FORSVARSMINISTERIET

**GRUND- OG NÆRHEDSNOTAT TIL
FOLKETINGETS EUROPAUDVALG**

Europa-Kommissionens henstilling om en koordineret gennemførelseskøreplan for overgangen til kvantesikker kryptografi

KOM (2024) 2393

Notatet sendes endvidere til Folketingets Forsvarsudvalg.

1. Resumé

Kommissionen har den 11. april 2024 offentliggjort en henstilling om en koordineret gennemførelsesplan for overgangen til kvantesikker kryptografi. Formålet med henstillingen er at udvikle en koordineret overgang til kvantesikker kryptografi med henblik på beskyttelse af den digitale infrastruktur i EU mod truslen fra kvanteteknologier. Kommissionen opfordrer medlemsstaterne til at udvikle en omfattende strategi for indførelse af kvantesikker kryptografi med klare mål, milepæle og tidsfrister. Strategien skal føre til fastlæggelsen af en fælles gennemførelseskøreplan for kvantesikker kryptografi med henblik på, at der i hele EU indføres kvantesikker kryptografi i de offentlige myndigheders eksisterende systemer og kritiske infrastrukturer.

Regeringen hilser henstillingen velkommen og støtter en koordineret indsats inden for overgangen til kvantesikker kryptografi i EU. Regeringen finder det væsentligt, at Danmark rettidigt igangsætter arbejdet med at styrke Danmarks kritiske digitale infrastruktur mod kompromittering fra eksempelvis kvantecomputere, og at dette sker i tæt samarbejde med ligesindede internationale partnere som understreget i den nationale kvantestrategi del 2.

Regeringen støtter derfor formålet om, at der udarbejdes en omfattende strategi og en koordineret gennemførelseskøreplan for kvantesikker kryptografi. Regeringen påpeger vigtigheden af synergi med arbejdet i NATO og hos EU's internationale partnere for at undgå dobbeltarbejde og sikre en sammenhængende tilgang til håndtering af nye udfordringer, særligt ved evaluering, udvælgelse og vedtagelse af kvantesikre algoritmer som EU-standarder, som bør ske proportionelt med kritikaliteten af overgangen til kvantesikker kryptografi i Unionen.

2. Baggrund

Kommissionen offentliggjorde den 11. april 2024 en henstilling om en koordineret gennemførelseskøreplan for overgangen til kvantesikker kryptografi. Meddelelsen er modtaget i dansk sprogversion den 11. april 2024.

Henstillingen kommer i kølvandet af både nationale og internationale indsatser for at udvikle og udvælge kvantesikre algoritmer i overgangen til en kvantesikker digital infrastruktur, herunder forskningsindsatsen fra EU-finansierede projekter, den nye rapport fra Det Europæiske Agentur for Cybersikkerhed (ENISA) og drøftelser om kvantesikker kryptografi i f.eks. EU's og USA's handels- og teknologiråd og cyberdialog.

Henstillingen bygger på de politiske mål, der er fastsat i EU's strategi for cybersikkerhed om at forbedre sikkerheden og modstandsdygtigheden fra første til sidste led i Unionens digitale infrastrukturer og tjenester for offentlige myndigheder og andre kritiske infrastrukturer, den fælles meddelelse om en europæisk økonomisk sikkerhedsstrategi og de risici mod den fysiske sikkerhed, cybersikkerheden og den kritiske infrastruktur, som er konstateret i forbindelse med den nyligt gennemførte risikovurdering af kvanteteknologier.

Kvantetruslen mod den digitale infrastruktur
Kommissionen baserer henstillingen på betragtninger om truslen fra kvantecomputere og kvantedatabehandlingskapacitet mod de eksisterende kryptografiske standarder, som for nuværende beskytter den digitale infrastruktur, herunder datafortrolighed og –integritet, følsom kommunikation og væsentlige elementer i netværkssikkerheden. Kvantesikker kryptografi vil fjerne de kendte sårbarheder i de nuværende kryptografiske standarder og øge robustheden over for truslen fra ondsindet brug af kvantecomputere og kvantedatabehandlingskapacitet. I en erkendelse af truslen, har EU-Kommissionen finansieret forskning i, og udvikling af, kvantesikker kryptografi og fremhævet kryptering som en central teknologi til at opnå modstandsdygtighed, teknologisk suverænitet og til at kunne forebygge cyberangreb.

