhed i cyberspace. FREMMER universel, prisoverkommelig og lige adgang til internettet, som bygger bro over de digitale kløfter, og navnlig empowerment af kvinder og piger og personer i sårbare eller marginaliserede situationer, både i politikudviklingen og i brugen af internettet.

10. FREMHÆVER behovet for at inkludere cybersikkerhed i digitale investeringer og initiativer i de kommende år og behovet for gradvis at bidrage til lige vilkår inden for cybersikkerhed og NOTERER SIG Kommissionens plan om at øge de offentlige udgifter og mobilisere private investeringer på cybersikkerhedsområdet. FREMHÆVER betydningen af små og mellemstore virksomheder (SMV'er) i cybersikkerhedsøkosystemet og ANERKENDER de relevante finansielle instrumenter, der er til rådighed til at støtte et stærkt cybersikkerhedsfokus inden for den digitale transformation i den flerårige finansielle ramme (FFR) for 2021-2027 samt i genopretnings- og resiliensfaciliteten.

11. SER FREM TIL en hurtig gennemførelse af forordningen om Det Europæiske Industri-, Teknologi- og Forskningskompetencecenter for Cybersikkerhed og Netværket af Nationale Koordinationscentre, herunder hurtig oprettelse og operationalisering af Det Europæiske Kompetencecenter for Cybersikkerhed i Bukarest. En hurtig vedtagelse af dets dagsorden vil bidrage til at maksimere virkningerne af investeringer med henblik på at styrke Unionens lederskab og strategiske autonomi inden for cybersikkerhed og støtte teknologiske kapaciteter og færdigheder og på at øge Unionens globale konkurrenceevne med input fra industrien og akademiske kredse inden for cybersikkerhed, herunder SMV'er og forskningscentre, som vil drage fordel af et mere systematisk, inklusivt og strategisk samarbejde under hensyntagen til samhørigheden i Unionen og alle dens medlemsstater.

12. HILSER det igangværende arbejde ledet af ENISA sammen med medlemsstaterne og interesserede interessenter VELKOMMEN med henblik på at forsyne EU med certificeringsordninger for IKT-produkter, -tjenester og -processer, som bør bidrage til at øge det generelle cybersikkerhedsniveau på det digitale indre marked. SER i denne forbindelse FREM TIL Unionens rullende arbejdsprogram med henblik på at udvikle EU's cybersikkerhedscertificeringsordninger inden for rammerne af forordningen om cybersikkerhed. ANERKENDER i denne forbindelse den afgørende rolle, som EU spiller med hensyn til at udvikle standarder, der kan forme cybersikkerhedslandskabet, og som bidrager til at sikre fair konkurrence i EU og på den globale scene, fremme markedsadgang og håndtere sikkerhedsrisici og samtidig sikre, at EU's lovgivningsmæssige rammer finder anvendelse.

13. GENTAGER betydningen på lang sigt af en vurdering af behovet for horisontal lovgivning, der også præciserer de nødvendige betingelser for omsætning, for at tackle alle relevante aspekter af cybersikkerheden ved forbundet udstyr, såsom tilgængelighed, integritet og fortrolighed. HILSER i denne forbindelse en drøftelse med henblik på at undersøge anvendelsesområdet for denne lovgivning og dens forbindelser med rammen for cybersikkerhedscertificering som defineret i forordningen om cybersikkerhed VELKOMMEN med henblik på at højne sikkerhedsniveauet på det digitale indre marked. UNDERSTREGER, at der for at undgå tvetydighed og fragmentering i lovgivningen bør fastsættes cybersikkerhedskrav i overensstemmelse med relevant EU-lovgivning, herunder forordningen om cybersikkerhed, den nye lovgivningsmæssige ramme, forordningen om europæisk standardisering og eventuel fremtidig horisontal lovgivning.

