Forsvarsministeriet
7. marts 2013

Grund- og Nærhedsnotat til Folketingets Europaudvalg

Europa-Kommissionens og Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitiks fælles meddelelse til Europa-Parlamentet, Rådet, den Europæiske Økonomiske og Sociale Komite og Regionskomiteen

**Cybersecurity Strategy of the European Union:
An Open, Safe and Secure Cyberspace**

JOIN (2013) 1 endelig

1. Resumé

Meddelelsen om en strategi for cybersikkerhed lægger op til en diskussion af EU's internetsikkerhed. I meddelelsen betones vigtigheden af informations- og kommunikationsteknologi (IKT) og af internettets rolle som international kommunikationsvej, og der peges på de risici, der er forbundet med anvendelsen af internettet, og de deraf følgende behov for at sikre netværkene bedre. En række medlemsstater, herunder Danmark, har allerede taget initiativ til at udfærdige strategier for cybersikkerhed, men der lægges op til en overordnet, fælles strategi for EU, fordi der stadig er mangler i medlemsstaternes egen beskyttelse.

Meddelelsen adresserer emnet bredt. I meddelelsen anbefales nationale tiltag overfor angreb fra internettet, herunder styrkelse af nettenes robusthed, tiltag med henblik på nedbringelse af cyberkriminalitet, samt at der udvikles en cyberforsvarspolitik i forbindelse med den fælles sikkerheds- og forsvarspolitik. Desuden anbefales det at styrke udvikling og produktion af sikkerhedsprodukter i EU. Den Fælles Udenrigstjeneste skal indgå i forhandlinger med andre lande om at få udviklet en international politik for cybersikkerhed. Det erkendes, at ansvaret for cybersikkerhed er fordelt på mange aktører, både nationalt og internationalt, og der opfordres til et øget samarbejde på alle planer.

Regeringen hilser meddelelsen velkommen. Der er behov for en fælles indsats til beskyttelse af den internationale kommunikations- og informationsstruktur. Regeringen afventer de konkrete udspil, som måtte komme fra Kommissionen med henblik på en implementering af denne strategi.

2. Baggrund

Kommissionen og Unionens højtstående repræsentant for udenrigsanliggender og sikkerhed har ved *JOIN(2013) 1* af 7. februar 2013 udsendt meddelelse om *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*.

Informations- og kommunikationsteknologi (IKT) er blevet rygraden i vores økonomiske vækst og er en kritisk ressource, som alle sektorer er afhængige af. IKT danner grundlaget for komplekse systemer indenfor nøglesektorer som finans, sundhed, energi og transport, og mange forretningsmodeller er bygget på uafbrudt internettilgængelighed og velfungerende informationssystemer.

I de senere år er det også blevet klart, at samtidig med den digitale verdens enorme fordele, er den også sårbar. Derfor er regeringer i hele verden begyndt at udvikle cybersikkerhedsstrategier.

Som et væsentligt initiativ under strategien har Kommissionen, ved KOM(2013) 48 af 7. februar 2013 fremsendt forslag til direktiv om foranstaltninger, der skal sikre et højt fælles niveau for net- og informationssikkerhed i hele EU med henblik på at implementere cybersikkerhedsstrategien.

Der forelægges Folketingets Europaudvalg et særskilt grund- og nærhedsnotat om direktivet vedrørende net- og informationssikkerhed (NIS-direktivet).

3. Formål og indhold

Meddelelsen er fremkommet som et fælles udspil fra DG CONNECT, DG HOME og Den Fælles Udenrigstjeneste, og der redegøres for de principper, der bør være ledende for en fælles cybersikkerhedspolitik for EU. Der lægges vægt på, at EU's kerneværdier, som gælder i dagligdagen, også er gældende på internettet, herunder beskyttelse af fundamentale rettigheder, ytringsfrihed, persondata og privatliv, uhindret adgang til informationer for alle, en demokratisk styring og et fælles ansvar for sikkerhed.

