Rådet for
Den Europæiske Union

Bruxelles, den 16. december 2020
(OR. en)

14133/20

Interinstitutionel sag:
2020/0305(NLE)

CYBER 280	**RECH 529**
JAI 1118	**COMPET 642**
JAIEX 121	**IND 273**
EJUSTICE 107	**COTER 115**
COSI 254	**ENFOPOL 350**
DATAPROTECT 154	**COPS 485**
COPEN 387	**MI 578**
TELECOM 269	**IXIM 139**
PROCIV 99	**POLMIL 201**
CSC 367	**HYBRID 48**
CIS 65	**CSCI 96**
RELEX 1019	**POLGEN 234**

FØLGESKRIVELSE

fra:	Martine DEPREZ, direktør, på vegne af generalsekretæren for Europa-Kommissionen
modtaget:	16. december 2020
til:	Jeppe TRANHOLM-MIKKELSEN, generalsekretær for Rådet for Den Europæiske Union
Komm. dok. nr.:	JOIN(2020) 18 final
Vedr.:	FÆLLES MEDDELELSE TIL EUROPA-PARLAMENTET OG RÅDET EU's strategi for cybersikkerhed for det digitale årti

Hermed følger til delegationerne dokument JOIN(2020) 18 final.

Bilag: JOIN(2020) 18 final

EUROPA-
KOMMISSIONEN

UNIONENS HØJTSTÅENDE
REPRÆSENTANT FOR
UDENRIGSANLIGGENDER
OG SIKKERHEDSPOLITIK

Bruxelles, den 16.12.2020
JOIN(2020) 18 final

FÆLLES MEDDELELSE TIL EUROPA-PARLAMENTET OG RÅDET

EU's strategi for cybersikkerhed for det digitale årti

FÆLLES MEDDELELSE TIL EUROPA-PARLAMENTET OG RÅDET

EU's strategi for cybersikkerhed for det digitale årti

I. INDLEDNING: EN CYBERSIKKER DIGITAL OMSTILLING I ET KOMPLEKST TRUSSELSMILJØ

Cybersikkerhed er en integrerende del af europæernes sikkerhed. Uanset om der er tale om forbundne enheder og elektricitetsnet eller banker, luftfartøjer, offentlige forvaltninger og hospitaler, fortjener folk at kunne benytte dem med sikkerhed for, at de vil blive beskyttet mod cybertrusler. EU's økonomi, demokrati og samfund er mere end nogensinde før afhængige af sikre og pålidelige digitale værktøjer og konnektivitet. Cybersikkerhed er derfor afgørende for opbygningen af et modstandsdygtigt, grønt og digitalt Europa.

Transport, energi og sundhed, telekommunikation, finans, sikkerhed, demokratiske processer, rumfart og forsvar er stærkt afhængige af net- og informationssystemer, som i stigende grad er indbyrdes forbundne. Den tværsektorielle afhængighed er meget stærk, fordi net- og informationssystemer er afhængige af en stabil elforsyning for at kunne fungere. Antallet af netforbundne enheder overstiger allerede nu antallet af mennesker på planeten, og antallet af enheder forventes at stige til 25 milliarder i 2025[1]. En fjerdedel af disse vil være i Europa. Digitaliseringen af arbejdsmønstrene er blevet fremskyndet af covid-19-pandemien, hvor 40 % af EU's arbejdstagere gik over til telearbejde, hvilket sandsynligvis vil få varige følger for hverdagen[2]. Dette øger sårbarheden over for cyberangreb[3]. Netforbundne enheder sendes ofte til forbrugeren med kendte sårbarheder, hvilket yderligere øger angrebsfladen for ondsindede cyberaktiviteter[4]. Industrilandskabet i EU bliver i stigende grad digitaliseret og forbundet, hvilket også betyder, at cyberangreb kan få langt større indvirkning på industrier og økosystemer end nogensinde før.

Trusselsbilledet forværres af geopolitiske spændinger over det globale og åbne internet og over kontrollen med teknologier i hele forsyningskæden[5]. Disse spændinger afspejles i det stigende antal nationalstater, der opstiller digitale grænser. Begrænsninger af og på internettet truer det globale, åbne cyberspace samt retsstatsprincippet, grundlæggende

---

[1] Anslået af telekommunikationsforeningen GSMA: https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf. I henhold til Den Internationale Telekommunikationssammenslutnings prognose 42,6 mia. forbundne maskiner, sensorer og kameraer: https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[2] Ifølge en undersøgelse fra juni 2020 forventede 47 % af alle virksomhedsledere at give medarbejderne mulighed for at arbejde hjemmefra på fuld tid, selv efter de ville kunne vende tilbage til arbejdspladsen: 82 % forventede at give medarbejderne mulighed for at arbejde hjemmefra mindst en del af tiden: https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time.

[3] https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf.

[4] En af de mest skadelige malware til dato, kendt som Mirai, skabte botnet med over 600 000 enheder, der forstyrrede en lang række større websteder i Europa og USA.

[5] Herunder elektroniske komponenter, dataanalyse, cloud, hurtigere og mere intelligente netværk med 5G og derover, kryptering, kunstig intelligens (AI) og nye, sikre databehandlingsparadigmer såsom blockchain, cloud til edge og kvantedatabehandling.

rettigheder, frihed og demokrati — EU's kerneværdier. Cyberspace udnyttes i stigende grad til politiske og ideologiske formål, og en øget polarisering på internationalt plan hindrer effektiv multilateralisme. Hybride trusler kombinerer desinformationskampagner med cyberangreb på infrastruktur, økonomiske processer og demokratiske institutioner, hvilket potentielt kan forårsage fysisk skade, give ulovlig adgang til personoplysninger, medføre tyveri af industrielle eller statslige hemmeligheder, skabe mistillid og svække den sociale samhørighed. Disse aktiviteter undergraver den internationale sikkerhed og stabilitet og de fordele, som cyberspace medfører for den økonomiske, sociale og politiske udvikling.

Ondsindede, målrettede angreb på kritisk infrastruktur er en stor global risiko[6]. Internettet har en decentraliseret arkitektur uden nogen central struktur og forvaltes af mange forskellige interessenter. Det har formået at håndtere eksponentielle stigninger i trafikmængden, samtidig med at det konstant er mål for ondsindede angreb[7]. Samtidig stiger afhængigheden af de centrale funktioner i det globale og åbne internet såsom domænenavnesystemet (DNS) og vigtige internettjenester til kommunikation og hosting, applikationer og data. Disse tjenester koncentreres i stigende grad i hænderne på nogle få private virksomheder[8]. Det gør den europæiske økonomi og det europæiske samfund sårbare over for forstyrrende geopolitiske eller tekniske hændelser, der påvirker kernen i internettet eller en eller flere af disse virksomheder. Den øgede brug af internettet og de ændrede mønstre som følge af pandemien har yderligere blotlagt skrøbeligheden ved de forsyningskæder, der er afhængige af denne digitale infrastruktur.

Bekymringer over sikkerhed er en stor hindring for brugen af onlinetjenester[9]**.** Omkring to femtedele af brugerne i EU har oplevet sikkerhedsrelaterede problemer, og tre femtedele føler sig ude af stand til at beskytte sig selv mod cyberkriminalitet[10]. En tredjedel har inden for de seneste tre år modtaget falske e-mails eller telefonopkald, hvor de bliver bedt om at afgive personoplysninger, men 83 % har aldrig indberettet cyberkriminalitet. En ud af otte virksomheder har været udsat for cyberangreb[11]. Over halvdelen af de computere i virksomheder og hos forbrugere, der er blevet inficeret med malware én gang, geninficeres inden for samme år[12]. Hvert år går flere hundrede millioner registreringer tabt på grund af brud på datasikkerheden, og de gennemsnitlige omkostninger ved et sådant brud for en enkelt

---

[6] World Economic Forum, Global Risks Report 2020.

[7] Pandemien har ifølge Organisationen for Økonomisk Samarbejde og Udvikling ført til en stigning i internettrafikken på 60 %: https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/. Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation og Kommissionen offentliggør regelmæssigt rapporter med status over internettets kapacitet i forbindelse med foranstaltninger til inddæmning af coronavirus. Ifølge en rapport fra ENISA steg det samlede antal Distributed Denial of Service-angreb (DDoS) i tredje kvartal 2019 med 241 % i forhold til tredje kvartal 2018. DDoS-angrebenes intensitet er stigende, og det største angreb nogensinde fandt sted i februar 2020, hvor spidsbelastningen var på 2,3 terabit pr. sekund. I CenturyLink-afbrydelsen i august 2020 førte et routingproblem hos den amerikanske internetudbyder til et fald på 3,5 % i den globale internettrafik: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service.

[8] Internet Society, The Global Internet Report: Consolidation in the Internet Economy: https://www.internetsociety.org/blog/2019/02/is-the-internet-shrinking-the-global-internet-report-consolidation-in-the-internet-economy-explores-this-question/

[9] https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG.

[10] 2020 Digital Economy and Society Index: https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020, https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG.

[11] Eurostats pressemeddelelse "ICT security measures taken by vast majority of enterprises in the EU", 6/2020, 13. januar 2020. "Cyberattacks on critical infrastructure have become the new normal across sectors such as energy, healthcare and transportation", WEF, The Global Risks Report 2020.

[12] Kilde: Comparitech.

virksomhed steg til over 3,5 mio. EUR i 2018[13]. Konsekvenserne af et cyberangreb kan ofte ikke isoleres og kan udløse kædereaktioner i hele økonomien og samfundet og dermed påvirke millioner af mennesker[14].

Efterforskningen af næsten alle former for kriminalitet har en digital komponent. I 2019 blev antallet af år-til-år hændelser tredoblet. Det anslås, at der er 700 millioner nye former for malware — den hyppigste måde til at fremme et cyberangreb på[15]. De årlige omkostninger til IT-kriminalitet for verdensøkonomien i 2020 anslås til 5,5 bio. EUR, hvilket er det dobbelte af omkostningerne i 2015[16]. Dette er den største overførsel af økonomisk velstand i historien, større end den globale narkotikahandel. Omkostningerne forbundet med en større hændelse, WannaCry-angrebet i 2017, blev anslået til over 6,5 mia. EUR for den globale økonomi[17].

Digitale tjenester og finanssektoren er blandt de hyppigste mål for cyberangreb sammen med den offentlige sektor og fremstillingsindustrien, men cyberparatheden og -bevidstheden blandt virksomheder og enkeltpersoner er fortsat lav[18], og arbejdsstyrken har en betydelig mangel på færdigheder inden for cybersikkerhed[19]. Der var næsten 450 cybersikkerhedshændelser i 2019, som involverede kritisk europæisk infrastruktur såsom finans og energi[20]. Sundhedsorganisationer og sundhedspersonale er blevet ramt særlig hårdt under pandemien. Efterhånden som teknologien bliver uløseligt forbundet med den fysiske verden, bringer cyberangreb de mest sårbare menneskers liv og velvære i fare[21]. Mere end to tredjedele af virksomhederne, navnlig SMV'er, betragtes som "novicer" inden for cybersikkerhed, og europæiske virksomheder anses for at være mindre velforberedte end virksomheder i Asien og Amerika[22]. Det anslås, at 291 000 stillinger til fagfolk inden for cybersikkerhed i Europa fortsat ikke er besat. Ansættelse og uddannelse af cybersikkerhedseksperter er en langsom proces, hvilket skaber større cybersikkerhedsrisici for organisationer[23].

EU mangler kollektiv situationsbevidsthed om cybertrusler. Dette skyldes, at de nationale myndigheder ikke systematisk indsamler og udveksler oplysninger — såsom oplysninger, der

---

[13] Årlig rapport om omkostningerne ved databrud, 2020, Ponemon Institute, og baseret på en kvantitativ analyse af 524 nylige overtrædelser i 17 geografiske områder og 17 industrier: https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf.

[14] Rapport fra Det Fælles Forskningscenter (JRC), "Cybersecurity, our digital anchor": https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/cybersecurity-our-digital-anchor.

[15] Kilde: AV-TEST, https://www.av-test.org/en/statistics/malware/

[16] JRC, Cybersecurity – Our Digital Anchor.

[17] Kilde: Cyence.

[18] Erhvervslivets bevidsthed er fortsat lav, også med hensyn til cybertyveri af forretningshemmeligheder, navnlig blandt SMV'er, PwC, Study on the scale and impact of industrial espionage and theft of trade secrets through cyber: Dissemination report on measures to tackle and prevent cyber-theft of trade secrets, 2018.

[19] Se ENISA Threat Landscape 2020. Også Verizon Data Breach Investigations Report 2020: https://enterprise.verizon.com/resources/reports/dbir/.

[20] https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f.

[21] Ransomware er blevet brugt målrettet mod hospitaler og patientjournaler, f.eks. i Rumænien (juni 2020), Düsseldorf (september 2020) og Vastaamo (oktober 2020).

[22] PwC, The Global State of Information Security 2018, ESI Thoughtlab, The Cybersecurity Imperative, 2019.