14. ANERKENDER betydningen af en omfattende og horisontal tilgang til cybersikkerhed i Unionen, samtidig med at medlemsstaternes kompetencer og behov respekteres fuldt ud, samt af løbende støtte til teknisk bistand og samarbejde med henblik på at opbygge medlemsstaternes kapacitet. NOTERER SIG i betragtning af udviklingen i cybertrusselslandskabet det nye forslag til direktiv om foranstaltninger til et højt fælles cybersikkerhedsniveau i hele Unionen, der bygger på NIS-direktivet, og gentager sin støtte til styrkelse og harmonisering af nationale rammer for cybersikkerhed og et vedvarende samarbejde mellem medlemsstaterne. UNDERSTREGER endvidere behovet for tilpasning og formulering af sektorspecifik lovgivning på dette område.

15. NOTERER SIG Kommissionens forslag om at støtte medlemsstaterne i at oprette og styrke sikkerhedsoperationscentre (SOC'er) med henblik på at opbygge et netværk af SOC'er i hele EU for yderligere at overvåge og foregribe advarsler om angreb mod netværk. AFVENTER i den forbindelse Kommissionens detaljerede planer vedrørende netværket af SOC'er, samtidig med at medlemsstaternes kompetencer respekteres. MINDER OM den indsats, som medlemsstaterne med støtte fra EU har gjort for at oprette sektorielle, nationale og regionale enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er), og nationale eller europæiske informationsudvekslings- og analysecentre (ISAC'er) som led i et effektivt netværk af cybersikkerhedspartnerskaber i Unionen. SER FREM TIL at undersøge dette netværks potentiale til at styrke SOC'er samt disses komplementaritet og koordinering med eksisterende netværk og aktører (navnlig netværket af CSIRT'er) med henblik på at fremme en effektiv, sikker og pålidelig informationsudvekslingskultur. FREMHÆVER, at denne proces vil bygge videre på det arbejde, som er udført i forbindelse med initiativerne vedrørende kunstig intelligens og højtydende databehandling, og som er foretaget af europæiske digitale innovationsknudepunkter.

16. NOTERER SIG den mulige udvikling af et sikkert konnektivitetssystem med udgangspunkt i en europæisk kvantekommunikationsinfrastruktur (EuroQCI) og Den Europæiske Unions statslige satellitkommunikation (GOVSATCOM) og ERKENDER, at en eventuel fremtidig udvikling bør bygge på en robust ramme for cybersikkerhed og tage hensyn til hele den elektroniske kommunikationsinfrastruktur såsom rum-, land- og undervandsnetsystemer.

17. SER FREM TIL drøftelserne med Kommissionen, ENISA, de to EU-udbydere af DNS-rodservere og multiinteressentsamfundet om en vurdering af de to EU-udbydere af DNS-rodserveres rolle med hensyn til at garantere, at internettet fortsat er globalt tilgængeligt uden at være fragmenteret. GLÆDER SIG OVER yderligere drøftelser om Kommissionens hensigt om at udvikle en alternativ europæisk tjeneste for adgang til det globale internet ("DNS4EU"-initiativet) baseret på en gennemsigtig model, som er i overensstemmelse med de seneste standarder og regler for sikkerhed, databeskyttelse og privatlivsbeskyttelse gennem design og standardindstillinger, med henblik på at bidrage til øget robusthed og samtidig opretholde og styrke den internationale konnektivitet for alle medlemsstater.

18. ERKENDER behovet for en fælles indsats fra Kommissionen og medlemsstaterne for at fremskynde udbredelsen af vigtige internetstandarder, herunder IPv6 og veletablerede standarder for internetsikkerhed, eftersom de er afgørende for at højne det globale internets overordnede sikkerhedsniveau, robusthed, åbenhed og interoperabilitet, samtidig med at konkurrenceevnen for EU's industri og navnlig for udbydere af internetinfrastruktur øges.