Der er endnu ikke taget stilling til den videre proces for Rådets stillingstagning til Kommissionens henstilling. Den vil dog potentielt blive refereret til i Rådskonklusionerne om fremtidens cybersikkerhed, der pt. er under forhandling og forventes vedtaget på Telerådsmødet den 21. maj.

3. Formål og indhold

En strategi for indførelse af kvantesikker kryptografi
Kommissionen opfordrer med henstillingen medlemsstaterne til at udvikle en omfattende strategi for indførelse af kvantesikker kryptografi for at sikre en koordineret og synkroniseret overgang blandt de forskellige medlemsstater og deres offentlige sektorer. Strategien bør fastlægge klare mål, milepæle og tidsfrister og til sidst føre til fastlæggelsen af en fælles gennemførelseskøreplan for kvantesikker kryptografi med henblik på at indføre kvantesikker kryptografi i de offentlige myndigheders eksisterende systemer og kritiske infrastrukturer. Dette bør føre til, at der i hele EU indføres kvantesikker kryptografi i de offentlige myndigheders eksisterende systemer og kritiske infrastrukturer via hybride ordninger, der kan kombinere kvantesikker kryptografi med eksisterende kryptografiske tilgange eller med kvantenøglefordeling ("Quantum Key Distribution" eller QKD).

Etablering af en undergruppe om kvantesikker kryptografi
I henstillingen anbefaler Kommissionen, at medlemsstaterne koordinerer deres indsats i EU gennem nedsættelsen af en undergruppe om kvantesikker kryptografi under NIS-samarbejdsgruppen[1]. Henstillingen opfordrer til at nedsætte undergruppen kort efter offentliggørelsen af henstillingen og udpege ekspertrepræsentanter fra hver medlemsstat. Undergruppen kan omfatte repræsentanter for nationale sikkerhedsagenturer og cybersikkerhedseksperter og ind-

[1] Danmark repræsenteres af Center for Cybersikkerhed i NIS-samarbejdsgruppen, og er repræsenteret af relevante myndigheder i de eksisterende undergrupper.

drage relevante eksterne interessenter i arbejdet, f.eks. rådgivende organer i offentlige organisationer, erhvervslivet, tjenesteudbydere og operatører. I henstillingen lægges op til, at undergruppen udarbejder en fællesgennemførelsesplan og indgår i arbejdet om udviklingen af fælles europæiske standarder. Dertil skal undergruppen indlede drøftelser med andre relevante organer såsom Europol og NATO for at undgå duplikation og sikre en sammenhængende tilgang.

En fælles gennemførelseskøreplan
I henstillingen udlægger Kommissionen, at den koordinerede gennemførelseskøreplan for kvantesikker kryptografi bør foreligge to år efter offentliggørelsen af henstillingen og skal udvikle en skabelon for fastlæggelsen af nationale planer for overgangen til kvantesikker kryptografi eller, hvor der allerede findes nationale planer, tilpasning af disse planer efter principperne i den fælles koordinerede gennemførelseskøreplan. Den koordinerede gennemførelseskøreplan skal i overensstemmelse med Unions konkurrenceregler og EU's databeskyttelseslovgivning indeholde en liste over foranstaltninger, som medlemsstaterne skal træffe, herunder overvejelser om algoritmer til kvantesikker kryptografi med en klar tidsplan for de forskellige faser og milepæle.

Udvikling af fælles europæiske standarder
I henstillingen opfordrer Kommissionen medlemsstaterne til på EU-plan at arbejde tæt med EU's cybersikkerhedseksperter, NIS-samarbejdsgruppen og Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) om evaluering og udvælgelse af passende algoritmer til kvantesikker kryptografi og deres vedtagelse som EU-standarder med henblik på harmoniseret indførelse i hele Unionen. Henstillingen udlægger, at medlemsstaterne fortsat bør samarbejde med internationale, strategiske partnere om udviklingen af internationale standarder inden for kvantesikker kryptografi fro at sikre kommunikationssystemernes interoperabilitet i fremtiden.