[23] EU Agency for Cybersecurity, Cybersecurity Skills Development in the EU: The certification of cybersecurity degrees and ENISA's Higher Education Database, december 2019.

er tilgængelige fra den private sektor — som kan bidrage til at vurdere cybersikkerhedssituationen i EU. Kun en brøkdel af alle hændelser indberettes af medlemsstaterne, og udvekslingen af oplysninger er hverken systematisk eller omfattende[24]. Cyberangreb er således måske kun en enkelt facet af samordnede ondsindede angreb på europæiske samfund. Der er i øjeblikket kun begrænset gensidig operationel bistand mellem medlemsstaterne, og der findes ingen operationel mekanisme mellem medlemsstaterne og EU's institutioner, agenturer og organer i tilfælde af omfattende grænseoverskridende cyberhændelser eller -kriser[25].

Forbedring af cybersikkerheden er derfor afgørende for, at folk kan stole på, anvende og drage fordel af innovation, konnektivitet og automatisering, og for at beskytte de grundlæggende rettigheder og frihedsrettigheder, herunder retten til privatlivets fred og retten til beskyttelse af personoplysninger samt ytrings- og informationsfriheden. Cybersikkerhed er uundværlig for netværksforbindelsen og det globale og åbne internet, som skal understøtte omstillingen af økonomien og samfundet i 2020'erne. Det bidrager til bedre og flere job, mere fleksible arbejdspladser, mere effektiv og bæredygtig transport og landbrug og lettere og mere retfærdig adgang til sundhedsydelser. Det er også afgørende for omstillingen til renere energi under den europæiske grønne pagt[26], der skal ske gennem grænseoverskridende net og intelligente målere og ved at undgå unødvendig overlapning af datalagring. Endelig er det afgørende for den internationale sikkerhed og stabilitet og for udviklingen af økonomier, demokratier og samfund på globalt plan. Myndigheder, virksomheder og enkeltpersoner skal derfor anvende digitale værktøjer på en ansvarlig og sikkerhedsbevidst måde. Bevidsthed om cybersikkerhed og IT-hygiejne skal understøtte den digitale omstilling af hverdagsaktiviteter.

EU's nye strategi for cybersikkerhed for det digitale årti udgør et centralt element i udformningen af Europas digitale fremtid[27], Kommissionens genopretningsplan for Europa[28], strategien for en sikkerhedsunion 2020-2025[29], den globale strategi for EU's udenrigs- og sikkerhedspolitik[30] og Det Europæiske Råds strategiske dagsorden 2019-2024[31]. Den beskriver, hvordan EU vil beskytte sine borgere, virksomheder og institutioner mod cybertrusler, og hvordan EU vil fremme internationalt samarbejde og føre an i sikringen af et globalt og åbent internet.

II. TÆNKE GLOBALT, HANDLE EUROPÆISK

Denne strategi har til formål at sikre et globalt og åbent internet med stærke værn for at imødegå risici for sikkerheden og de grundlæggende rettigheder og frihedsrettigheder for befolkningerne i Europa. Den bygger på de fremskridt, der er gjort under de tidligere strategier, og indeholder konkrete forslag til anvendelse af **de tre vigtigste instrumenter — regulerings-, investerings- og politikinstrumenter — til at håndtere tre af EU's indsatsområder — 1) modstandsdygtighed, teknologisk suverænitet og lederskab, 2)**

[24] Medlemsstaterne skal forelægge samarbejdsgruppen en årlig sammenfattende rapport om de underretninger om hændelser, de har modtaget i henhold til artikel 10, stk. 3, i direktivet om sikkerhed i net- og informationssystemer (direktiv (EU) 2016/1148).
[25] Der findes standardprocedurer for gensidig bistand mellem medlemmerne af CSIRT-netværket.
[26] Den europæiske grønne pagt, COM(2019) 640 final.
[27] Europas digitale fremtid i støbeskeen, COM(2020) 67 final.
[28] Et vigtigt øjeblik for Europa: Genopretning og forberedelser til den næste generation, COM(2020) 98 final.
[29] Strategien for EU's sikkerhedsunion 2020-2025, COM(2020) 605 final.
[30] https://eeas.europa.eu/topics/eu-global-strategy_en.
[31] https://www.consilium.europa.eu/en/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/#.

opbygning af operationel kapacitet til at forebygge, modvirke og reagere og 3) fremme af et globalt og åbent cyberspace. EU er fast besluttet på at støtte denne strategi gennem et **hidtil uset investeringsniveau i EU's digitale omstilling i løbet af de næste syv år** — potentielt en firedobling af tidligere niveauer — som led i nye teknologiske og industrielle politikker og genopretningsdagsordenen[32].

Cybersikkerhed skal integreres i alle disse digitale investeringer, navnlig centrale teknologier som kunstig intelligens (KI), kryptering og kvantedatabehandling under anvendelse af incitamenter, forpligtelser og benchmarks. Dette kan stimulere væksten i den europæiske cybersikkerhedsindustri og skabe den sikkerhed, der er nødvendig for at lette udfasningen af eksisterende systemer. Den Europæiske Forsvarsfond støtter europæiske cyberforsvarsløsninger som en del af det europæiske forsvars teknologiske og industrielle grundlag. Cybersikkerhed indgår i eksterne finansielle instrumenter til støtte for vores partnere, navnlig instrumentet for naboskab, udviklingssamarbejde og internationalt samarbejde. Forebyggelse af misbrug af teknologier, beskyttelse af kritisk infrastruktur og sikring af forsyningskædernes integritet gør det også muligt for EU at overholde FN's normer, regler og principper for ansvarlig statslig adfærd[33].

1. MODSTANDSDYGTIGHED, TEKNOLOGISK SUVERÆNITET OG LEDERSKAB

EU's kritiske infrastruktur og væsentlige tjenester er i stigende grad indbyrdes afhængige og digitaliserede. Alle netforbundne ting i EU, hvad enten der er tale om selvkørende biler, industrielle kontrolsystemer eller husholdningsapparater, og alle de forsyningskæder, der gør dem tilgængelige, skal være sikret ved design, være modstandsdygtige over for cyberhændelser og hurtigt patcheres, når der opdages sårbarheder. Dette er afgørende for at give EU's private og offentlige sektor mulighed for at vælge mellem de mest sikre infrastrukturer og tjenester. Det kommende årti er EU's mulighed for at blive førende i udviklingen af sikre teknologier i hele forsyningskæden. Sikring af robusthed og stærkere industriel og teknologisk kapacitet inden for cybersikkerhed bør mobilisere alle nødvendige regulerings-, investerings- og politikinstrumenter. Cybersikkerhed gennem design for industrielle processer, operationer og udstyr kan mindske risici, potentielt reducere omkostningerne for både virksomheder og samfundet som helhed og dermed øge modstandsdygtigheden.

1.1 Robust infrastruktur og kritiske tjenester

EU's **regler om sikkerheden i net- og informationssystemer (NIS)** er kernen i det indre marked for cybersikkerhed. Kommissionen foreslår at ændre disse regler i et revideret NIS-direktiv for at øge **cyberrobustheden i alle relevante offentlige og private sektorer, der varetager en vigtig funktion for økonomi og samfund[34].** Revisionen er nødvendig for at mindske uoverensstemmelser på tværs af det indre marked ved at tilpasse kravene til

[32] Investeringer i hele forsyningskæden for digital teknologi, der bidrager til den digitale omstilling eller til at håndtere de deraf følgende udfordringer bør udgøre mindst 20 % — svarende til 134,5 mia. EUR — af genopretnings- og resiliensfaciliteten på 672,5 mia. EUR bestående af gavebistand og lån. EU-finansieringen i den flerårige finansielle ramme for 2021-2027 til cybersikkerhed under programmet for et digitalt Europa og til forskning i cybersikkerhed under Horisont Europa med særligt fokus på støtte til SMV'er, kan beløbe sig til i alt 2 mia. EUR plus medlemsstaternes og industriens investeringer.

[33] https://undocs.org/A/70/174.

[34] [*indsæt henvisning til NIS-forslag*]

anvendelsesområde, sikkerhed og indberetning om hændelser, nationalt tilsyn og national håndhævelse og de kompetente myndigheders kapacitet.

Et revideret NIS-direktiv vil danne grundlag for mere specifikke regler, som også er nødvendige for strategisk vigtige sektorer, herunder energi, transport og sundhed. For at sikre en konsekvent tilgang som bebudet i strategien for sikkerhedsunionen 2020-2025 fremsættes forslaget til det reviderede direktiv sammen med en revision af lovgivningen om kritisk infrastrukturs modstandsdygtighed[35]. Energiteknologier med indbyggede digitale komponenter og sikkerheden i de tilknyttede forsyningskæder er vigtige for kontinuiteten i væsentlige tjenester og for den strategiske kontrol med kritisk energiinfrastruktur. Kommissionen vil derfor foreslå foranstaltninger, herunder en "netkodeks" med regler for cybersikkerhed i grænseoverskridende elektricitetsstrømme, som skal vedtages inden udgangen af 2022. Som Kommissionen har foreslået , skal den finansielle sektor også styrke den digitale operationelle modstandsdygtighed og sikre evnen til at modstå alle former for IKT-relaterede afbrydelser og trusler[36]. På transportområdet har Kommissionen indarbejdet bestemmelser om cybersikkerhed[37] i EU-lovgivningen om luftfartssikkerhed og vil arbejde videre med at øge cyberrobustheden på tværs af alle transportformer. Styrkelse af cyberrobustheden i **demokratiske processer og institutioner** er et centralt element i den europæiske handlingsplan for demokrati, hvis mål er at sikre og fremme frie valg, demokratisk diskurs og medierpluralisme[38]. Endelig vil Kommissionen, for så vidt angår sikkerheden af infrastruktur og tjenester under det fremtidige rumprogram, fortsat uddybe Galileos cybersikkerhedsstrategi for den næste generation af globale satellitnavigationssystemer og andre nye komponenter i rumprogrammet[39].

1.2 Opbygning af et europæisk cyberskjold

Med udbredelsen af konnektivitet og de stedse mere sofistikerede cyberangreb har informationsudvekslings- og analysecentre, ISAC'er, en værdifuld funktion på bl.a. sektorniveau, fordi de muliggør informationsudveksling mellem flere interessenter om cybertrusler[40]. Dertil kommer, at netværk og computersystemer kræver konstant overvågning og analyse, hvis indtrængen og anomalier skal opdages i realtid. Mange private virksomheder, offentlige organisationer og nationale myndigheder har derfor oprettet enheder, som håndterer IT-sikkerhedshændelser og sikkerhedsoperationscentre.

Sikkerhedsoperationscentre er afgørende for indsamling af logfiler[41] og isolering af mistænkelige hændelser på de kommunikationsnetværk, de overvåger. Det gør de ved hjælp af signal- og mønsteridentifikation og udtræk af viden om trusler fra de store mængder data, der skal vurderes. De har medvirket til at afsløre skadelige eksekverbare filers aktiviteter og

---

[35] [indsæt henvisning til *forslag* til direktiv om kritiske enheders modstandsdygtighed]

[36] Forslag til forordning om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 og (EU) nr. 909/2014, COM(2020) 595 final.

[37] Kommissionens gennemførelsesforordning 2019/1583.

[38] Meddelelse om handlingsplanen for europæisk demokrati (COM(2020) 790). I henhold til planen støtter det europæiske samarbejdsnetværk om valg, der er medlemsstaternes valgnetværk, udsendelsen af fælles eksperthold for at imødegå trusler — herunder cybertrusler — mod valgprocesser: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en.

[39] Dette omfatter det nye statslige satellitkommunikationsinitiativ (GOVSATCOM) og rumaffald (SST).

[40] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing.

[41] På en sådan måde at de retshåndhævende myndigheder og retsvæsenet kan anvende dem som bevismateriale.

dermed til at dæmme op for cyberangreb. Det arbejde, der skal udføres i disse centre, er meget krævende og sker i et højt tempo, og derfor kan kunstig intelligens og navnlig maskinindlæringsteknikker yde uvurderlig støtte til medarbejderne[42].

Kommissionen foreslår, at der opbygges et **netværk af sikkerhedsoperationscentre i hele EU**[43], og at der ydes støtte til forbedring af eksisterende centre og oprettelse af nye centre. Den vil også støtte uddannelse af og kompetenceudvikling for personalet i disse centre. Den kan på grundlag af en behovsanalyse, der gennemføres med relevante interessenter og støttes af EU's Agentur for Cybersikkerhed (ENISA), afsætte over 300 mio. EUR i støtte til offentlig-privat og grænseoverskridende samarbejde om etablering af nationale og sektorspecifikke netværk, som også inddrager SMV'er, på grundlag af hensigtsmæssig styring, datadeling og sikkerhedsbestemmelser.

Medlemsstaterne opfordres til at deltage i investeringen af dette projekt. Centrene vil så kunne dele data mere effektivt, sammenholde de afslørede signaler og udarbejde trusselsefterretninger af høj kvalitet, som skal deles med informationsudvekslings- og analysecentre og nationale myndigheder og dermed muliggøre et mere omfattende situationskendskab. Målet er at forbinde så mange centre som muligt i hele EU for at skabe kollektiv viden og udveksle bedste praksis. Der vil blive ydet støtte til disse centre med henblik på at forbedre opdagelsen og analysen af og reaktionshastigheden i forbindelse med hændelser gennem den nyeste kapacitet inden for kunstig intelligens og maskinindlæring suppleret med supercomputerinfrastruktur, der er udviklet i EU af det europæiske fællesforetagende for højtydende databehandling[44].

Gennem et vedvarende samarbejde vil dette netværk udsende advarsler om cybersikkerhedshændelser til myndigheder og alle interesserede parter, herunder Den Fælles Cyberenhed (se afsnit 2.1). **Dette vil fungere som et egentligt cybersikkerhedsskjold for EU** i form af et solidt net af kontroltårne, der kan opdage potentielle trusler, før de kan forårsage omfattende skader.