Visionen, der præsenteres i strategien, er udtrykt i fem strategiske prioriteringer:

- Robusthed over for cyberangreb.
- Drastisk reduktion af cyberkriminalitet.
- Udvikling af cyberforsvarspolitik og kapabiliteter i forbindelse med den fælles sikkerheds- og forsvarspolitik.
- Udvikling af de industrielle og teknologiske ressourcer inden for cybersikkerhed.
- Etablering af en sammenhængende international cyberpolitik for den Europæiske Union og fremme EU-kerneværdier.

Robusthed over for cyberangreb

At styrke cybersikkerhed er et fælles ansvar. For at fremme robusthed mod cyberangreb må både det offentlige og den private sektor udvikle yderligere kapaciteter og indgå i et effektivt samarbejde.

Den private sektors deltagelse sikres, fordi en stor del af netværks- og informationssystemerne er privatejede. Cyberøvelser på EU-niveau meget vigtige for at stimulere samarbejde mellem medlemsstaterne og den private sektor.

Slutbrugerne spiller en vigtig rolle i arbejdet med at sikre netværks- og informationssystemer. Kommissionen inviterer derfor medlemsstaterne til at organisere en årlig cybersikkerhedsmåned.

Drastisk reduktion af cyberkriminalitet

Af meddelelsen fremgår det, at cyberkriminalitet er en af de hurtigst voksende former for kriminalitet. Cyberkriminelle og deres netværk bliver mere og mere sofistikerede, og det er nødvendigt at have de rigtige operationelle redskaber og kapaciteter til at håndtere dem. Cyberkriminalitet kender ingen grænser - den globale rækkevidde af internettet betyder, at retshåndhævelse skal anvende en koordineret, samarbejdende og grænseoverskridende tilgang til denne voksende trussel.

I meddelelsen påpeges, at EU og medlemsstaterne har brug for en stærk og effektiv lovgivning for at bekæmpe it-kriminalitet. Der er behov for en forbedret operationel kapacitet til bekæmpelse af internetkriminalitet. I øjeblikket er det ikke alle EU-medlemsstater, der har den nødvendige kapacitet til effektivt at kunne reagere på cyberkriminalitet. Alle medlemsstaterne har brug for effektive nationale enheder til at bekæmpe cyberkriminalitet.

Kommissionen vil gennem sine programmer støtte medlemsstaterne med henblik på at styrke deres kapacitet til at efterforske og bekæmpe it-kriminalitet, og arbejde tæt sammen med Eurojust og det nyligt lancerede europæiske Cybercrime Centre (EC3), som er etableret under Europol.

Udvikling af en cyberforsvarspolitik og kapabiliteter i forbindelse med den fælles sikkerheds- og forsvarspolitik

I meddelelsen fremhæves, at indsatsen for cybersikkerhed i EU også må inddrage cyberforsvar. Da truslerne er mangeartede, bør synergier mellem civile og militære tilgange til at beskytte kritiske cyberaktiver styrkes. Disse bestræbelser bør støttes af forskning og udvikling, og et tættere samarbejde mellem regeringer, den private sektor og forskning i EU.

Unionens højtstående repræsentant for udenrigsanliggender og sikkerhed vil fokusere på følgende aktiviteter, som medlemsstaterne og det Europæiske Forsvarsagentur inviteres til samarbejde om at:

- undersøge krav til EU-cyberforsvaret samt fremme udvikling af EU-cyberforsvars kapaciteter og teknologier med henblik på at håndtere alle aspekter af kapacitetsudvikling,
- udvikle EU's cyberforsvarspolitiske struktur for at beskytte netværk inden for den fælles sikkerheds og forsvarspolitiks missioner og operationer, herunder dynamisk risikostyring, forbedret trusselsanalyse og informationsdeling. Mulighederne for cyberforsvarsuddannelse samt øvelser skal forbedres for militæret i europæisk og multinationale sammenhæng, herunder integration af cyberforsvarselementer i den eksisterende øvelseskontekst,
- fremme dialog og koordinering mellem civile og militære aktører i EU – med særlig vægt på udveksling af god praksis, udveksling af oplysninger og tidlig varsling, hændelseshåndtering, risikovurdering, sikkerhedsbevidsthed og at prioritere cybersikkerhed og
- sikre en dialog med internationale partnere, herunder NATO, andre internationale organisationer og multinationale ekspertcentre, at sikre et effektivt forsvar, identificere områder for samarbejde og undgå dobbeltarbejde.