Foranstaltninger på EU-plan
Kommissionen vil overvåge de foranstaltninger, der træffes som reaktion på henstillingen og opfordrer medlemsstaterne til på Kommissionens anmodning at forelægge alle relevante oplysninger. Forelæggelsen heraf vil være frivillig for medlemsstaterne. På grundlag af de indhentede oplysninger og andre tilgængelige oplysninger vil Kommissionen vurdere virkningerne af denne henstilling og afgøre, om der er behov for yderligere foranstaltninger, herunder forslag til bindende EU-retsakter.

1. Europa-Parlamentets udtalelser
Europa-Parlamentet skal ikke høres.

2. Nærhedsprincippet
Ej relevant.

3. Gældende dansk ret
Der redegøres ikke for gældende dansk ret, da en henstilling fra Kommissionen ikke er juridisk bindende for medlemsstaterne.

4. Konsekvenser

Lovgivningsmæssige, økonomiske og andre konsekvenser, herunder beskyttelsesniveauet

Henstillingen medfører i sig selv ikke lovgivningsmæssige eller økonomiske konsekvenser. Indholdet i henstillingen kan dog senere blive udmøntet i konkrete retsakter eller initiativer, der kan medføre konsekvenser. Der vil i den forbindelse blive foretaget en særskilt vurdering af det konkrete forslag, såfremt det fremsættes. Det bemærkes, at afledte nationale udgifter som følge af EU-retsakter afholdes inden for de berørte ministeriers eksisterende bevillingsramme, jf. budgetvejledningens bestemmelser herom.

5. Høring

Henstillingen er sendt i høring i EU-specialudvalget for civilbeskyttelsesområdet, Uddannelses- og Forskningsministeriet, Forsvarsministeriets Materiel- og Indkøbsstyrelse, Forsvarets Efterretningstjeneste, regeringens rådgivende gruppe for dansk forsvarsindustri og Danish Quantum Community.

Dansk Industri

Cybersikkerhed, databeskyttelse og sikring af følsom kommunikation er afgørende for økonomien, sikkerheden og tilliden til den digitale omstilling af samfundet. Cybersikkerhed er af strategisk betydning for Danmark og EU i forhold til vores erhvervsudvikling og værne om danske interesser.

Kvantecomputerne er allerede på markedet i dag – dog er de endnu ikke særligt kraftige og derfor er deres anvendelse for nu yderst begrænset. Men i de kommende år er det forventningen, at der vil komme teknologiske gennembrud, som vil påvirke trusselslandskabet. Kvanteteknologien er i hastig udvikling, og den tilbyder betydelige på den ene side nye muligheder, og på den anden side introducerer den også sårbarheder, som ondsindede aktører kan udnytte. Det er afgørende, at vi kan forstå og afbøde disse risici. Det kræver samarbejde internationalt og med erhvervslivet.

Udviklingen mod at udvikle brugbare kvantecomputere, som kan løse komplekse problemstillinger og kryptering accelereres voldsomt i disse år – både på forskningsinstitutionerne og i virksomhederne.

Dansk Industri hilser derfor Kommissionens henstilling om en koordineret gennemførelsesplan for overgangen til kvantesikker kryptografi velkommen. Danmark har et rigtig godt udgangspunkt for at udarbejde og implementere en strategi pga. vores dybe digitalisering af samfundet. I den sammenhæng er det vigtigt, at vi i Danmark fortsætter med at arbejde for teknologineutrale løsninger.

Vi har i Danmark forskere og virksomheder, som allerede i dag eksperimenterer og implementerer løsninger hos offentlige myndigheder og i vores kritiske infrastruktur. Vi har forskere og virksomheder, som leverer kvantesikker kryptering, kvanteinternet og hardware til kryptering. Det er vigtigt, at den fremtidige strategi har et fokus på erhvervsudvikling, så vi anvender vores internationale styrkeposition inden for kvanteteknologi, så vi kan levere danske løsninger, der kan konkurrere på dette nye vækstmarked.

Vigtigt med rød tråd til eksisterende strategier og god koordinering til samarbejdspartnere
Det er vigtigt, at vi får skabt en rød tråd mellem tidligere strategier og eksisterende initiativer med at teste og udrulle cybersikkerhed og kvantesikker kommunikation i Danmark. Det er vigtigt, at der skabes kvantesikre løsninger med vores internationale samarbejdspartnere, da vores kritiske infrastrukturer er integreret med vores nabolandes. Derfor bør vi have en god inddragelse og koordinering af vores samarbejdspartnere, så vi får skabt de bedste mulige løsninger i Danmark og med vores nabolande.