1.3 En ultrasikker kommunikationsinfrastruktur

EU's statslige satellitkommunikation[45], der er en del af rumprogrammet, vil tilvejebringe sikker og omkostningseffektiv rumbaseret kommunikationskapacitet for de sikkerheds- og sikkerhedskritiske missioner og operationer, der forvaltes af EU og medlemsstaterne, herunder nationale sikkerhedsaktører og EU-institutionernes organer og agenturer.

Medlemsstaterne har forpligtet sig til at samarbejde med Kommissionen om udrulning af en sikker kvantekommunikationsinfrastruktur (QCI) i Europa[46]. Denne infrastruktur vil give

[42] Kilde: Undersøgelse foretaget af Ponemon Institute Research, "Improving the Effectiveness of the SOC, 2019", andre undersøgelser af brugen af kunstig intelligens i sikkerhedsoperationscentre er f.eks. Khraisat, A., Gondal, I., Vamplew, P. *et al.* Survey of intrusion detection systems: techniques, datasets and challenges, *Cybersecur* 2, 20 (2019).

[43] Der vil blive udviklet mere detaljerede ordninger for ledelse, driftsprincipper og finansiering med hensyn til disse centre, og hvordan de supplerer eksisterende strukturer såsom digitale innovationsknudepunkter.

[44] https://ec.europa.eu/digital-single-market/en/eurohpc-joint-undertaking.

[45] GOVSATCOM er en del af EU's rumprogram.

[46] EuroQCI-erklæringen er undertegnet af de fleste medlemsstater, og udvikling og udrulning af infrastrukturen skal finde sted i 2021-2027 med midler fra Horisont Europa og det digitale Europa og Den Europæiske Rumorganisation med forbehold af passende forvaltningsordninger. https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network.

offentlige myndigheder en helt ny måde at formidle fortrolige oplysninger på ved hjælp af en ultrasikker krypteringsform som beskyttelse mod cyberangreb, der er bygget med europæisk teknologi. Den vil bestå af to hovedkomponenter: eksisterende jordbaserede fibernet, der forbinder strategiske anlæg på nationalt og tværnationalt plan og forbundne rumsatellitter, som dækker hele EU, herunder de oversøiske territorier[47]. Dette initiativ til at udvikle og udrulle nye og mere sikre former for kryptering og til at udvikle nye metoder til beskyttelse af kritiske kommunikations- og dataaktiver kan bidrage til at holde følsomme oplysninger og dermed kritiske infrastrukturer sikre.

I og ud over dette perspektiv vil Kommissionen undersøge muligheden for at indføre et sikkert konnektivitetssystem med flere kredsløb. På grundlag af GOVSATCOM og QCI integrerer det banebrydende teknologier (såsom Quantum, 5G, KI og edge computing), der overholder de mest restriktive rammer for cybersikkerhed, for at støtte tjenester, der er sikret ved design, såsom pålidelig, sikker og omkostningseffektiv konnektivitet og krypteret kommunikation til kritiske statslige aktiviteter.

1.4 Sikring af næste generation af mobile bredbåndsnet

EU-borgere og -virksomheder, der anvender avancerede og innovative applikationer, som muliggøres af **5G og fremtidige generationer af netværk**, bør have adgang til den højeste sikkerhedsstandard. Medlemsstaterne har sammen med Kommissionen og med støtte fra ENISA med EU's 5G-værktøjskasse[48] fra januar 2020 indført en omfattende og objektiv risikobaseret tilgang til 5G-cybersikkerhed, som bygger på en vurdering af mulige beredskabsplaner og identifikation af de mest effektive foranstaltninger. Desuden konsoliderer EU sin kapacitet i 5G og derover for at undgå afhængighed og fremme en bæredygtig og mangfoldig forsyningskæde.

I december 2020 offentliggjorde Kommissionen en rapport om virkningerne af henstillingen af 26. marts 2019 om cybersikkerhed i 5G-net[49]. Det fremgik af rapporten, at der er gjort betydelige fremskridt, siden værktøjskassen blev vedtaget, og at de fleste medlemsstater i den nærmeste fremtid vil have gennemført en betydelig del af værktøjskassen, om end med visse forskelle og resterende mangler som allerede påpeget i statusrapporten, der blev offentliggjort i juli 2020[50].

I oktober 2020 opfordrede Det Europæiske Råd EU og medlemsstaterne til "at gøre fuld brug af 5G-cybersikkerhedsværktøjskassen" og "anvende de relevante restriktioner over for højrisikoleverandører med hensyn til centrale aktiver, der er udpeget som kritiske og

[47] Udviklingen af en rumkomponent er nødvendig for at opnå punkt-til-punkt-forbindelser over lange afstande (> 1 000 km), som jordbaseret infrastruktur ikke kan understøtte. Ved at udnytte kvantemekanikkens egenskaber vil denne infrastruktur i første omgang gøre det muligt for parterne at dele tilfældige hemmelige nøgler på en sikker måde til brug for kryptering og dekryptering af meddelelser. Den omfatter også etablering af en test- og overholdelsesinfrastruktur til vurdering af, om europæiske kvantekommunikationsenheder og -systemer er i overensstemmelse med QCI-infrastrukturen, og af deres certificering og validering, inden de integreres i QCI'en. Den vil blive udformet med henblik på at støtte yderligere applikationer, i takt med at de når den nødvendige teknologiske modenhed. Det nuværende OpenQKD-pilotprojekt (https://openqkd.eu/) er en forløber for denne test- og overholdelsesinfrastruktur.

[48] Meddelelse om sikker udrulning af 5G i EU — Gennemførelse af EU-værktøjskassen (COM(2020) 50).

[49] Kommissionens rapport om virkningerne af Kommissionens henstilling af 26. marts 2019 om cybersikkerheden i 5G-net, 15. december 2020.

[50] NIS-samarbejdsgruppens rapport om gennemførelsen af værktøjskassen, 24. juli 2020.

følsomme i EU's koordinerede risikovurderinger ... på grundlag af fælles objektive kriterier"[51].

Fremadrettet bør EU og medlemsstaterne sikre, at de identificerede risici er blevet afbødet på en passende og koordineret måde, navnlig for så vidt angår målet om at minimere eksponeringen for højrisikoleverandører og undgå afhængighed af disse leverandører på nationalt plan og EU-plan, og at der tages hensyn til enhver ny væsentlig udvikling eller risiko. Medlemsstaterne opfordres til at gøre fuld brug af værktøjskassen i forbindelse med deres investeringer i digital kapacitet og konnektivitet.

På grundlag af rapporten om virkningerne af henstillingen fra 2019 opfordrer Kommissionen medlemsstaterne til at have gennemført de vigtigste værktøjskasseforanstaltninger senest i andet kvartal af 2021. Den opfordrer også medlemsstaterne til fortsat sammen at overvåge de fremskridt, der gøres, og sikre yderligere tilpasning af tilgangene. På EU-plan vil tre hovedmål blive fulgt for at støtte denne proces: sikring af yderligere konvergens i tilgange til risikobegrænsning i hele EU, støtte til løbende udveksling af viden og kapacitetsopbygning og fremme af modstandsdygtighed i forsyningskæden og andre af EU's strategiske sikkerhedsmål. Konkrete foranstaltninger i forbindelse med disse centrale mål er beskrevet i det særlige tillæg til denne meddelelse.

Kommissionen vil fortsat arbejde tæt sammen med medlemsstaterne for at opfylde disse mål og aktioner med støtte fra ENISA (se bilaget).

EU's 5G-værktøjskassetilgang har tillige øget interessen for tredjelande, der i øjeblikket udvikler deres tilgange til sikring af deres kommunikationsnet. Kommissionens tjenestegrene er sammen med Tjenesten for EU's Optræden Udadtil og netværket af EU-delegationer rede til på anmodning at afgive supplerende oplysninger om sin omfattende, objektive og risikobaserede tilgang til myndigheder rundt om i verden.

1.5 Et sikkert tingenes internet

Enhver netforbunden ting indeholder sårbarheder, der kan udnyttes med potentielt omfattende konsekvenser. Reglerne for det indre marked omfatter beskyttelsesforanstaltninger mod usikre produkter og tjenesteydelser. Kommissionen arbejder allerede nu på at sikre **gennemsigtige sikkerhedsløsninger og certificering i henhold til forordningen om cybersikkerhed** og på at skabe incitamenter til udvikling af sikre produkter og tjenester, uden at der gås på kompromis med ydeevnen[52]. Den vil vedtage sit første rullende EU-arbejdsprogram i første kvartal af 2021 (ajourføres mindst hvert tredje år) for at give industri, nationale myndigheder og standardiseringsorganer mulighed for på forhånd at forberede sig på fremtidige europæiske cybersikkerhedscertificeringsordninger[53]. Efterhånden som

[51] EUCO 13/20, ekstraordinært møde i Det Europæiske Råd (1.-2. oktober 2020) — Konklusioner.

[52] Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed) og om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed). Forordningen om cybersikkerhed fremmer IKT-certificering på EU-plan gennem en europæisk ramme for cybersikkerhedscertificering for etablering af frivillige europæiske cybersikkerhedscertificeringsordninger med henblik på at sikre et tilstrækkeligt cybersikkerhedsniveau for IKT-produkter, -tjenester og -processer i EU samt mindske fragmenteringen af det indre marked med hensyn til cybersikkerhedscertificeringsordninger i EU. Parallelt hermed er der en tendens til, at cybersikkerhedsvurderingsselskaber er baseret uden for EU med deraf følgende begrænset gennemsigtighed og tilsyn: https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings.

[53] Jf. artikel 47, stk. 5, i forordningen om cybersikkerhed.

tingenes internet udbredes, skal regler, der kan håndhæves, styrkes, både for at sikre generel modstandsdygtighed og for at styrke cybersikkerheden.

Kommissionen vil overveje en samlet tilgang, herunder eventuelle **nye horisontale regler for at forbedre cybersikkerheden for alle forbundne produkter og tilknyttede tjenester, der bringes i omsætning i det indre marked**[54]. Sådanne regler kan omfatte en **ny pligt for fabrikanter af forbundne enheder** til at tage hånd om softwarens sårbarhed, herunder videreførelsen af software og sikkerhedsopdateringer, samt sikre, at personoplysninger og andre følsomme oplysninger slettes, når enhederne tages ud af brug. Disse regler vil styrke initiativet "den forældede software til reparation", der blev præsenteret i handlingsplanen for den cirkulære økonomi, og supplere de igangværende foranstaltninger, som vedrører specifikke typer produkter, såsom obligatoriske krav, der skal foreslås for markedsadgang for visse trådløse produkter (gennem vedtagelse af en delegeret retsakt i henhold til radioudstyrsdirektivet[55]), og målet om at gennemføre cybersikkerhedsregler for motorkøretøjer for alle nye køretøjstyper fra juli 2022[56]. De vil desuden bygge videre på den foreslåede revision af de generelle produktsikkerhedsregler, som ikke direkte omhandler cybersikkerhedsaspekter[57].

1.6 Større global internetsikkerhed

Et sæt centrale protokoller og en støtteinfrastruktur sikrer internettets funktionalitet og integritet i hele verden[58]. Dette sæt omfatter DNS og dets hierarkiske og delegerede system af zoner, begyndende i toppen af hierarkiet med rodzonen og de tretten DNS-rodservere[59], som World Wide Web er afhængigt af. Kommissionen agter at udarbejde **en beredskabsplan med støtte fra EU-midler til håndtering af ekstreme scenarier, som påvirker integriteten og tilgængeligheden af det globale DNS-rodsystem**. Den vil sammen med ENISA, medlemsstaterne, de to EU-udbydere af DNS-rodservere[60] og multiinteressentsamfundet vurdere disse operatørers rolle med hensyn til at sikre, at internettet forbliver tilgængeligt på verdensplan under alle omstændigheder.

For at en kunde kan få adgang til en ressource under et bestemt domænenavn på internettet, skal dennes anmodning (typisk om en Uniform Resource Locator eller URL) oversættes til en IP-adresse ved henvisning til DNS-navneservere. Men folk og organisationer i EU er i stigende grad afhængige af nogle få offentlige DNS-oversættere, der administreres af enheder uden for EU. En sådan konsolidering af DNS-oversættelsen i hænderne på nogle få

[54] Rådet opfordrer i sine konklusioner til horisontale foranstaltninger vedrørende internetsikkerhed i forbindelse med netforbundne enheder, 13629/20, 2. december 2020.
[55] Direktiv 2014/53/EU.
[56] Følger FN-regulativet, der blev vedtaget i juni 2020: http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf.
[57] Revision af de gældende generelle produktsikkerhedsregler (direktiv 2001/95/EF). Der er desuden planlagt forslag til tilpasning af regler for producentansvar i den digitale kontekst inden for rammerne af EU's lovramme for erstatningsansvar.
[58] "Den offentligt tilgængelige kerne af det åbne internet, dvs. dets vigtigste protokoller og infrastruktur, som er et globalt offentligt gode, sikrer internettet som helhed dets grundlæggende funktioner og understøtter dets normale drift. ENISA bør støtte sikkerheden for den offentlige tilgængelige kerne af det åbne internet og stabiliteten i dets drift, herunder, men ikke kun, de vigtigste protokoller (navnlig DNS, BGP og Ipv6), driften af domænenavnssystemet (såsom driften af alle topdomæner) og driften af rodzonen", Betragtning 23 i forordningen om cybersikkerhed.
[59] https://www.iana.org/domains/root/servers.
[60] i.rodservere, der drives af Netnod i Sverige, og k.rootservere, der drives af RIPE NCC i Nederlandene.

virksomheder[61] gør selve processen sårbar i tilfælde af væsentlige begivenheder, der berører én stor udbyder, og gør det vanskeligere for EU's myndigheder at håndtere eventuelle ondsindede cyberangreb og større geopolitiske og tekniske hændelser[62].