19. PÅPEGER betydningen af en koordineret tilgang samt udvikling og gennemførelse af effektive foranstaltninger på nationalt plan til styrkelse af cybersikkerheden i 5G-net. STØTTER de næste skridt, der skal tages med hensyn til 5G-nets cybersikkerhed, som blev fremlagt i tillægget til EU's strategi for cybersikkerhed, og som er baseret på resultaterne af rapporten om virkningerne af Kommissionens henstilling om 5G-nets sikkerhed, f.eks. med hensyn til fastlæggelse af en langsigtet og samlet tilgang med fokus på hele 5G-værdikæden og -økosystemet. OPFORDRER INDTRÆNGENDE medlemsstaterne, EU-institutionerne og andre relevante interessenter TIL med henblik på yderligere at styrke den koordinerede tilgang til 5G-net at fortsætte med deres regelmæssige statusopgørelser sammen med udveksling af oplysninger og bedste praksis inden for den særlige NIS-samarbejdsgruppes arbejdsområde for 5G-nets cybersikkerhed og regelmæssigt rapportere om de fremskridt, der er opnået, til Rådet. FREMHÆVER, samtidig med at det understreger medlemsstaternes ansvar for at beskytte den nationale sikkerhed, at det er fast besluttet på at anvende og hurtigt afslutte gennemførelsen af foranstaltningerne vedrørende EU's 5G-værktøjskasse og fortsætte bestræbelserne på at garantere 5G-nets sikkerhed og udviklingen af fremtidige generationer af net. Det tætte samarbejde mellem medlemsstaterne, Kommissionen og ENISA om 5G-nets sikkerhed kan tjene som eksempel i forbindelse med andre problemstillinger på cybersikkerhedsområdet, samtidig med at medlemsstaternes kompetencer og nærheds- og proportionalitetsprincippet respekteres.

20. ERKENDER relevansen af yderligere at integrere cybersikkerhed i EU's kriseaktionsmekanismer og teste disse i relevante øvelser og FREMHÆVER betydningen af at styrke samarbejdet og informationsudvekslingen mellem de forskellige cyberfællesskaber i EU og forbinde de eksisterende initiativer, strukturer og procedurer (såsom IPCR, CSIRT-netværket, NIS-samarbejdsgruppen, CyCLONe, Det Europæiske Center for Bekæmpelse af Cyberkriminalitet, EU INTCEN og andre relevante EU-organer) i tilfælde af væsentlige og grænseoverskridende cyberhændelser og -trusler. TAGER HENSYN TIL de fremskridt, der allerede er gjort på dette område, og AFVENTER Kommissionens forslag om proceduren, milepælene og tidsplanen for oprettelse af den fælles cyberenhed (JCU) med henblik på at skabe merværdi for, sætte klart fokus på og strømline EU's ramme for håndtering af cybersikkerhedskriser, herunder gennem beredskab, fælles situationsbevidsthed og styrkelse af den koordinerede indsats og øvelser, på en gennemsigtig og trinvis måde, samtidig med at dobbeltarbejde og overlapning undgås, med respekt for medlemsstaternes kompetencer.

21. PÅPEGER dels betydningen af at fremme samarbejde og informationsudveksling mellem de relevante cybersikkerhedsaktører og de kompetente myndigheder på sikkerheds- og strafferetsområdet, f.eks. de retshåndhævende og judicielle myndigheder, dels behovet for at udvide og forbedre disse myndigheders kapacitet til at efterforske og retsforfølge cyberkriminalitet og fremme internationale forhandlinger og EU-regler om grænseoverskridende adgang til elektronisk bevismateriale. Uafhængigt af dagens teknologiske klima er det afgørende, at de kompetente myndigheder på sikkerheds- og strafferetsområdet bevarer deres beføjelser, så de lovligt kan udføre deres opgaver som foreskrevet og godkendt ved lov. Sådanne love, der giver håndhævelsesbeføjelser, skal altid fuldt ud respektere en retfærdig procedure og andre garantier samt de grundlæggende rettigheder, navnlig retten til respekt for privatliv og kommunikation og retten til beskyttelse af personoplysninger.