Danmark som international anerkendt frontløber i udviklingen og implementeringen af kvantesikker kryptografi i kritisk infrastruktur
Strategien skal have et stærkt fokus på at udvikle soft- og hardware løsninger samt implementere løsninger i den offentlige sektor og den kritiske infrastruktur. I Danmark er vores kritiske infrastruktur og offentlige myndigheder gennemdigitaliseret. Samtidigt er vi globalt set blandt de førende lande i verden, når det kommer til forskning og anvendelse af kvanteteknologi. Vi er et samfund, som i høj grad er åbne overfor nye løsninger og med stærke digitale kompetencer i offentlige myndigheder, virksomheder og hos borgerne. Vi ser allerede en række initiativer af forskere og virksomheder, som eksperimenterer med at skabe fremtidens kvantesikre løsninger. Vi bør derfor udnytte og udbygge dette ved at gøre Danmark til en nøgleaktør, hvor virksomheder kan komme til landet og eksperimentere og implementere kvantesikre cyberløsninger.

Der er åbenlyse synergier mellem eksisterende projekter og strategier fx Danish Quantum Communication Infrastructure (QCI.dk), projektet "CryptQ" med test af kvanteløsninger i elnettet, NATO-acceleratoren, de danske kvante strategier mv. Vi har allerede vist, at vi i Danmark kan løse udfordringerne som kvanteteknologier skaber på cyberområdet og derfor skal vi omsætte løsningerne til erhvervsudvikling og sætte Danmark på verdenskortet. Dansk Industri står naturligvis til rådighed, hvis der er behov for uddybende bemærkninger eller bilaterale drøftelser af dagsorden. Vi vil meget gerne komme med løbende inputs til strategiarbejdet.

Dansk Erhverv
Dansk Erhverv finder det positivt, at EU ønsker, at medlemsstaterne udarbejder en strategi for implementering af kvantesikker kryptografi i offentlige myndigheder, der danner grundlag for nationale planer. Udviklingen af it-systemer, der kan beskytte os mod fremtidige kvantecybertrusler, er en langvarig, kompleks og dyr proces. Derfor er det vigtigt at komme i gang hurtigst muligt. Danmark bør, bl.a. qua sin forskningsposition på området, spille en proaktiv rolle i udviklingen af standarderne på området. Dansk Erhverv ser frem til at bidrage til processen fremadrettet.

Nationalt Forsvarsteknologisk Center (NFC)
Nationalt Forsvarsteknologisk Center (NFC) støtter opfordringen til at oprette arbejdsgrupper og gennemførelseskøreplaner for postkvantekryptografi. NFC kan se fra Kommissionens henstilling, at opgaven vil kræve en del ressourcer, der forlanger involvering af industrien, standardiseringsorganisationer og forskere, samt vil skabe udfordringer med monitorering og håndhævelse. NFCs forskningsmiljø bestående af universiteter og GTS'ere er klar til at bistå på nationalt og EU-niveau.

Vores forskere har påpeget vigtigheden i at involvere forskere, industri og standardiseringsorganisationer (ISO, IEC, mfl.) i det videre arbejde, for at sikre, at postkvantekryptografi bliver integreret i en vifte af produkter og løsninger og i internationale tekniske standarder. For at sikre en bred implementering af kvantesikre algoritmer er det kritisk, at resultatet (de valgte kvantesikre algoritmerne) bliver inkluderet i standarder og standard teknologier. Den tekniske sikkerhed i de fleste IT/OT-systemer, herunder kritisk infrastruktur, er beskrevet i standarder som eksempelvis ISO 27002, ISO/IEC 62443 serien, IEC 62351, m.fl. Disse standarder bygger alle på andre mere tekniske standarder og specifikationer til at opnå den ønskede sikkerhed, eksempelvis er TLS (IETF) og de underliggende X.509 TLS certifikater (ITU-T), med dertilhørende cipher suites (IANA), grundstenen i stort set al kommunikation.