For at mindske sikkerhedsproblemerne ved markedskoncentration vil Kommissionen tilskynde relevante interessenter, herunder EU-virksomheder, internetudbydere og browsere, til at vedtage en diversificeringsstrategi for DNS-oversættelser. Kommissionen agter også at bidrage til sikker internetkonnektivitet ved at støtte udviklingen af en offentlig europæisk **DNS-tjeneste.** Dette "DNS4EU"-initiativ bliver en alternativ europæisk tjeneste for adgang til det globale internet. DNS4EU bliver gennemsigtigt, vil være i overensstemmelse med de nyeste standarder og regler for databeskyttelse gennem design og standardindstillinger og for privatlivets fred og udgøre en del af EU's Industrial Alliance on Data and Cloud[63].

Kommissionen vil også i samarbejde med medlemsstaterne og industrien **fremskynde udbredelsen af vigtige internetstandarder, herunder IPv6[64] og veletablerede standarder for internetsikkerhed og god praksis for DNS, routing og e-mail-sikkerhed[65]**, men udelukker ikke lovgivningsmæssige foranstaltninger såsom en europæisk udløbsklausul for IPv4 for at styre markedet, hvis der ikke gøres tilstrækkelige fremskridt hen imod deres vedtagelse. EU bør (som f.eks. under EU-Afrika-strategien[66]) fremme gennemførelsen af disse standarder i partnerlandene som et middel til at støtte udviklingen af det globale, åbne internet og modvirke lukkede, kontrolbaserede internetmodeller. Endelig vil Kommissionen overveje behovet for en mekanisme til mere systematisk overvågning og indsamling af aggregerede data om internettrafik og rådgivning om potentielle afbrydelser[67].

1.7 Øget tilstedeværelse i teknologiforsyningskæden

Med den planlagte finansielle støtte til cybersikker digital omstilling under den flerårige finansielle ramme for 2021-2027 har EU en enestående mulighed for at samle sine aktiver og dermed fremme sin industristrategi[68] og sit lederskab inden for digitale teknologier og cybersikkerhed i hele den digitale forsyningskæde (herunder data og cloud, næste generation af processorteknologier, ultrasikker konnektivitet og 6G-net) i overensstemmelse med EU's værdier og prioriteter. Den offentlige sektors intervention bør være baseret på værktøjerne i EU's regelsæt for offentlige indkøb og vigtige projekter af fælleseuropæisk interesse. Derudover kan der frigøres private investeringer gennem offentlig-private partnerskaber (herunder på grundlag af erfaringerne fra det kontraktlige offentlig-private partnerskab om

[61] Konsolidering på DNS-markedet — hvor meget, hvor hurtigt, hvor farligt? (), Evidence of decreasing Internet entropy – the lack of redundancy in DNS resolution by major websites and services ( ).
[62] Der er også dokumentation for, at DNS-data kan anvendes til profilering, hvilket har betydning for privatlivets fred og databeskyttelsesrettigheder.
[63] Fælles erklæring: Building the next generation cloud for businesses and the public sector in the EU: https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe
[64] Udrulningen af IPv6 er længere fremme nu på grund af det reducerede udbud af og stigningen i omkostningerne til IPv4-adresser. Udrulningen af IPv6 sker imidlertid ujævnt i EU.
[65] Disse standarder omfatter DNSSEC, HTTPS, DNS-over-HTTPS (DoH), DNS-over-TLS (DoT), SPF, DKIM, DMARC, STARTTLS, DANE og normer for routing og god praksis, f.eks. Mutually Agreed Norms for Routing Security (MANRS).
[66] Fælles meddelelse, "Mod en samlet strategi med Afrika", 9.3.2020, JOIN(2020) 4 final.
[67] Et sådant "internetobservatorium" kan indgå i aktiviteterne i det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed, forslag til forordning om oprettelse af det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed og netværket af nationale koordinationscentre (COM(2018) 630 final).
[68] Meddelelse om en ny industristrategi for Europa (COM(2020) 102 final).

cybersikkerhed og gennemførelsen deraf gennem den europæiske cybersikkerhedsorganisation), venturekapital til støtte for SMV'er eller industrielle alliancer og strategier vedrørende teknologikapacitet.

Der vil også blive lagt særlig vægt på det tekniske støtteinstrument[69] og på SMV'ernes bedste brug af de seneste cybersikkerhedsværktøjer — navnlig dem, der ikke er omfattet af anvendelsesområdet for det reviderede NIS-direktiv — herunder gennem særlige aktiviteter under de digitale innovationsknudepunkter i programmet for et digitalt Europa. Målet er at udløse et tilsvarende investeringsbeløb fra medlemsstaterne, som skal modsvares af industrien inden for rammerne af et partnerskab, der forvaltes i samarbejde med medlemsstaterne i det foreslåede **industri-, teknologi- og forskningskompetencecenter for cybersikkerhed og netværket af koordinationscentre (CCCN)**. CCCN bør med input fra industrien og akademiske kredse spille en central rolle med hensyn til at udvikle EU's teknologiske suverænitet inden for cybersikkerhed, opbygge kapacitet til at sikre følsomme infrastrukturer såsom 5G og mindske afhængigheden af andre dele af verden for de mest afgørende teknologier.

Kommissionen har til hensigt, eventuelt sammen med CCCN, at støtte udviklingen af et dedikeret program for cybersikkerhedsmasterprogrammer og bidrage til en fælles europæisk køreplan for forskning og innovation i cybersikkerhed efter 2020. Investeringer gennem CCCN vil også bygge på det samarbejde om forskning og udvikling, der udføres af netværk af ekspertisecentre for cybersikkerhed, og samle Europas bedste forskerhold og industrien om at udforme og gennemføre fælles forskningsdagsordener i overensstemmelse med køreplanen for den europæiske cybersikkerhedsorganisation[70]. Kommissionen vil fortsat basere sig på ENISA's og Europols forskningsarbejde, og vil også fortsat som en del af Horisont Europa støtte individuelle internetinnovatorer, der udvikler privatlivsfremmende og sikre kommunikationsteknologier baseret på open source-software og hardware, som i øjeblikket er omfattet af internetinitiativet Next Generation.

1.8 En cyberkvalificeret EU-arbejdsstyrke

EU's indsats for at opkvalificere arbejdsstyrken, udvikle, tiltrække og fastholde de bedste talenter inden for cybersikkerhed og investere i forskning og innovation i verdensklasse udgør en vigtig del af beskyttelsen mod cybertrusler generelt. Der er et stort potentiale inden for dette område. Der skal derfor lægges særlig vægt på at udvikle, tiltrække og fastholde mere forskelligartede talenter. Den reviderede handlingsplan for digital uddannelse vil skabe opmærksomhed omkring cybersikkerhed hos privatpersoner, navnlig børn og unge, og blandt virksomheder, navnlig SMV'er[71]. Den vil også tilskynde kvinder 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. Derudover vil Kommissionen sammen med Den Europæiske Unions Kontor for Intellektuel Ejendomsret under Europol, ENISA, medlemsstaterne og den private sektor udvikle oplysningsværktøjer og retningslinjer med henblik på at øge de europæiske virksomheders modstandsdygtighed **over for cyberbaseret tyveri af intellektuel ejendom**[72].

[69] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:0409:FIN.
[70] https://ecs-org.eu/working-groups/wg6-sria-and-cyber-security-technologies.
[71] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_da.
[72] https://ec.europa.eu/commission/presscorner/detail/da/IP_20_2187.

Uddannelse – herunder erhvervsuddannelse, oplysning og øvelser – bør desuden øge cybersikkerheden og cyberforsvarskapaciteten på EU-plan yderligere. I denne forbindelse bør de relevante EU-aktører såsom ENISA, Det Europæiske Forsvarsagentur (EDA) og Det Europæiske Sikkerheds- og Forsvarsakademi (ESDC)[73] søge at skabe synergi mellem deres respektive aktiviteter.

Strategiske initiativer

EU bør sikre:

- at det reviderede NIS-direktiv vedtages
- at de lovgivningsmæssige foranstaltninger for et sikkert tingenes internet iværksættes
- at de offentlige og private investeringer i perioden 2021-2027 når op på 4,5 mia. EUR via CCCN's investering i cybersikkerhed (navnlig gennem programmet for et digitalt Europa, Horisont Europa og genopretningsfaciliteten)
- at der indføres et EU-netværk af sikkerhedsoperationscentre baseret på kunstig intelligens og en ultrasikker kommunikationsinfrastruktur ved udnyttelse af kvanteteknologier
- at der i udbredt grad indføres cybersikkerhedsteknologier gennem målrettet støtte til SMV'er under de digitale innovationsknudepunkter
- at der udvikles en DNS-resolvertjeneste på EU-plan som et sikkert og åbent alternativ for EU's borgere, virksomheder og offentlige forvaltninger i deres tilgang til internettet og
- at gennemførelsen af 5G-værktøjskassen afsluttes senest i andet kvartal af 2021(jf. bilag).

2. OPBYGNING AF OPERATIONEL KAPACITET TIL AT FOREBYGGE, MODVIRKE OG REAGERE

Cyberhændelser, hvad enten der er tale om utilsigtede handlinger eller forsætlige handlinger udført af kriminelle, statslige eller andre ikkestatslige aktører, kan medføre enorme skader. Sådanne hændelser indebærer ofte udnyttelse af tredjeparters tjenester, hardware og software til at kompromittere et endeligt mål, og deres omfang og kompleksitet gør det vanskeligt at gøre front mod EU's kollektive trusselsmiljø uden systematisk og omfattende informationsudveksling og samarbejde om en fælles indsats. EU ønsker **gennem fuldstændig gennemførelse af lovgivningsværktøjer, mobilisering og samarbejde** at støtte medlemsstaterne i deres bestræbelser på at beskytte deres borgere og deres økonomiske og nationale sikkerhedsinteresser under fuld overholdelse af de grundlæggende rettigheder og frihedsrettigheder samt retsstatsprincippet. En række fællesskaber bestående af netværk, EU-institutioner, -organer og -agenturer og medlemsstaternes myndigheder har ansvaret for at forebygge, modvirke, hindre og reagere på cybertrusler ved anvendelse af deres respektive instrumenter og initiativer[74]. Disse fællesskaber omfatter: i) NIS-myndigheder såsom

[73]Via platformen for uddannelse inden for cyberforsvar, træning, øvelser og evaluering (ETEE).

[74] Herunder støtte fra Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) til operationelt samarbejde og krisestyring, CSIRT-netværket, Cyber Crises Liaison Organisation Network (CyCLONe, der som foreslået i

CSIRT'er og katastrofeberedskab, ii) retshåndhævende og retslige myndigheder, iii) cyberdiplomati og iv) cyberforsvar.

2.1 En fælles cyberenhed

En fælles cyberenhed vil tjene som en virtuel og fysisk samarbejdsplatform for de forskellige cybersikkerhedsfællesskaber i EU, med fokus på operationel og teknisk koordinering til imødegåelse af større grænseoverskridende cyberhændelser og -trusler.

Den fælles cyberenhed er et vigtigt skridt fremad med henblik på at færdiggøre den **europæiske ramme for håndtering af cybersikkerhedskriser**. Som nævnt i kommissionsformandens politiske retningslinjer[75] bør enheden give medlemsstaterne og EU's institutioner, organer og agenturer mulighed for at anvende de eksisterende strukturer, ressourcer og færdigheder fuldt ud og fremme et "**need-to-share**"-mindset. Den vil give mulighed for at konsolidere de hidtidige fremskridt for så vidt angår gennemførelsen af henstillingen fra 2017 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser ("planen")[76]. Den vil endvidere give mulighed for yderligere at styrke samarbejdet omkring planens arkitektur og udnytte de fremskridt, der hidtil er gjort, navnlig inden for NIS-samarbejdsgruppen og CyCLONe-netværket.

Dette vil kunne afhjælpe to **centrale mangler**, som for øjeblikket øger sårbarheden og skaber ineffektivitet i reaktionen på grænseoverskridende trusler og hændelser, som er rettet mod Unionen. For det første har civile, diplomatiske og retshåndhævende **fællesskaber** og fællesskaber inden for cybersikkerhedsforsvar endnu ikke et fælles rum, hvor de kan pleje et struktureret samarbejde og fremme det operationelle og tekniske samarbejde. For det andet har relevante interessenter inden for cybersikkerhed endnu ikke været i stand til at udnytte det fulde **potentiale** af det operationelle samarbejde og den gensidige bistand inden for eksisterende netværk og fællesskaber. Der mangler også en platform, som muliggør operationelt samarbejde med den private sektor. Enheden bør forbedre og accelerere koordinationsindsatsen og give EU mulighed for at imødegå og reagere på væsentlige cyberhændelser og -kriser.