22. BEKRÆFTER PÅ NY sin støtte til udvikling, gennemførelse og anvendelse af solid kryptering som et nødvendigt middel til beskyttelse af de grundlæggende rettigheder og den digitale sikkerhed for enkeltpersoner, regeringer, industri og samfund og ERKENDER samtidig behovet for at sikre, at de kompetente myndigheder på sikkerheds- og strafferetsområdet, f.eks. retshåndhævende og judicielle myndigheder, kan udøve deres retmæssige beføjelser, både online og offline, til at beskytte vores samfund og borgerne. De kompetente myndigheder skal kunne få adgang til data på lovlig og målrettet vis under fuld overholdelse af de grundlæggende rettigheder og de relevante databeskyttelseslove, samtidig med at cybersikkerheden opretholdes. FREMHÆVER, at alle de foranstaltninger, der træffes, skal afveje disse interesser omhyggeligt i forhold til principperne om nødvendighed, proportionalitet og nærhed.

23. STØTTER og FREMMER Budapestkonventionen om IT-kriminalitet og det igangværende arbejde med anden tillægsprotokol til nævnte konvention. Deltager desuden fortsat i multilaterale udvekslinger om cyberkriminalitet, herunder i processer vedrørende Europarådet, FN's Kontor for Narkotikakontrol og Kriminalitetsbekæmpelse (UNODC) og Kommissionen for Kriminalitetsforebyggelse og Strafferet (CCPCJ), for at sikre et styrket internationalt samarbejde om bekæmpelse af cyberkriminalitet, herunder udveksling af bedste praksis og teknisk viden og støtte til kapacitetsopbygning, samtidig med at menneskerettighederne og de grundlæggende frihedsrettigheder respekteres, fremmes og beskyttes.

24. ERKENDER betydningen af strategisk efterretningssamarbejde om cybertrusler og -aktiviteter, selv om den nationale sikkerhed forbliver den enkelte medlemsstats eneansvar, og OPFORDRER medlemsstaterne gennem deres kompetente myndigheder TIL at fortsætte med at bidrage til EU INTCEN's arbejde som knudepunkt for situationsbevidsthed og trusselsvurderinger vedrørende cyberspørgsmål for EU og undersøge forslaget om en mulig oprettelse af en arbejdsgruppe om cyberintelligens for medlemsstaterne for at styrke INTCEN's særlige kapacitet på dette område på grundlag af medlemsstaternes frivillige efterretningsbidrag, og uden at dette berører deres kompetencer.

25. FREMHÆVER betydningen af en solid og konsekvent sikkerhedsramme til beskyttelse af al EU's personale, data, kommunikationsnet og informationssystemer samt beslutningsprocesser på grundlag af omfattende, konsekvente og ensartede regler. Dette bør navnlig ske ved at styrke robustheden og forbedre EU's sikkerhedskultur over for cybertrusler og ved at styrke sikkerheden i klassificerede og ikkeklassificerede EU-net, samtidig med at der sikres en passende forvaltning, og at der stilles tilstrækkelige ressourcer og kapaciteter til rådighed, herunder i forbindelse med styrkelse af CERT-EU's mandat. SER i den forbindelse MED TILFREDSHED PÅ de igangværende drøftelser om indførelse af fælles regler om informationssikkerhed under behørig hensyntagen til Rådets sikkerhedsregler til beskyttelse af EU's klassificerede informationer samt fastsættelsen af fælles bindende regler om cybersikkerhed for alle EU-institutioner, -organer og -agenturer.