For at sikre, at produkter og løsninger kan anvende kvantesikre algoritmer, er det derfor vigtigt, at de basale tekniske standarder og specifikationer kommer til at indeholde de nye kvantesikre algoritmer. Ligeledes er det vigtigt at få producenterne af implementationerne af disse komponenter involveret, så der findes produkter, der kan implementere kvantesikre algoritmer. Hvis ikke disse standardiseringsorganisationer og private producenter involveres i arbejdet, er det vores frygt, at henstillingen blot vil resultere i en række krav og påbud omkring brugen af nye algoritmer, som ingen standardprodukter kan levere. Det vil betyde, at en stor mængde tekniske implementationer vil skulle genimplementeres, hvilket kan have stor økonomisk konsekvens for de involverede.

Syddansk Universitet (SDU)
Det er væsentligt, at arbejdet med kvantekrypteret sikring er meget bevist om den relativt hurtige udvikling af kvantesikre krypteringer. Vi har set en udvikling over de senere år, hvor en række algoritmer, man troede var kvantesikre, ikke var det alligevel efter nærmere analyse. Dette er et fortsat udviklende felt og antallet af algoritmer som opfattes at være kvantesikre er for støt nedadgående. Det er derfor vigtigt, at arbejdet på dette område er opmærksom på denne udvikling og tager dette i betragtning, når man vægter kvantekryptering op imod kvantenøgledeling (QKD). QKD kan ikke brydes af en kvantecomputer og har derfor en langt længere garanteret horisont, men kræver selvfølgelig også en større investering og omlægning. Sydkorea er førende i verden på dette område, og der er indikationer på, at der arbejdes en del med denne model i Kina.

Det er også vigtigt at være opmærksom på, at der er firmware kryptering i en stor del af vores kritiske infrastruktur, som kræver en stor indsats i forhold til opdatering af kryptering. Dette er hardware, som sidder i mange forskellige fysiske komponenter, og hvor krypteringen er integreret i hardware og muligvis ikke kan gøres kvantesikker uden udskiftning. Mange sådanne komponenter godkendes til brug 20-30 år ud i fremtiden, hvilket også gør, at der er en vis mænge af komponenter, som er i funktion med en alder på over 10 eller 20 år og med deraf følgende ringe sikkerhed i forhold til kvanteangreb. Der forligger en stor opgave i at identificere de mest kritiske af disse og få dem opdateret, og i nogle tilfælde vil dette kun kunne ske ved fysisk udskiftning af komponenten. Desuden det selvfølgelig vigtigt, at vi ikke fortsætter med at godkende komponenter nu, som ikke kan bruge kvantesikret kryptering i 20-30 år ud i fremtiden.

Aarhus Universitet og Security Tech Space
Vi vil gerne henlede opmærksomhed på, at man i forbindelse med implementeringen 1) også kigger på standarder som er udviklet uden for EU og 2) tager højde for at quantum key distribution (QKD, som er nævnt en enkelt gang) kun giver mening hvis den rigtige infrastruktur er til stede. QKD kan desuden ikke stå alene, men må nødvendigvis kombineres med klassiske metoder til autentifikation.

Herudover vil vi gerne henlede opmærksomheden på, at Aarhus Universitet og Aarhus Kommune har taget initiativ til konsortiet Security Tech Space, hvor vi i samarbejde med foreløbigt ca. 65 partnere fra industri og myndigheder arbejder på at styrke forskning, innovation og erhvervsudvikling inden for cybersikkerhed. Udgangspunktet for etableringen af konsortiet er det stærke økosystem i Aarhus, hvor Aarhus Universitet er verdensførende inden for cybersikkerhed. Med inspiration fra andre lande etablerer vi desuden Cyber Campus Denmark og som en del heraf har vi blandt andet foreslået etableringen af en ny cyberværnepligt i Aarhus. Med udgangspunkt i Cyber Campus Denmark bidrager vi meget gerne til implementeringen af kvantesikker kommunikation.

Danmarks Tekniske Universitet (DTU)
DTU byder EU-Kommissionens henstilling om en koordineret gennemførelseskøreplan for overgangen til kvantesikkerkryptografi (post quantum cryptography, PQC) velkommen. Det er vigtigt at både europæiske og nationale myndigheder såvel som virksomheder allerede nu forbereder sig på de udfordringer, som kvantecomputere kan betyde for dansk og europæisk cybersikkerhed, og dermed er "quantum ready". Det gælder PQC, som rummer muligheder for at højne det eksisterende cybersikkerhedsniveau, men det er samtidigt vigtigt at forstå nogle af manglerne ved teknologien. Et for snævert fokus på PQC kan netop skabe nye risici, hvor PQC bliver et muligt "single point of failure", hvor for stor tillid til teknologien kan skabe systematisk usikkerhed i IT-systemet. Der er derfor behov for fortsat at have traditionelle, testede og validerede cybersikkerhedsløsninger og se på andre kvantekrypteringsmetoder, så som kvantenøglefordeling (quantum key distribution (QKD)). QKD benytter kvanteteknologi til at skabe kvantesikre forbindelser, og har dermed potentiale til at styrke sikkerhedsniveauet markant. Et fokus på kvantesikre netværk bør derfor kombinere traditionelle metoder, PQC og QKD.