Den fælles cyberenhed vil ikke være et nyt selvstændigt organ og vil heller ikke berøre de nationale cybersikkerhedsmyndigheders eller EU-deltagernes kompetencer og beføjelser. Enheden vil snarere fungere som en bagstopper, hvor deltagerne kan trække på hinandens støtte og ekspertise, navnlig hvis forskellige cyberfællesskaber skal arbejde tæt sammen. Samtidig viser nye begivenheder, at EU er nødt til at øge sit ambitionsniveau og sin parathed til at håndtere cybertrusselsbilledet og de faktiske forhold. Som led i deres bidrag til den fælles cyberenhed vil EU-aktørerne (Kommissionen og EU's agenturer og organer) derfor

---

det reviderede NIS-direktiv bliver til EU-CyCLONe), NIS-samarbejdsgruppen, rescEU, Det Europæiske Center for Bekæmpelse af Cyberkriminalitet og Europols fælles taskforce vedrørende cyberkriminalitet (Joint Cybercrime Action Task Force) og beredskabsprotokollen om retshåndhævelsesindsatsen (Law Enforcement Emergency Response Protocol), Den Europæiske Unions Efterretnings- og Situationscenter (EU INTCEN) og den cyberdiplomatiske værktøjskasse, den fælles efterretningsanalysekapacitet (SIAC), cyberprojekterne under det permanente strukturerede samarbejde (PESCO), navnlig projektet vedrørende cyberberedskabshold og gensidig bistand inden for cybersikkerhed (CRRT).

[75] "En mere ambitiøs Union: Min dagsorden for Europa", Politiske retningslinjer for den næste Europa-Kommission 2019-2024, af kandidat til posten som formand for Europa-Kommissionen Ursula von der Leyen.

[76] Henstilling C(2017) 6100 final af 13.9.2017 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser.

være villige til at øge deres ressourcer og kapacitet betydeligt for at styrke deres beredskab og modstandsdygtighed.

Den fælles cyberenhed vil opfylde tre hovedmålsætninger. For det første vil den sikre **beredskabet** på tværs af cybersikkerhedsfællesskaber. For det andet vil den gennem informationsudveksling sikre en konstant **situationsbevidsthed** hos alle parter, og for det tredje vil den styrke den koordinerede **indsats** og genopretning. For at opfylde disse målsætninger bør enheden bygge på veldefinerede **blokke og mål** såsom at garantere **sikker og hurtig informationsudveksling**, forbedre **samarbejdet** blandt deltagerne, herunder interaktionen mellem medlemsstaterne og de relevante EU-enheder, etablere strukturerede **partnerskaber med et pålideligt industrigrundlag** og fremme en koordineret tilgang til **samarbejdet med eksterne partnere**. Med henblik herpå kan enheden ud fra en kortlægning af den kapacitet, der er til rådighed på nationalt og EU-plan, lette opstillingen af en ramme for samarbejdet.

For at den fælles cyberenhed kan blive omdrejningspunktet for EU's operationelle cybersikkerhedssamarbejde, vil Kommissionen arbejde sammen med medlemsstaterne og de relevante EU-institutioner, -organer og -agenturer, herunder ENISA, CERT-EU og Europol, for at fremme en **trinvis og inkluderende tilgang** under fuld overholdelse af alle involverede parters kompetencer og mandater. I overensstemmelse hermed kan enheden bidrage til yderligere samarbejde mellem komponenterne i specifikke cyberenheder, når disse komponenter finder det nødvendigt.

Det foreslås at følge fire hovedtrin ved oprettelsen af den fælles cyberenhed:

- *Definition* ved at kortlægge den kapacitet, der er til rådighed på nationalt og EU-plan
- *Forberedelse* ved at opstille en ramme for struktureret samarbejde og bistand
- *Udbredelse* ved at trække på deltagernes ressourcer og gennemføre rammen, så den fælles cyberenhed bliver operationel
- *Udvidelse* ved at styrke den koordinerede reaktionskapacitet med input fra industri og partnere.

På baggrund af høringen af medlemsstaterne og EU's institutioner, organer og agenturer[77] vil Kommissionen med inddragelse af den højtstående repræsentant og i overensstemmelse med dennes kompetencer senest i februar 2021 præsentere proceduren, milepælene og tidsplanen for **definition, forberedelse, udbredelse og udvidelse af den fælles cyberenhed**.

2.2 Bekæmpelse af cyberkriminalitet

Vores afhængighed af onlineværktøjer har øget angrebsfladen for cyberkriminelle eksponentielt og betyder, at efterforskningen af stort set alle former for kriminalitet har en digital komponent. Desuden er centrale dele af vores samfund truet af cyberaktører og af dem, der anvender cyberværktøjer til at planlægge og udføre deres ulovlige handlinger. Der er derfor en tæt forbindelse til EU's overordnede sikkerhedspolitik, som det fremgår af de

[77] Høring af medlemsstaterne (bl.a. under Blue OLEx20-øvelsen med deltagelse af lederne af de nationale cybersikkerhedsmyndigheder) samt EU's institutioner, organer og agenturer i perioden juli til november 2020.

cyberrelaterede dele af strategien for EU's sikkerhedsunion fra 2020 og af EU's dagsorden for bekæmpelse af terrorisme[78].

Bekæmpelsen af cyberkriminalitet er en central faktor for at garantere cybersikkerheden: Den afskrækkende virkning kan ikke opnås alene ved at øge modstandsdygtigheden, men kræver også identifikation og retsforfølgning af lovovertræderne. Det er derfor afgørende at styrke samarbejdet og drøftelserne mellem cybersikkerhedsaktørerne og de retshåndhævende myndigheder. På EU-plan har Europol og ENISA derfor allerede opbygget et stærkt samarbejde, hvor de har afholdt fælles konferencer og workshopper og udarbejdet fælles rapporter til Kommissionen, medlemsstaterne og andre interessenter om cybersikkerhedstrusler og teknologiske udfordringer. Kommissionen vil fortsat støtte denne integrerede tilgang til at sikre en sammenhængende og effektiv reaktion baseret på et omfattende informationsbillede.

Som en vigtig del af denne reaktion skal EU og de nationale myndigheder øge og forbedre de retshåndhævende myndigheders kapacitet til at efterforske cyberkriminalitet under fuld overholdelse af de grundlæggende rettigheder og under hensyntagen til den påkrævede balance mellem de forskellige rettigheder og interesser. EU bør være i stand til at bekæmpe cyberkriminalitet med en lovgivning, der er egnet til formålet, og som er gennemført fuldt ud, idet der i særlig grad fokuseres på bekæmpelse af seksuelt misbrug af børn online og digital efterforskning, herunder kriminalitet på "det mørke net". De retshåndhævende myndigheder skal være fuldt udrustede til at foretage digital efterforskning. Kommissionen vil derfor komme med en handlingsplan til forbedring af de retshåndhævende myndigheders digitale kapacitet, hvor de får stillet de nødvendige færdigheder og værktøjer til rådighed. Derudover vil Europol gå et skridt videre i sin rolle som ekspertisecenter for at støtte de nationale retshåndhævende myndigheder i deres bekæmpelse af cyberbaseret og cyberafhængig kriminalitet og bidrage til fastlæggelsen af fælles kriminaltekniske standarder (gennem Europols innovationslaboratorium og -knudepunkt). Alle disse aktiviteter kræver en passende gennemførelse fra medlemsstaternes side, og de derfor opfordres til at gøre brug af Fonden for Intern Sikkerheds nationale programmer og foreslå projekter i forbindelse med indkaldelse af forslag som led i den tematiske facilitet.

Kommissionen vil gøre brug af alle egnede midler, herunder traktatbrudsprocedurer, for at sikre, at 2013-direktivet om angreb på informationssystemer[79] gennemføres fuldt ud, herunder også bestemmelserne om medlemsstaternes statistiske indberetninger. Den vil skærpe indsatsen for at forhindre misbrug af domænenavne til distribution af ulovligt indhold og tilstræbe, at der er nøjagtige registreringsdata til rådighed, ved fortsat at samarbejde med Internet Corporation for Assigned Names and Numbers (ICANN) og andre interessenter i internetforvaltningssystemet, navnlig gennem arbejdsgruppen om offentlig sikkerhed i ICANN's mellemstatslige rådgivende udvalg. Forslaget i det reviderede NIS-direktiv tager således sigte på at vedligeholde nøjagtige og komplette databaser over domænenavne og registreringsdata — "WHOIS-data" — og på at give lovlig adgang til sådanne data, som er afgørende for at sikre domænenavnssystemets sikkerhed, stabilitet og modstandsdygtighed.

[78] Meddelelse fra Kommissionen "A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond" af 9.12.2020 (COM(2020) 795 final).
[79] Direktiv 2013/40/EU om angreb på informationssystemer.

Kommissionen vil endvidere fortsætte sit arbejde for at tilvejebringe egnede kanaler og klarlægge reglerne for grænseoverskridende adgang til elektronisk bevismateriale i forbindelse med strafferetlig efterforskning (hvilket der er behov for i 85 % af tilfældene, og 65 % af det samlede antal anmodninger er rettet til udbydere i en anden jurisdiktion) ved at lette vedtagelsen og den efterfølgende gennemførelse af pakken om elektronisk bevismateriale og de praktiske foranstaltninger[80]. Europa-Parlamentets og Rådets hurtige vedtagelse af forslagene om elektronisk bevismateriale er afgørende for at give aktørerne et effektivt værktøj. Elektronisk bevismateriale skal være læsbart, og Kommissionen vil derfor arbejde videre på at støtte retshåndhævelseskapaciteten inden for digital efterforskning, herunder håndtering af kryptering i forbindelse med strafferetlig efterforskning, samtidig med at krypteringens funktion, som er at beskytte de grundlæggende rettigheder og cybersikkerheden, opretholdes.

2.3 EU's cyberdiplomatiske værktøjskasse

EU har anvendt sin **cyberdiplomatiske værktøjskasse**[81] til at forebygge, modvirke, hindre og reagere på ondsindede cyberaktiviteter. Efter indførelsen af den retlige ramme for målrettede restriktive foranstaltninger til bekæmpelse af cyberangreb i maj 2019[82] listeopførte EU seks personer og tre enheder, der var ansvarlige for eller involveret i forskellige cyberangreb rettet mod EU og medlemsstaterne, i juli 2020[83]. Yderligere to personer og ét organ blev opført på listen i oktober 2020[84]. Ondsindede cyberaktiviteter, herunder også dem, der "brænder langsomt", bør bekæmpes med en effektiv og omfattende diplomatisk indsats fra EU's side under anvendelse af alle de foranstaltninger, som er til rådighed på EU-plan.

En hurtig og effektiv diplomatisk indsats fra EU's side kræver en solid fælles situationsbevidsthed og en evne til hurtigt at udarbejde en fælles EU-holdning. Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik vil tilskynde til og lette oprettelsen af en **EU-arbejdsgruppe om cyberintelligens for medlemsstaterne** under EU's Efterretnings- og Situationscenter (INTCEN) med henblik på at fremme strategisk efterretningssamarbejde om cybertrusler og -aktiviteter. Dette arbejde vil yderligere støtte EU's situationsbevidsthed og beslutningstagning om en fælles diplomatisk indsats.

---

[80] COM(2018) 225 og 226, C(2020) 2779 final. Navnlig modtog Sirius-projektet for nylig yderligere midler under partnerskabsinstrumentet til at forbedre kanalerne til opnåelse af lovlig grænseoverskridende adgang til elektronisk bevismateriale i forbindelse med strafferetlig efterforskning (hvilket er nødvendigt i efterforskningen af 85 % af alvorlige forbrydelser, og 65 % af det samlede antal anmodninger er rettet til udbydere i en anden jurisdiktion) og fastlægge indbyrdes forenelige regler på internationalt plan.

[81] https://www.consilium.europa.eu/da/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/.

[82] Rådets afgørelse (FUSP) 2019/797 af 17. maj 2019 om restriktive foranstaltninger til bekæmpelse af cyberangreb, der truer Unionen eller dens medlemsstater (EUT L 129I af 17.5.2019, s. 13), og Rådets forordning (EU) 2019/796
af 17. maj 2019 om restriktive foranstaltninger til bekæmpelse af cyberangreb, der truer Unionen eller dens medlemsstater (EUT L 129I af 17.5.2019, s. 1).

[83] Rådets afgørelse (FUSP) 2020/1127 af 30. juli 2020 om ændring af afgørelse (FUSP) 2019/797 om restriktive foranstaltninger til bekæmpelse af cyberangreb, der truer Unionen eller dens medlemsstater (ST/9564/2020/INIT) (EUT L 246 af 30.7.2020, s. 12), og Rådets gennemførelsesforordning (EU) 2020/1125 af 30. juli 2020 om gennemførelse af forordning (EU) 2019/796 om restriktive foranstaltninger til bekæmpelse af cyberangreb, der truer Unionen eller dens medlemsstater (ST/9568/2020/INIT) (EUT L 246 af 30.7.2020, s. 4.).

[84] Rådets afgørelse (FUSP) 2020/1537 af 22. oktober 2020 om ændring af afgørelse (FUSP) 2019/797 om restriktive foranstaltninger til bekæmpelse af cyberangreb, der truer Unionen eller dens medlemsstater (EUT L 351I af 22.10.2020, s. 5), og Rådets gennemførelsesforordning (EU) 2020/1536 af 22. oktober 2020 om gennemførelse af forordning (EU) 2019/796 om restriktive foranstaltninger til bekæmpelse af cyberangreb, der truer Unionen eller dens medlemsstater (EUT L 351I af 22.10.2020, s. 1).