Udvikle de industrielle og teknologiske ressourcer inden for cybersikkerhed

Mange af de globale, ledende virksomheder, der tilbyder innovative IKT-produkter og -tjenester er uden for EU. Der er en risiko for, at Europa ikke kun bliver for afhængig af IKT produceret andre steder, men også af sikkerhedsløsninger, der er udviklet uden for egne grænser. Det er væsentligt at sikre, at hardware og softwarekomponenter er pålidelige og sikre.

Af meddelelsen fremgår det, at en høj grad af sikkerhed kun kan opnås, hvis alle i værdikæden (fx fabrikanter, softwareudviklere, tjenesteudbydere) prioriterer sikkerhed. Det ser dog ud til, at mange aktører stadig betragter sikkerhed som en ekstra byrde. Den private sektor har brug for incitamenter til at sikre et højt niveau for sikkerheden på internettet. En efterspørgsel efter meget sikre produkter bør stimuleres.

Strategien sigter mod at øge samarbejde og åbenhed om sikkerheden i IKT-produkter. Den opfordrer til oprettelse af en platform, der samler relevante europæiske offentlige og private interessenter med henblik på at skabe gunstige markedsforhold for udvikling af sikre IKT-løsninger. Muligvis kan der etableres en frivillig EU-dækkende certificering, der bygger på eksisterende ordninger i EU og internationalt.

Desuden vil Kommissionen støtte udviklingen af sikkerhedsstandarder.

Forskning og udvikling kan understøtte en stærk industripolitik med henblik på at fremme en pålidelig europæisk IKT-industri, styrke det indre marked og reducere Europas afhængighed af udenlandske teknologier.

Kommissionen vil bruge Horisont 2020 (rammeprogram for forskning og innovation 2014-2020) for at udforske en række problemstillinger omkring privatlivets fred. Horisont 2020 kan også anvendes til at udvikle værktøjer til at bekæmpe kriminalitet og terrorisme på cyberområdet. Kommissionen opfordrer medlemsstaterne til at anvende den købekraft, offentlige myndigheder har gennem offentlige indkøb, til at stimulere udvikling og udbredelse af sikkerhedsfunktioner i IKT-produkter og -tjenester.

Etablere en sammenhængende international cyberpolitik for den Europæiske Union og fremme EU-kerneværdier

Via en international cyberpolitik vil EU søge at fremme åbenhed og frihed på internettet og fremme bestræbelserne på at udvikle normer for adfærd på internettet. Hertil vil EU anvende eksisterende internationale love, og EU vil deltage aktivt i de internationale bestræbelser på at opbygge cybersikkerhed. EU's internationale engagement i cyberspørgsmål vil blive styret af EU-kerneværdier, menneskelig værdighed, frihed, demokrati, ligestilling, retsstaten og respekten for de grundlæggende rettigheder.

Fremhæve internetforhold over for EU's eksterne forbindelser og den fælles udenrigs- og sikkerhedspolitik

Kommissionen og Den Fælles Udenrigstjeneste bør jævnfør meddelelsen udtrykke en sammenhængende international EU internetpolitik.

EU vil søge tættere samarbejde med internationale partnere om cyberspørgsmål. Samarbejdet med USA er særlig vigtigt og vil blive videreudviklet. Et af de vigtigste elementer i EU's internationale cyberpolitik vil være at fremme internettet som et område med frihed og grundlæggende rettigheder. Øget global mulighed for forbindelse til internettet bør ikke være ledsaget af censur eller masseovervågning.