26. FORPLIGTER SIG MED UDGANGSPUNKT I EU's cyberdiplomatiske indsats TIL at øge den cyberdiplomatiske værktøjskasses effektivitet og SER FREM TIL at uddybe drøftelserne om dens anvendelsesområde og anvendelse på baggrund af de hidtidige erfaringer med anvendelsen af dette instrument. Disse drøftelser bør bidrage til at fremme sikkerheden på internationalt plan ved at fremme dialog og en fælles vision for cybersikkerhedsspørgsmål, styrke forebyggelse, stabilitet og samarbejde og fremme tillid og kapacitetsopbygning og, hvis det er relevant, indføre restriktive foranstaltninger med henblik på at forhindre, modvirke, afskrække fra og reagere på ondsindede cyberaktiviteter, der er rettet mod EU's og dets medlemsstaters integritet og sikkerhed, og derved bidrage til international sikkerhed og stabilitet og konsolidere EU's cyberposition med fuld respekt for nationale kompetencer og beføjelser. Der bør navnlig lægges særlig vægt på at forebygge og bekæmpe cyberangreb med systemiske virkninger, som kan påvirke vores forsyningskæder, kritiske infrastruktur og væsentlige tjenester, demokratiske institutioner og processer og underminere vores økonomiske sikkerhed, herunder cyberbaseret tyveri af intellektuel ejendom. Medlemsstaterne og EU-institutionerne bør også yderligere overveje forbindelsen mellem EU's ramme for håndtering af cybersikkerhedskriser, den cyberdiplomatiske værktøjskasse og bestemmelserne i artikel 42, stk. 7, i TEU og artikel 222 i TEUF, navnlig gennem scenariebaseret arbejde for at skabe en fælles forståelse af de praktiske betingelser for gennemførelsen af artikel 42, stk. 7, i TEU.

27. ERKENDER betydningen af at styrke samarbejdet med internationale organisationer og partnerlande for at fremme en fælles forståelse af cybertrusselsbilledet, udvikle dialoger og samarbejdsmekanismer, fastlægge en samarbejdsbaseret diplomatisk indsats, hvor det er relevant, samt forbedre informationsudvekslingen, herunder gennem uddannelse og øvelser. FREMHÆVER navnlig, at et stærkt transatlantisk partnerskab på cybersikkerhedsområdet bidrager til vores fælles sikkerhed, stabilitet og velstand, og NOTERER SIG bestemmelserne om cybersikkerhedssamarbejde i handels- og samarbejdsaftalen mellem EU og UK. SOM MINDER OM de vigtigste resultater af samarbejdet mellem EU og NATO på cybersikkerhedsområdet inden for rammerne af gennemførelsen af de fælles erklæringer fra Warszawa i 2016 og Bruxelles i 2018, gentager betydningen af et øget, gensidigt forstærkende og gavnligt samarbejde gennem uddannelse, øvelser og en koordineret indsats mod ondsindede cyberaktiviteter med fuld respekt for begge organisationers beslutningsautonomi og procedurer på grundlag af principperne om gennemsigtighed, gensidighed og inklusivitet.

28. FORPLIGTER SIG med henblik på at bidrage til et globalt, åbent, frit, stabilt og sikkert cyberspace, som er af stadig større betydning for fortsat velstand, vækst, sikkerhed, trivsel, konnektivitet og integritet i vores samfund, TIL løbende at engagere sig i processer for fastsættelse af normer i internationale organisationer, navnlig i FN's første udvalgsrelaterede processer, fremme og bidrage til anerkendelse af anvendelsen af folkeretten i cyberspace og overholdelse af normer, regler og principper for ansvarlig statslig adfærd i cyberspace, herunder ved at fremme en hurtig oprettelse af et handlingsprogram til fremme af ansvarlig statslig adfærd i cyberspace som en konstruktiv, inklusiv og konsensusbaseret opfølgning af begge nuværende processer for Gruppen af Regeringseksperter og den åbne arbejdsgruppe.