Arbejdsgruppen skal samarbejde med eksisterende strukturer[85], herunder eventuelt dem, der dækker den bredere trussel vedrørende hybrid og udenlandsk indblanding, for at indhente oplysninger om og vurdere situationsbevidstheden.

For at styrke sin evne til at forebygge, modvirke, hindre og reagere på ondsindet adfærd i cyberspace vil den højtstående repræsentant med inddragelse af Kommissionen i overensstemmelse med dennes kompetencer stille forslag om, at EU gør sin **holdning til et cyberforsvar med afskrækkende virkning** endnu mere klar. Med udgangspunkt i det arbejde, der hidtil er gjort ved anvendelse af den cyberdiplomatiske værktøjskasse, bør holdningen bidrage til ansvarlig statslig adfærd og samarbejde i cyberspace og udstikke særlige retningslinjer for imødegåelse af de cyberangreb, der har den største virkning, navnlig dem, der er rettet mod vores kritiske infrastruktur, demokratiske institutioner og processer[86], samt cyberangreb på forsyningskæder og cyberbaseret tyveri af intellektuel ejendom. Holdningen bør skitsere, hvordan EU og medlemsstaterne kan udnytte deres politiske, økonomiske, diplomatiske, juridiske og strategiske kommunikationsværktøjer til at bekæmpe ondsindede cyberaktiviteter, og se på, hvordan EU og medlemsstaterne kan blive bedre til at finde kilden til ondsindede cyberaktiviteter. Derudover vil den højtstående repræsentant i samarbejde med Rådet og Kommissionen undersøge **yderligere foranstaltninger under den cyberdiplomatiske værktøjskasse**, herunder eventuelle yderligere muligheder for restriktive foranstaltninger, og muligheden for **afstemning med kvalificeret flertal om listeopførelser under den horisontale sanktionsordning til bekæmpelse af cyberangreb.** Desuden bør EU gøre en yderligere indsats for at **styrke samarbejdet med internationale partnere**, herunder NATO, for at fremme den fælles forståelse af trusselsbilledet, udvikle samarbejdsmekanismer og identificere forskellige former for samarbejdsbaseret diplomatisk reaktion.

Den højtstående repræsentant vil med inddragelse af Kommissionen endvidere stille forslag om en ajourføring af **gennemførelsesretningslinjerne for den cyberdiplomatiske værktøjskasse[87]**, bl.a. med henblik på at øge effektiviteten af beslutningsprocessen, og fortsætte med regelmæssigt at afholde øvelser og foretage vurderinger af den cyberdiplomatiske værktøjskasse. Derudover bør EU **integrere den cyberdiplomatiske værktøjskasse yderligere i EU's krisemekanismer**, søge synergier med arbejdet for at imødegå hybride trusler, desinformation og udenlandsk indblanding under den fælles ramme for imødegåelse af hybride trusler[88] og den europæiske handlingsplan for demokrati. I denne forbindelse bør EU overveje interaktionen mellem den cyberdiplomatiske værktøjskasse og den mulige anvendelse af artikel 42, stk. 7, i TEU og artikel 222 i TEUF[89].

2.4 Styrkelse af cyberforsvarskapaciteten

EU og medlemsstaterne skal blive bedre til at forebygge og reagere på cybertrusler i overensstemmelse med EU's ambitionsniveau, som fremgår af EU's globale strategi fra 2016[90]. I denne forbindelse vil den højtstående repræsentant i samarbejde med Kommissionen forelægge en **revision af politikrammen for cyberforsvar (CDPF)** for

[85] Såsom EU's fælles efterretningsanalysekapacitet (SIAC) og om nødvendigt de relevante projekter under PESCO samt det hurtige varslingssystem (RAS) fra 2018, der blev oprettet for at støtte EU's overordnede tilgang til at håndtere desinformation.
[86] Navnlig ved at søge at skabe synergi med initiativerne i handlingsplanen for europæisk demokrati.
[87] 13007/17
[88] https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52016JC0018&from=DA.
[89] Henholdsvis bestemmelsen om gensidigt forsvar og bestemmelsen om solidaritet.
[90] Rådets konklusioner (14149/16) om gennemførelse af EU's globale strategi på sikkerheds- og forsvarsområdet.

yderligere at styrke koordineringen og samarbejdet mellem EU's aktører[91] samt med og mellem medlemsstaterne, herunder for så vidt angår missioner og operationer under den fælles sikkerheds- og forsvarspolitik (FSFP). CDPF bør anvendes i forbindelse med det kommende strategiske kompas[92] for at sikre, at cybersikkerhed og cyberforsvar får en mere fremtrædende plads på den bredere sikkerheds- og forsvarsdagsorden.

I 2018 identificerede EU cyberspace som et operationsområde[93]. En kommende "**Military Vision and Strategy on Cyberspace as a Domain of Operations**" (militær vision og strategi for cyberspace som et operationsområde**)** fra EU's Militærkomité bør yderligere fastlægge, hvordan cyberspace som et operationsområde forbedrer EU's muligheder for at gennemføre militære FSFP-missioner og -operationer. Det **militære CERT-netværk**[94], som Det Europæiske Forsvarsagentur (EDA) er ved at oprette, vil i høj grad fremme medlemsstaternes samarbejde. For at garantere cybersikkerheden af kritiske ruminfrastrukturer under rumprogrammet vil Den Europæiske Unions Agentur for Rumprogrammet og navnlig Galileo-sikkerhedsovervågningscentret blive styrket, og dets mandat vil blive udvidet til at omfatte andre kritiske aktiver under rumprogrammet.

EU og medlemsstaterne bør sætte yderligere skub i **udviklingen af avanceret cyberforsvarskapacitet** gennem forskellige EU-politikker og -instrumenter, navnlig CDPF, og når det er hensigtsmæssigt med udgangspunkt i EDA's arbejde. Dette kræver, at der lægges stor vægt på at udvikle og anvende nøgleteknologier såsom kunstig intelligens, kryptering og kvantedatabehandling. I overensstemmelse med EU's kapacitetsudviklingsprioriteter fra 2018[95] og på baggrund af resultaterne af den første fuldstændige samordnede årlige gennemgang vedrørende forsvar (CARD)[96] bør EU yderligere fremme medlemsstaternes samarbejde om forskning i **cyberforsvar, innovation og kapacitetsudvikling** og tilskynde medlemsstaterne til at udnytte det fulde potentiale af det **permanente strukturerede samarbejde (PESCO)[97]** og **EDF[98].**

Kommissionens kommende **handlingsplan om synergier mellem den civile, forsvars- og rumindustrien**, som skal fremlægges i første kvartal af 2021, vil omfatte foranstaltninger, som yderligere vil støtte synergier for så vidt angår programmer, teknologier, innovation og nyetablerede virksomheder i overensstemmelse med forvaltningen af de respektive programmer[99].

---

[91] Navnlig EU-Udenrigstjenesten, herunder EU's Militærstab (EUMS), Det Europæiske Sikkerheds- og Forsvarsakademi (ESDC), Kommissionen og EU-agenturer, bl.a. Det Europæiske Forsvarsagentur (EDA).

[92] Rådets konklusioner om sikkerhed og forsvar af 17. juni 2020 (8910/20).

[93] https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/da/pdf.

[94] Oprettelsen af et europæisk militært CERT-netværk opfylder et af de mål, der blev fastlagt i rammen for cyberforsvarspolitik fra 2018, og har til formål at fremme aktiv interaktion og informationsudveksling mellem EU-medlemsstaternes militære CERT'er.

[95] I juni 2018 enedes medlemsstaterne i EDA's styringsråd om at lede forsvarssamarbejdet på EU-plan.

[96] Godkendt af forsvarsministrene i EDA's styringsråd i november 2020. https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-(card).

[97] Der er for øjeblikket adskillige cyberrelaterede PESCO-projekter i gang, navnlig platformen til informationsudveksling om reaktion på cybertrusler og -hændelser, cyberberedskabshold og gensidig bistand inden for cybersikkerhed, EU's forsknings- og innovationsknudepunkt på cyberområdet og koordineringscentret på cyber- og informationsområdet (CIDCC).

[98] Under EUF har Kommissionen allerede identificeret muligheder for potentielle samarbejdsbaserede forsknings- og udviklingstiltag inden for cyberforsvar, som har til formål at styrke samarbejdet, innovationskapaciteten og forsvarsindustriens konkurrenceevne.

[99] Såsom Horisont Europa, et digitalt Europa og EUF.

Derudover skal der skabes relevante synergier og grænseflader mellem cyberforsvarsinitiativer, som gennemføres inden for andre rammer, herunder medlemsstaternes cyberrelaterede samarbejdsprojekter[100] under PESCO, samt med EU's cybersikkerhedsstrukturer for at støtte informationsudveksling og gensidig bistand.

Strategiske initiativer

EU bør:

- færdiggøre den europæiske ramme for håndtering af cybersikkerhedskriser og fastlægge proceduren, milepælene og tidsplanen for oprettelse af den fælles cyberenhed
- fortsætte gennemførelsen af dagsordenen for cyberkriminalitet under strategien for EU's sikkerhedsunion
- tilskynde til og lette nedsættelsen af en arbejdsgruppe om cyberintelligens for medlemsstaterne, der hører under EU INTCEN
- fremsætte EU's holdning til cyberforsvar med afskrækkende virkning for at forebygge, modvirke, hindre og reagere på ondsindede cyberaktiviteter
- revidere politikrammen for cyberforsvar
- lette udviklingen af EU's militære vision og strategi for cyberspace som et operationsområde med henblik på militære FSFP-missioner og -operationer
- støtte synergier mellem den civile, forsvars- og rumindustrien og
- styrke cybersikkerheden af kritiske ruminfrastrukturer under rumprogrammet.

3. FREMME AF ET GLOBALT OG ÅBENT CYBERSPACE

EU bør fortsat arbejde sammen med de internationale partnere om at fremme en politisk model og vision for cyberspace baseret på retsstatsprincippet, menneskerettighederne, de grundlæggende frihedsrettigheder og de demokratiske værdier, der skaber social, økonomisk og politisk udvikling globalt og bidrager til en sikkerhedsunion. Internationalt samarbejde er afgørende for at bevare et globalt, åbent, stabilt og sikkert cyberspace. EU bør i denne forbindelse fortsat arbejde sammen med tredjelande, internationale organisationer og multiinteressentfællesskabet om at udvikle og gennemføre en sammenhængende og holistisk international cyberpolitik under hensyntagen til den stigende indbyrdes sammenhæng mellem de økonomiske aspekter ved nye teknologier, den indre sikkerhed og udenrigs-, sikkerheds- og forsvarspolitikken. Som en stærk økonomisk blok og handelsblok, der bygger på centrale demokratiske værdier, respekt for retsstatsprincippet og de grundlæggende rettigheder, er EU også godt rustet til at føre an i forbindelse med opstilling og fremme af internationale normer og standarder.

[100] https://pesco.europa.eu/.

3,1. EU's lederskab inden for standarder, normer og rammer i cyberspace

Intensivering af den internationale standardisering

For at fremme og forsvare sin vision for cyberspace på internationalt plan skal EU **intensivere sit engagement i og lederskab inden for internationale standardiseringsprocesser og styrke sin repræsentation i internationale og europæiske standardiseringsorganer samt i andre standardudviklingsorganisationer**[101]. Da de digitale teknologier udvikler sig hurtigt, er de internationale standarder af stigende betydning som et supplement til de traditionelle lovgivningsmæssige tiltag inden for områder som kunstig intelligens, cloudteknologi, kvantedatabehandling og kvantekommunikation. International standardisering anvendes i stigende grad af tredjelande til at fremføre deres politiske og ideologiske dagsorden, som ofte ikke stemmer overens med EU's værdier. Desuden øges risikoen for konkurrerende rammer for international standardisering, hvilket skaber fragmentering.

Det er vigtigt at forme de internationale standarder for nye teknologier og internettets centrale arkitektur i overensstemmelse med EU's værdier for at sikre, at internettet forbliver globalt og åbent, at teknologierne er menneskecentrerede, privatlivsorienterede, og at de anvendes lovligt, sikkert og etisk korrekt. Som led i sin kommende standardiseringsstrategi bør EU fastlægge sine **mål for international standardisering** og gennemføre proaktive og koordinerede oplysningskampagner for at fremme disse mål på internationalt plan. Der bør stræbes efter et stærkere samarbejde og byrdefordeling med ligesindede partnere og europæiske interessenter.