Meddelelsen fremhæver, at EU ikke finder det er nødvendigt at oprette nye internationale retlige instrumenter for cyberspørgsmål. De juridiske forpligtelser, der er nedfældet i den internationale konvention om borgerrettigheder, den europæiske menneskerettighedskonvention og Den Europæiske Unions charter om grundlæggende rettigheder, bør også respekteres online. EU vil fokusere på, hvordan man sikrer, at disse foranstaltninger også

kan håndhæves på internettet. Hvis væbnede konflikter udvides til cyberspace, vil folkeretten og i givet fald Den Internationale Menneskerettighedskonvention gælde i det konkrete tilfælde.

Udvikle kapacitetsopbygning i forhold til cybersikkerhed og modstandsdygtige informationsinfrastrukturer i tredjelande

I samarbejde med medlemsstaterne vil Kommissionen og Den Fælles Udenrigstjeneste:

- arbejde for en sammenhængende international internetpolitik for at styrke samarbejdet med de vigtigste internationale partnere og organisationer, integrere cyberspørgsmål i den fælles udenrigs- og sikkerhedspolitik, og forbedre koordineringen af globale cyberspørgsmål,
- støtte udvikling af normer for adfærd og tillidsskabende foranstaltninger inden for internetsikkerhed, og iværksætte samtaler om, hvordan man kan anvende folkeretten i cyberspace og inkludere cyberkriminalitet i Budapest-konventionen,
- støtte, fremme og beskytte de grundlæggende rettigheder, herunder adgang til information og ytringsfrihed,
- samarbejde med internationale partnere og organisationer, den private sektor og civilsamfundet for at støtte den globale udvikling i tredjelande og forbedre adgang til information og til et åbent internet,
- anvende forskellige EU-støttemuligheder til opbygning af cybersikkerhed, herunder bistå med uddannelse af personale til at imødegå cybertrusler, samt støtte oprettelsen af relevante nationale politikker, strategier og institutioner i tredjelande og
- øge den politiske koordinering og informationsdeling gennem internationale netværk, der beskæftiger sig med beskyttelse af kritisk informationsinfrastruktur.

Roller og ansvar

I det digitale samfund stopper cyberhændelser ikke ved grænserne. Alle aktører må iflg. Kommissionen tage ansvar både nationalt og på EU-niveau og arbejde sammen om at styrke cybersikkerhed. Da forskellige retlige rammer og jurisdiktioner er involveret, er det en central udfordring for EU at klarlægge de roller og det ansvar, de mange involverede aktører har.

I betragtning af problemets kompleksitet og de mange forskellige aktører, er en centraliseret europæisk overvågning ikke svaret. Nationale regeringer har de bedste forudsætninger for at organisere forebyggelse af og reaktioner på cyberhændelser og etablere kontakter med den private sektor og offentligheden. Men en effektiv håndtering af et angreb vil ofte også kræve involvering på EU-niveau. Derfor bør der iværksættes aktiviteter indenfor de tre vigtigste søjler – netværksinformationssikkerhed, retshåndhævelse og forsvar.

Koordinering mellem kompetente myndigheder for NIS/CERT, retshåndhævelse og forsvar

Nationalt

Meddelelsen understreger, at medlemsstaterne bør være i stand til at håndtere angreb fra internettet, cyberkriminalitet og cyberforsvar. Men i betragtning af, at det operationelle ansvar for de forskellige dimensioner af cybersikkerhed kan være spredt på mange myndigheder, bør koordinering på nationalt plan optimeres på tværs af ministerier. Medlemsstaterne bør i deres nationale cybersikkerhedsstrategier fastlægge roller og ansvar for deres forskellige nationale myndigheder.

Informationsdeling mellem de nationale myndigheder og den private sektor bør fremmes, så det er muligt for medlemsstaterne og den private sektor at opretholde et samlet overblik over forskellige trusler og få en bedre forståelse for nye tendenser og de teknikker, der anvendes.