DTU er i verdensklasse, når det drejer sig om at få kvanteteknologi til at virke, og vi udvikler kvantekrypteringsnetværk i tæt samarbejde med danske virksomheder, myndigheder og andre universiteter. DTU kan derfor sammen med de andre universiteter, GTS'er og i regi af NFC bistå med rådgivning i forhold til kvantekryptering på nationalt og europæisk niveau.

6. Generelle forventninger til andre landes holdninger

Der forventes generelt at være støtte til henstillingen og formålet om at fremme overgangen til kvantesikker kryptografi gennem fastlæggelsen af en koordineret gennemførelsesplan for kvantesikker kryptografi og træffe passende og forholdsmæssige foranstaltninger til at forberede denne overgang. Det bemærkes, at nogle medlemsstater allerede har annonceret nationale planer for ovegangen til kvantesikker kryptografi. Det gælder blandt andet Tyskland, Frankrig og Nederlandene.

Der har været indledende drøftelser om henstillingen i forbindelse med forhandlingerne om Rådskonklusioner ang. fremtidens cybersikkerhed. Det forventes i den videre drøftelse, at en gruppe medlemsstater vil give udtryk for, at medlemsstaterne skal kunne gennemføre deres egne tekniske analyser, inden der udarbejdes en koordineret, europæiske gennemførelseskøreplan. Dertil forventes det, at andre medlemsstater vil fremhæve, at en koordineret gennemførelseskøreplan skal respektere medlemsstaternes nationale kompetencer ift. at beskytte deres kritiske, digitale infrastruktur.

Dertil er der en forventning om, at nogle medlemsstater vil have en stærk præference for at udelukkende at fokusere på kvantesikker kryptografi i den koordinerede gennemførelseskøreplan. En anden gruppe medlemsstater ønsker både at udforske kvantenøglefordeling og kvantesikker kryptografi.

Hvad angår evaluering og udvælgelse af relevante EU-algoritmer til kvantesikker kryptografi og fremme af yderligere indførelse af disse algoritmer som EU-standarder, ventes det, at der vil være fokus på at sikre sammenhæng til den første standard for kvantesikker kryptografi fra USA's National Institute of Standards and Technology (NIST), der forventes annonceret i 2024.

7. Regeringens foreløbige generelle holdning

Regeringen hilser Kommissionens henstilling om en koordineret gennemførelseskøreplan for overgangen til kvantesikker kryptografi velkommen og finder det positivt, at der skal arbejdes med at fremme overgangen til kvantesikker kryptografi med henblik på beskyttelse af offentlige myndigheders digitale infrastrukturer og tjenester og andre kritiske infrastrukturer.

Databeskyttelse og sikring af følsom kommunikation er afgørende for samfundet, økonomien, sikkerheden og velstanden i EU, og kryptering er en central teknologi ift. at opnå modstandsdygtighed og opbygge kapacitet til at forebygge fx cyberangreb eller andre hybride angreb. Regeringen stiller sig derfor positiv over for initiativer, der lægger op til en styrkelse af EU's kollektive modstandsdygtighed over for cybertrusler og ondsindede handlinger i cyberspace.

Regeringen finder det væsentligt, at Danmark rettidigt igangsætter arbejdet med at styrke Danmarks kritiske digitale infrastruktur mod kompromittering fra eksempelvis kvantecomputere, som det understreges i den nationale kvantestrategi del 2 og ved etableringen af Sekretariatet for kvantesikker, kritisk digital infrastruktur (SEKDI) i Center for Cybersikkerhed. Regeringen finder det ligeledes vigtigt, at dette sker i tæt samarbejde i EU og med ligesindede internationale partnere.