Fremme af ansvarlig statslig adfærd i cyberspace

EU vil fortsat arbejde sammen med de internationale partnere om at fremme et globalt, åbent, stabilt og sikkert cyberspace, hvor **folkeretten, navnlig De Forenede Nationers pagt (FN-pagten)**[102]**, overholdes**, og de **frivillige, ikkebindende normer, regler og principper for ansvarlig statslig adfærd**[103] efterkommes. Med svækkelsen af den multilaterale debat om den internationale sikkerhed i cyberspace er der et klart behov for, at EU og medlemsstaterne indtager en mere proaktiv holdning i drøftelserne i FN og andre relevante internationale fora. EU er bedst rustet til at **fremme, koordinere og konsolidere medlemsstaternes holdninger i** internationale **fora** og bør **udarbejde en EU-holdning om anvendelsen af folkeretten i cyberspace**. Den højtstående repræsentant vil i samarbejde med medlemsstaterne præsentere deres inkluderende og konsensusbaserede forslag til et politisk engagement i et **handlingsprogram til fremme af ansvarlig statslig adfærd i cyberspace**[104] i FN. Handlingsprogrammet, der bygger på gældende EU-ret som godkendt af FN's

[101] F.eks. Den Internationale Standardiseringsorganisation (ISO), Den Internationale Elektrotekniske Kommission (IEC), Den Internationale Telekommunikationsunion (ITU), Den Europæiske Standardiseringsorganisation (CEN), Den Europæiske Komité for Elektroteknisk Standardisering (CENELEC), Det Europæiske Standardiseringsinstitut for Telekommunikation (ETSI), Internet Engineering Task Force (IETF), tredjegenerationspartnerskabsprojektet (3GPP) og Institute of Electrical and Electronics Engineers (IEEE).

[102] https://www.un.org/en/sections/un-charter/un-charter-full-text/.

[103] Som det fremgår af de relevante rapporter fra grupperne af regeringseksperter vedrørende udviklingen inden for information og telekommunikation i forbindelse med international sikkerhed, der er godkendt af FN's Generalforsamling, navnlig rapporterne fra 2015, 2013 og 2010.

[104] https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf.

Generalforsamling[105], udgør en platform for samarbejde og udveksling af bedste praksis inden for FN og indeholder forslag om, at der oprettes en mekanisme til at indføre normerne for ansvarlig statslig adfærd i praksis og fremme kapacitetsopbygning. Desuden sigter den højtstående repræsentant mod at styrke og tilskynde til gennemførelse af **tillidsskabende foranstaltninger** mellem stater, herunder udveksling af bedste praksis på regionalt og multilateralt plan og medvirken til et tværregionalt samarbejde.

Øget global konnektivitet bør ikke medføre censur, masseovervågning, brud på datasikkerheden og undertrykkelse af civilsamfundet, den akademiske verden og borgerne. EU bør fortsat føre an hvad angår beskyttelse og fremme af **menneskerettighederne og de grundlæggende frihedsrettigheder** online. I denne forbindelse bør EU fremme yderligere overholdelse af international menneskerettighedslovgivning og internationale menneskerettighedsstandarder[106] og gennemføre sin handlingsplan om menneskerettigheder og demokrati 2020-2024[107] samt fremlægge sine menneskerettighedsbaserede retningslinjer for ytringsfrihed online og offline[108] **og dermed sætte skub i den praktiske anvendelse af EU's instrumenter**. EU bør gøre en vedvarende indsats for at **beskytte menneskerettighedsforkæmpere, civilsamfundet og akademikere, der arbejder med emner som cybersikkerhed, databeskyttelse, overvågning og onlinecensur**. I dette øjemed bør EU give yderligere praktisk vejledning, fremme bedste praksis og optrappe sin indsats for at forhindre misbrug af nye teknologier, navnlig ved anvendelse af diplomatiske foranstaltninger, hvor det er nødvendigt, samt eksportkontrol af sådanne teknologier. EU bør også fortsætte sin kamp for at beskytte de mest sårbare medlemmer af onlinesamfundet ved at komme med lovgivning om bedre beskyttelse af børn mod seksuelt misbrug og seksuel udnyttelse og en strategi for børns rettigheder.

Budapestkonventionen om IT-kriminalitet

EU støtter fortsat tredjelande, der ønsker at tiltræde **Europarådets konvention om IT-kriminalitet (Budapestkonventionen)** og arbejder på at færdiggøre **den anden tillægsprotokol til Budapestkonventionen**, som indeholder foranstaltninger og forholdsregler til forbedring af det internationale samarbejde mellem retshåndhævende og retslige myndigheder samt mellem myndigheder og tjenesteudbydere i andre lande. Kommissionen deltager i forhandlingerne om den anden tillægsprotokol på EU's vegne[109]. Det nuværende initiativ vedrørende et nyt retligt instrument om cyberkriminalitet i FN-regi risikerer at forstærke splittelserne og bremse de hårdt tiltrængte nationale reformer og den tilhørende indsats for kapacitetsopbygning, hvilket potentielt kan forhindre et effektivt internationalt samarbejde om bekæmpelse af cyberkriminalitet. EU mener ikke, at der er behov for et nyt retligt instrument vedrørende cyberkriminalitet på FN-plan. EU deltager fortsat i de **multilaterale udvekslinger om cyberkriminalitet** for at sikre overholdelsen af menneskerettighederne og de grundlæggende frihedsrettigheder gennem inklusivitet og gennemsigtighed og under hensyntagen til den tilgængelige ekspertviden med det formål at skabe merværdi for alle.

---

[105] Som det fremgår af de relevante rapporter fra grupperne af regeringseksperter vedrørende udviklingen inden for information og telekommunikation i forbindelse med international sikkerhed, der er godkendt af FN's Generalforsamling, navnlig rapporterne fra 2015, 2013 og 2010.

[106] Navnlig FN-pagten og verdenserklæringen om menneskerettigheder.

[107] https://www.consilium.europa.eu/da/press/press-releases/2020/11/19/council-approves-conclusions-on-the-eu-action-plan-on-human-rights-and-democracy-2020-2024/.

[108] https://www.consilium.europa.eu/media/28348/142549.pdf.

[109] Rådets afgørelse fra juni 2019 (ref. 9116/19).

3.2 Samarbejde med partnere og multiinteressentfællesskabet

EU bør **styrke og udvide sin cyberdialog med tredjelande** for at fremme sine værdier og visioner for cyberspace, udveksle bedste praksis og søge at skabe et mere effektivt samarbejde. EU bør også indgå i **strukturerede udvekslinger med regionale organisationer** som Den Afrikanske Union, ASEAN Regional Forum, Organisationen af Amerikanske Stater og Organisationen for Sikkerhed og Samarbejde i Europa. Samtidig bør EU, hvor det er muligt og hensigtsmæssigt, bestræbe sig på at finde fælles fodfæste med andre partnere med udgangspunkt i emner af fælles interesse. I samarbejde med EU's delegationer og eventuelt medlemsstaternes ambassader rundt om i verden bør EU oprette et uformelt **EU-netværk for cyberdiplomati** for at fremme EU's vision for cyberspace, udveksle oplysninger og regelmæssigt koordinere udviklingen i cyberspace[110].

På grundlag af de fælles erklæringer af 8. juli 2016[111] og 10. juli 2018[112] bør EU fortsat fremme **samarbejdet mellem EU og NATO**, navnlig med hensyn til kravene om cyberforsvarsinteroperabilitet. I denne forbindelse bør EU fortsætte arbejdet med at tilslutte de relevante FSFP-strukturer til NATO's Federated Mission Networking og dermed sikre netværksinteroperabiliteten med NATO og partnerne, når det er nødvendigt. Desuden bør samarbejdet mellem EU og NATO om uddannelse, træning og øvelser udforskes yderligere, bl.a. ved at søge synergier mellem Det Europæiske Sikkerheds- og Forsvarsakademi og NATO's cyberforsvarscenter.

EU støtter og fremmer på det kraftigste **multiinteressentmodellen for internetforvaltning** i overensstemmelse med EU's værdier. Ingen enhed, regering eller international organisation bør forsøge at kontrollere internettet alene. EU bør fortsat deltage i fora[113] for at styrke samarbejdet og sikre beskyttelsen af de grundlæggende rettigheder og frihedsrettigheder, navnlig retten til værdighed, privatlivets fred og ytrings- og informationsfriheden. For at komme videre med multiinteressentsamarbejdet om cybersikkerhed sigter Kommissionen og den højtstående repræsentant mod, i overensstemmelse med deres respektive kompetencer, at styrke **regelmæssige og strukturerede udvekslinger med interessenterne**, herunder den private sektor, den akademiske verden og civilsamfundet, idet det understreges, at sammenkoblingen af cyberspace kræver, at alle interessenter dialogerer om og påtager sig deres specifikke ansvar for at opretholde et globalt, åbent, stabilt og sikkert cyberspace. Dette arbejde vil give værdifuldt input til potentielle nøgleaktioner på EU-plan.

3,3. Styrkelse af den globale kapacitet for at øge den globale modstandsdygtighed

For at sikre, at alle lande kan nyde godt af de sociale, økonomiske og politiske fordele ved internettet og anvendelsen af teknologier, vil EU fortsat støtte sine partnere i deres bestræbelser på at forbedre deres cyberrobusthed og kapacitet til at efterforske og retsforfølge cyberkriminalitet og imødegå cybertrusler. For at sikre den overordnede sammenhæng bør EU opstille en **dagsorden for ekstern cyberkapacitetsopbygning** for at lede dette arbejde i henhold til EU's retningslinjer for ekstern cyberkapacitetsopbygning[114] og 2030-dagsordenen

[110] EU kunne eventuelt også udnytte aktiviteterne i det uformelle EU-netværk for digitalt diplomati, som omfatter medlemsstaternes udenrigsministerier.
[111] http://www.consilium.europa.eu/da/press/press-releases/2016/07/08-eu-nato-joint-declaration/.
[112] https://www.consilium.europa.eu/da/press/press-releases/2018/07/10/eu-nato-joint-declaration/
[113] Såsom ICANN (Internet Cooperation for Assigned Names and Numbers) og IGF (Internet Governance Forum).
[114] https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf.

for bæredygtig udvikling[115]. Dagsordenen bør udnytte medlemsstaternes og de relevante EU-institutioners, -organers og -agenturers ekspertviden og initiativer, herunder EU's netværk for cyberkapacitetsopbygning[116], i overensstemmelse med deres respektive mandater. Der skal oprettes et **europæisk råd for cyberkapacitetsopbygning**, som samler relevante institutionelle interessenter i EU og overvåger fremskridt og identificerer yderligere synergier og potentielle fejl og mangler. Rådet kan desuden støtte samarbejdet med medlemsstaterne samt med partnere fra den offentlige og private sektor og andre relevante internationale organer for at sikre, at indsatsen koordineres, og undgå dobbeltarbejde.

EU's cyberkapacitetsopbygning bør fortsat fokusere på Vestbalkan og EU's nabolande samt på partnerlande, der oplever en hastig digital udvikling. EU's arbejde bør støtte udarbejdelsen af lovgivning og politikker i partnerlandene i overensstemmelse med EU's relevante politikker og standarder for cyberdiplomati. I denne forbindelse bør EU's kapacitetsopbygningsindsats inden for digitalisering som standard omfatte cybersikkerhed. I dette øjemed bør EU udvikle et uddannelsesprogram for EU-personale med ansvar for gennemførelsen af EU's indsats inden for digital og ekstern cyberkapacitetsopbygning. EU bør desuden hjælpe disse lande med at tackle de tiltagende udfordringer som følge af ondsindede cyberaktiviteter, der skader udviklingen i deres samfund og de **demokratiske systemers integritet og sikkerhed**, i overensstemmelse med indsatsen under den europæiske handlingsplan for demokrati. Peer-to-peer-læring mellem EU-medlemsstaterne og de relevante EU-agenturer og tredjelande kan være særlig nyttig i denne henseende.

Endelig kan civile FSFP-missioner inden for rammerne af den civile FSFP-aftale fra 2018[117] også bidrage til EU's bredere indsats for at tackle cybersikkerhedsudfordringer, navnlig ved at styrke retsstatsprincippet og de retshåndhævende og civile myndigheders kapacitet i partnerlandene.

Strategiske initiativer

EU bør:

- definere en række mål i internationale standardiseringsprocesser og fremme disse på internationalt plan
- fremme international sikkerhed og stabilitet i cyberspace, navnlig gennem forslaget fra EU og medlemsstaterne til et handlingsprogram for fremme af ansvarlig statslig adfærd i cyberspace (PoA) i De Forenede Nationer
- tilbyde praktisk vejledning om anvendelse af menneskerettigheder og grundlæggende frihedsrettigheder i cyberspace
- bedre beskytte børn mod seksuelt misbrug og seksuel udnyttelse samt en strategi for børns rettigheder
- styrke og fremme Budapestkonventionen om IT-kriminalitet, herunder gennem arbejdet med anden tillægsprotokol til Budapestkonventionen om IT-kriminalitet
- udvide EU's dialog med tredjelande, regionale og internationale organisationer om

[115] https://ec.europa.eu/environment/sustainable-development/SDGs/index_en.htm.
[116] https://www.eucybernet.eu/.
[117] https://data.consilium.europa.eu/doc/document/ST-14611-2019-INIT/da/pdf.

cyberspørgsmål, herunder gennem et uformelt cyberdiplomatisk EU-netværk

- styrke udvekslingerne med multiinteressentfællesskabet, navnlig ved regelmæssige og strukturerede udvekslinger med den private sektor, den akademiske verden og civilsamfundet og
- stille forslag om en dagsorden for EU's eksterne cyberkapacitetsopbygning samt et råd for EU's cyberkapacitetsopbygning.