29. MINDER OM sit stærke engagement i effektiv multilateralisme og en regelbaseret international orden med FN i centrum, og at det er fast besluttet på at styrke samarbejdet og koordineringen med internationale og regionale organisationer, navnlig FN-systemet, NATO, Europarådet, OSCE, OECD, AU, OAS, ASEAN, ARF, GCC og LAS, med hensyn til drøftelser om cyberrelaterede spørgsmål samt videreførelse og udvidelse af EU's strukturerede cyberdialoger med og -høringer af tredjelande. UNDERSTREGER sin aktive støtte til FN, navnlig i forbindelse med 2030-dagsordenen, herunder verdensmålene for bæredygtig udvikling, og SER MED TILFREDSHED PÅ FN's generalsekretærs køreplan for digitalt samarbejde og FN's generalsekretærs dagsorden for nedrustning, som fremmer ansvarlighed og overholdelse af normer i cyberspace og bidrager til forebyggelse og fredelig løsning af konflikter som følge af ondsindede aktiviteter i cyberspace. GLÆDER SIG OVER forslaget fra den højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik om at oprette et uformelt cyberdiplomatisk EU-netværk med henblik på at udvikle både EU's og medlemsstaternes engagement og ekspertise i internationale cyberspørgsmål med henblik på at styrke koordinerede oplysningskampagner.

30. SER FREM TIL det kommende forslag om en revision af rammen for cyberforsvarspolitik og FORPLIGTER SIG TIL at fortsætte bestræbelserne på at styrke aspekter af cybersikkerhed og cyberforsvar for at sikre, at de fuldt ud indarbejdes på det bredere sikkerheds- og forsvarsområde, navnlig i forbindelse med arbejdet med det strategiske kompas. MENER, at den kommende "Military Vision and Strategy on Cyberspace as a Domain of Operations" (militær vision og strategi for cyberspace som et operationsområde) vil bidrage til at fremme disse drøftelser. SER MED TILFREDSHED PÅ Det Europæiske Forsvarsagenturs (EDA's) initiativ til at fremme samarbejdet mellem militære CERT'er og STØTTER indsatsen, der er gjort for at styrke civil-militære synergier for og koordinering af cyberforsvar og cybersikkerhed, herunder vedrørende rumrelaterede aspekter, herunder gennem de særlige PESCO-projekter.

31. GLÆDER SIG OVER forslaget om at udarbejde en dagsorden for EU's eksterne cyberkapacitetsopbygning, forslaget om at nedsætte et råd for EU's cyberkapacitetsopbygning og oprettelsen og gennemførelsen af EU's CyberNet (EU-netværk for cyberkapacitetsopbygning) med henblik på at øge cyberrobustheden og -kapaciteten på globalt plan. HILSER i den forbindelse samarbejdet med medlemsstaterne samt partnere i den offentlige og private sektor VELKOMMEN, navnlig det globale forum for cyberekspertise (GFCE) og andre relevante internationale organer, for at sikre koordinering og undgå overlapning. TILSKYNDER navnlig TIL samarbejde med partnere på Vestbalkan og i EU's østlige og sydlige nabolande.

32. FORPLIGTER SIG TIL at bistå partnerlande med at tackle den stigende udfordring med ondsindede cyberaktiviteter, navnlig cyberaktiviteter, der skader udviklingen af deres økonomier, samfund og de demokratiske systemers integritet og sikkerhed, herunder i overensstemmelse med indsatsen i handlingsplanen for europæisk demokrati, for at sikre at alle lande har mulighed for at høste de sociale, økonomiske og politiske fordele ved internettet og anvendelsen af teknologier.

33. OPFORDRER Kommissionen og den højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik TIL at udarbejde en detaljeret gennemførelsesplan med angivelse af prioriteterne og tidsplanen for de planlagte foranstaltninger med henblik på at sikre udvikling, gennemførelse og overvågning af forslagene i EU's strategi for cybersikkerhed og under hensyntagen til visse initiativers flerårige karakter. vil OVERVÅGE fremskridtene med gennemførelsen af disse konklusioner i form af en handlingsplan, som regelmæssigt gennemgås og ajourføres af Rådet i tæt samarbejde med Europa-Kommissionen og den højtstående repræsentant.