Opbygningen af ondsindede aktørers kvantedatabehandlingskapacitet og den fremtidige udvikling af kvantecomputere udgør en trussel mod vores datafortrolighed og –integritet, følsom kommunikation og væsentlige elementer i netværkssikkerhed, herunder i EU. Regeringen er derfor positivt indstillet over for formålet om, at der fastlægges en koordineret tilgang til overgangen til kvantesikker kryptografi, som kan synkronisere medlemsstaternes indsats for at udforme og gennemføre nationale overgangsplaner til kvantesikker kryptografi. Dette til fordel for cybersikkerhed i Europa, beskyttelse af digitale infrastrukturer samt interoperabiliteten og funktionaliteten på tværs af grænser.

Regeringen finder det vigtigt, at en koordineret overgang til kvantesikker kryptografi sker med respekt for kompetencefordeling mellem medlemsstaterne og EU, herunder i respekt for medlemsstaternes kompetence på området for national sikkerhed, samt den fælles udenrigs-, forsvars- og sikkerhedspolitik. Regeringen finder det vigtigt, at køreplanen for implementering af kvantesikker kryptografi i EU sker i overensstemmelse med Unionens konkurrenceregler og EU's databeskyttelseslovgivning.

Regeringen hilser nedsættelsen af en undergruppe om kvantesikker kryptografi velkommen. Regeringen er dog foreløbigt skeptisk over for at nedsætte undergruppen ved NIS-samarbejdsgruppen. NIS-samarbejdsgruppen er oprettet med det formål at sikre betimelig implementering af NIS1 og NIS2-direktiverne, hvorfor oprettelsen af en ny undergruppe ved NIS-samarbejdsgruppen risikerer at tage vigtig fokus og ressourcer væk fra NIS2 implementeringen i medlemsstaterne, inklusiv i Danmark. Regeringen finder derfor foreløbigt, at undergruppen om kvantesikker kryptografi bør nedsættes i andet regi, fx ved Security Comitee's Crypto Task Force undergruppe, der beskæftiger sig med kryptografering.

I arbejdet med udviklingen af kvantesikker kryptografi, finder regeringen det vigtigt, at medlemsstaterne koordinerer indsatsen og i relevant omfang inddrager offentlige og private interessenter. Regeringen finder det desuden centralt, at undergruppen indleder drøftelser med relevante aktører for at undgå dobbeltarbejde og sikre en sammenhængende tilgang til håndtering af nye udfordringer.

Regeringen finder det vigtigt, at rammen for evalueringen og udvælgelsen af relevante EU-algoritmer til kvantesikker kryptografi og deres efterfølgende indførelse som EU-standarder i digitale tjenester netværk og tjenester samt kritiske infrastrukturer, sker med udgangspunkt i den løbende udvikling, afprøvning og offentliggørelse af relevante kvantesikre kryptografiske algoritmestandarder, herunder den forventeligt første standard for kvantesikker kryptografi fra USA's NIST, som ventes offentliggjort i 2024. Regeringen finder det ligeledes vigtigt, at dette sker proportionelt med vigtigheden af overgangen til kvantesikker kryptografi i EU. Ligeledes finder regeringen det væsentligt, at fremtidige kryptografiske løsninger, herunder kvantenøglefordelingsteknologi ("Quantum Key Distribution" eller QKD), også tages i betragtning i forbindelse med overgangen til kvantesikker kryptografi.

Regeringen mener, at der bør sikres sammenhæng og undgås unødvendige overlap mellem gældende og fremtidig regulering og indsatser. Regeringen finder det her vigtigt, at der også tages højde for eksisterende lovgivning, der skal bidrage til et højt cybersikkerhedsniveau i EU, så der ikke skabes unødige administrative og økonomiske byrder for virksomheder og offentlige myndigheder.

Regeringen finder det væsentligt, at arbejdet sammentænkes med EU's initiativer på området, herunder EuroQCI, samt ambitionerne i NATO's strategi for kvanteteknologi, herunder arbejde i NATO-regi omkring udvikling af standarder for kvantesikker kommunikation.

Regeringen vil tage nærmere stilling til konkrete forslag eller foranstaltninger som følge af gennemførelsesplanen for kvantesikker kryptografi når disse foreligger.

8. Tidligere forelæggelser for Folketingets Europaudvalg

Sagen har ikke tidligere været forelagt Folketingets Europaudvalg.