III. CYBERSIKKERHED I EU'S INSTITUTIONER, ORGANER OG AGENTURER

På grund af deres politiske synlighed, kritiske missioner med hensyn til koordinering af meget følsomme emner samt deres rolle i forvaltning af store summer af offentlige midler er **EU's institutioner, organer og agenturer regelmæssigt mål for cyberangreb**, særligt cyberspionage. Men graden af cyberrobusthed og evnen til at reagere på ondsindede cyberaktiviteter varierer betydeligt i disse enheder for så vidt angår modenhed. Det er derfor nødvendigt at styrke det generelle cybersikkerhedsniveau ved hjælp af konsekvente og ensartede regler.

På IT-sikkerhedsområdet er der gjort fremskridt hen imod mere konsekvente **regler for beskyttelse af EU's klassificerede informationer samt følsomme ikkeklassificerede oplysninger**. Interoperabiliteten mellem klassificerede IT-systemer er dog stadig begrænset, hvilket forhindrer sømløs overførsel af oplysninger mellem de forskellige enheder. Der bør gøres yderligere fremskridt i retning af at muliggøre en interinstitutionel tilgang til behandlingen af EU's klassificerede informationer og følsomme ikkeklassificerede oplysninger, som også kan fungere som model for interoperabilitet medlemsstaterne imellem. Der bør også etableres en referenceværdi for at forenkle procedurer indledt med medlemsstaterne. EU bør også yderligere styrke sine muligheder for at kommunikere med relevante partnere på en sikker måde, der i videst muligt omfang bygger på eksisterende ordninger og procedurer.

Som det fremgår af Unionens sikkerhedsstrategi, vil Kommissionen derfor foreslå **fælles bindende regler om informationssikkerhed og fælles bindende regler for cybersikkerhed for alle EU's institutioner, organer og agenturer i 2021**, baseret på EU's igangværende interinstitutionelle drøftelser om cybersikkerhed[118].

Den nuværende situation og fremtidige tendenser med hensyn til telearbejde vil desuden kræve yderligere investeringer i sikkerhedsudstyr, infrastrukturer og værktøjer, der giver mulighed for at arbejde hjemmefra med følsomme og klassificerede filer.

Det stadig mere fjendtlige cybertrusselsbillede og det stigende antal mere avancerede cyberangreb mod EU's institutioner, organer og agenturer øger desuden behovet for større investering for at nå et højt modenhedsniveau for så vidt angår cybersikkerhed. Der er indført et oplysningsprogram vedrørende cybersikkerhed for alle EU's institutioner, organer og agenturer til fremme af personalets bevidsthed og cyberhygiejnen og til understøttelse af en fælles kultur for cybersikkerhed.

[118] Jævnlige interinstitutionelle drøftelser om cybersikkerhed på EU-plan er en del af den bredere drøftelse af mulighederne for og udfordringerne ved den digitale omstilling for EU's institutioner.

Styrkelsen af CERT-EU med en forbedret finansieringsmekanisme er nødvendig for at øge dens evne til at hjælpe EU's institutioner, organer og agenturer med at anvende de nye regler for cybersikkerhed og forbedre deres cyberrobusthed. CERT-EU's mandat skal også styrkes, således at den kan opnå disse målsætninger på en stabil måde.

Strategiske initiativer

1. Forordning om informationssikkerhed i EU's institutioner, organer og agenturer
2. Forordning om fælles regler for cybersikkerhed for EU's institutioner, organer og agenturer
3. Nyt retsgrundlag for styrkelse af CERT-EU's mandat og finansiering.

IV. KONKLUSIONER

Den samordnede gennemførelse af denne strategi bidrager til et cybersikkert digitalt årti for EU, etablering af en sikkerhedsunion og til styrkelse af EU's position på verdensplan.

EU bør fremme standarder og normer for løsninger i verdensklasse og cybersikkerhedsstandarder for grundlæggende tjenester og kritiske infrastrukturer samt udvikling og anvendelse af nye teknologier. Hver organisation og person, der bruger internettet, er en del af løsningen for at sikre en cybersikker digital omstilling.

Kommissionen og den højtstående repræsentant vil overvåge fremskridtene under denne strategi og udarbejde kriterier for vurdering. Bidrag til denne overvågning omfatter rapporter fra ENISA samt Kommissionens regelmæssige rapporter om sikkerhedsunionen. Resultaterne bidrager til de kommende målsætninger for det digitale årti[119]. I overensstemmelse med de respektive kompetencer vil Kommissionen og den højtstående repræsentant fortsat samarbejde med medlemsstaterne med henblik på at træffe praktiske foranstaltninger for at slå bro over de fire cybersikkerhedsfællesskaber i EU for kritisk infrastruktur og resiliens i det indre marked, retsvæsen og retshåndhævelse, cyberdiplomati og cyberforsvar efter behov. Derudover vil Kommissionen og den højtstående repræsentant fortsat samarbejde med multinteressentfællesskabet for at understrege behovet for at alle, som benytter internettet, yder deres bidrag for at fastholde et globalt, åbent, stabilt og sikkert cyberspace, hvor alle sikkert kan leve sit digitale liv.

[119] Som bebudet i Kommissionens arbejdsprogram 2021.

Tillæg: Næste skridt hen mod cybersikkerhed i 5G-net

På baggrund af resultaterne af gennemgangen af Kommissionens henstilling om cybersikkerheden i 5G-net[120] bør de næste skridt i samordningen på EU-plan fokusere på tre centrale målsætninger og på de vigtigste aktioner på kort og mellemlang sigt som anført i tabellen nedenfor, der skal gennemføres af myndighederne i medlemsstaterne, Kommissionen og ENISA.

Den første prioritet i næste fase er at **afslutte gennemførelsen af værktøjskassen på nationalt plan og at behandle de problemstillinger, der er angivet i statusrapporten fra juli 2020**. I denne sammenhæng vil nogle af de strategiske foranstaltninger i værktøjskassen kunne drage fordel af **styrket samordning af arbejdet eller udveksling af oplysninger** i NIS-arbejdsstrømmen som allerede konstateret i statusrapporten, hvilket potentielt kan føre til udarbejdelse af **bedste praksis eller retningslinjer**. Med hensyn til tekniske foranstaltninger kan ENISA yde yderligere støtte, der bygger på det arbejde, de allerede har udført, og undersøge visse emner mere dybtgående og **udvikle en samlet oversigt over alle relevante retningslinjer for krav til 5G-cybersikkerhed for mobilnetoperatører.**

For det andet understregede medlemsstaterne vigtigheden af at være på forkant med udviklingen ved **løbende at overvåge udviklingen inden for teknologien, 5G-arkitektur, trusler og anvendelser og applikationer i 5G samt eksterne faktorer** for at kunne **identificere og imødekomme nye risici**. Der bør endvidere kigges nærmere på en række aspekter i den indledende risikoanalyse, navnlig for at sikre at den omfatter hele 5G-økosystemet, herunder alle relevante dele af netværksinfrastrukturen og 5G-forsyningskæden. Selv om værktøjskassen er designet som et fleksibelt og tilpasningsparat instrument, kunne der om nødvendigt tages skridt på mellemlang sigt til at udvide eller ændre den med henblik på at sikre, at vedbliver at være fyldestgørende og ajour.

For det tredje bør der træffes **foranstaltninger på EU-plan** som støtte og supplement til værktøjskassens målsætninger for fuldt ud at integrere dem i EU's og Kommissionens politik, navnlig som opfølgning på de bebudede foranstaltninger i Kommissionens henstilling om værktøjskassen af 29. januar 2020[121] inden for et bredt område (f.eks. EU-støtte til sikre 5G-net, investeringer i 5G samt post-5G-teknologier, handelspolitiske beskyttelsesinstrumenter og konkurrence for at undgå fordrejninger på 5G-forsyningsmarkedet osv.).

De nærmere regler og milepæle for nedenstående centrale foranstaltninger bør aftales med de førende aktører primo 2021, hvis det er relevant.

Hovedmål 1: Sikring af samordning af nationale fremgangsmåder for effektiv risikoafbødning i hele EU		
Områder	**Centrale foranstaltninger på kort og mellemlang sigt**	**Førende aktører**
Medlemsstaternes gennemførelse af værktøjskassen	Afslutte gennemførelsen af foranstaltningerne som anbefalet i værktøjskassens konklusioner inden andet kvartal 2021, med regelmæssige statusopgørelser i NIS-	Medlemsstaternes myndigheder

[120] Kommissionens Rapport om virkningerne af Kommissionens henstilling 2019/534 af 26. marts 2019 om cybersikkerheden i 5G-net.

[121] Kommissionens meddelelse (COM(2020) 50) om en EU-værktøjskasse til udrulning af sikre 5G-net i EU af 29. januar 2020.

	arbejdsstrømmen.	
Udveksling af oplysninger og bedste praksis om strategiske foranstaltninger vedrørende leverandører	Intensivere udveksling af oplysninger og overveje eventuel bedste praksis, navnlig vedrørende: - restriktioner for højrisikoleverandører (SM03) og foranstaltninger relateret til levering af forvaltede tjenester (SM04) - forsyningskædens sikkerhed og modstandsdygtighed, navnlig opfølgning på undersøgelsen gennemført af BEREC vedrørende SM05-SM06.	Medlemsstaternes myndigheder, Kommissionen
Kapacitetsopbygning og vejledning om tekniske foranstaltninger	Gennemføre grundige tekniske undersøgelser og udvikle fælles retningslinjer og værktøjer, herunder: - en samlet og dynamisk oversigt over sikkerhedskontroller og bedste praksis for 5G-sikkerhed retningslinjer til støtte for gennemførelse af udvalgte tekniske foranstaltninger fra værktøjskassen.	ENISA, medlemsstaternes myndigheder
Hovedmål 2: Støtte til løbende videnudveksling og kapacitetsopbygning		
Områder	**Centrale foranstaltninger på kort og mellemlang sigt**	**Førende aktører**
Løbende videnopbygning	Planlægge videnopbygningsaktiviteter om teknologiske og dertilhørende udfordringer (åbne arkitekturer, 5G-funktioner – f.eks. virtualisering, containerisation, slicing, osv.), udvikling i trusselsbilledet, hændelser fra det virkelige liv, osv.	ENISA, medlemsstaternes myndigheder, andre aktører
Risikovurderinger	Ajourføre og udveksle oplysninger om opdaterede nationale risikovurderinger	Medlemsstaternes myndigheder, Kommissionen, ENISA
Fælles EU-finansierede projekter til støtte for gennemførelsen af værktøjskassen	Yde økonomisk støtte til projekter, der støtter gennemførelse af værktøjskassen ved hjælp af EU-finansiering, navnlig under programmet for et digitalt Europa (f.eks. kapacitetsopbyggende projekter for nationale myndigheder, afprøvningsredskaber eller anden avanceret kapacitet, osv.)	Medlemsstaternes myndigheder, Kommissionen
Samarbejde mellem de berørte parter	Fremme samarbejdet mellem nationale myndigheder, der beskæftiger sig med 5G-cybersikkerhed (f.eks. NIS-samarbejdsgruppen, cybersikkerhedsmyndigheder, telekommunikationsregulerende myndigheder) og med private interessenter	Medlemsstaternes myndigheder, Kommissionen, ENISA
Hovedmål 3: Fremme af modstandsdygtighed i forsyningskæden og andre strategiske sikkerhedsmål i EU		
Områder	**Centrale foranstaltninger på kort og mellemlang sigt**	**Førende aktører**
Standardisering	Definere og gennemføre en konkret handlingsplan for at styrke EU's repræsentation i organer for udarbejdelse af standarder som led i de næste skridt i NIS-underudvalgets arbejde med standardisering med henblik på at nå specifikke sikkerhedsmål, herunder fremme af interoperable grænseflader til fremme af diversificering af leverandører.	Medlemsstaternes myndigheder
Modstandsdygtighed i forsyningskæden	— Gennemføre en grundig analyse af 5G-økosystemet og forsyningskæden for bedre at kunne identificere og	Medlemsstaternes myndigheder,

	overvåge centrale aktiver og potentielt kritiske afhængigheder — Sikre 5G-markedets funktion og forsyningskæden er i overensstemmelse med EU's handelsforpligtelser og konkurrenceregler samt målsætninger, som omhandlet i Kommissionens meddelelse af 29. januar, og at screening af udenlandske direkte investeringer anvendes på investeringsudvikling, der kan påvirke 5G-værdikæden, under hensyntagen til værktøjskassens målsætninger. — Overvåge eksisterende og forventede markedstendenser og vurdere risici og muligheder på området for Open RAN, navnlig gennem en uafhængig undersøgelse	Kommissionen
Certificering	Igangsætte forberedelser af gældende kandidatcertificeringsordning(er) for centrale 5G-komponenter og leverandørprocesser med henblik på at afbøde visse risici i relation til tekniske sårbarheder som defineret i værktøjskassens planer for risikobegrænsning.	Kommissionen, ENISA, nationale myndigheder, andre aktører
EU's kapacitet og sikre udrulninger af net	— Investere i FoI og kapacitet, navnlig gennem vedtagelsen af partnerskabet vedrørende intelligente netværk og tjenester — Gennemføre relevante sikkerhedsbetingelser for EU-finansieringsprogrammer og finansielle instrumenter (interne og eksterne) som bebudet i Kommissionens meddelelse af 29. januar.	Medlemsstaterne, Kommissionen, interessenter i 5G-branchen
Eksterne aspekter	Svare positivt på anmodninger fra tredjelande, der ønsker at forstå og potentielt anvende værktøjskassetilgangen udviklet af EU.	Medlemsstaterne, Kommissionen Tjenesten for EU's Optræden Udadtil, EU-delegationer