EU

På EU-niveau er der en række aktører, der beskæftiger sig med cybersikkerhed, især ENISA, Europol/EC3 og EDA. Koordinering og samarbejde vil blive fremmet mellem disse på en række områder. Disse agenturer bør sammen med CERT-EU, Kommissionen og medlemsstaterne støtte etablering af en fælles gruppe af tekniske og politiske eksperter på dette område.

Internationalt

Kommissionen og EU's udenrigstjeneste vil sammen med medlemsstaterne sikre en koordineret international indsats inden for sikkerhed på internettet. Herigennem vil de opretholde EU's kerneværdier og fremme en fredelig, åben og gennemsigtig brug af cyberteknologier.

EU-støtte i tilfælde af en større cyberhændelse eller et angreb

Større cyberhændelser eller angreb kan forventes at have en indvirkning på EU-landenes regeringer, erhvervsliv og enkeltpersoner. Denne strategi, og navnlig forslaget til direktiv om netværksinformationssikkerhed, bør forbedre medlemsstaternes og Kommissionens håndtering af cyberhændelser og styrke udveksling af relevante informationer.

Meddelelsens konklusion og Kommissionens opfølgning

Forslaget til en cybersikkerhedsstrategi for Den Europæiske Union, som er fremsat af Kommissionen og Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik, skitserer EU's vision og de nødvendige tiltag, med henblik på at gøre EU's in-

ternet-miljø til det sikreste i verden. Denne vision kan kun realiseres gennem et ægte partnerskab mellem mange aktører.

Kommissionen og den højtstående repræsentant opfordrer derfor Rådet og Europa-Parlamentet til at godkende strategien og bidrage til at levere de foreslåede aktiviteter.

For at sikre, at strategien gennemføres hurtigt og bliver revurderet i lyset af den fremtidige udvikling, vil alle relevante parter blive inviteret til en konference på højt plan med henblik på at vurdere fremskridtene om 12 måneder.

4. Europa-Parlamentets udtalelser

Europa-Parlamentet skal ikke høres.

5. Nærhedsprincippet

Spørgsmålet om nærhedsprincippet er ikke relevant.

6. Gældende dansk ret

Meddelelsen har ingen umiddelbar retsvirkning i forhold til dansk lov.

7. Konsekvenser

Lovgivningsmæssige eller statsfinansielle konsekvenser

Meddelelsen har ingen umiddelbare lovgivningsmæssige eller statsfinansielle konsekvenser.

Finansieringen af strategien foreslås af Kommissionen at ske inden for de fastsatte beløb for de relevante politiske områder (CEF, Horisont 2020, Fonden for Intern Sikkerhed, FUSP og eksternt samarbejde), som er fastsat i Kommissionens forslag til den flerårige finansielle ramme for 2014-2020. I den udstrækning agenturerne bliver opfordret til at påtage sig nye opgaver som foreslået i strategien, vil dette skulle ske i den udstrækning, de har mulighed for det i forhold til deres samlede kapacitet.

Det kan på nuværende tidspunkt ikke udelukkes, at senere konkrete EU-initiativer indenfor Cyberforsvar, der må udspringe af strategien, vil være underlagt det danske forsvarsforbehold.

Samfundsøkonomiske konsekvenser
Meddelelsen skønnes at kunne bidrage til at styrke sikkerheden ved den danske internetanvendelse, og derigennem få positive samfundsøkonomiske konsekvenser, hvis omfang dog ikke på indeværende tidspunkt kan opgøres.

Administrative konsekvenser for erhvervslivet
Meddelelsen har ingen umiddelbare administrative konsekvenser for erhvervslivet.

8. Høring
Meddelelsen har været i høring i Specialudvalget for civilbeskyttelse (cyberkreds-format) med frist for bemærkninger den 21. februar 2013.

Advokatrådet har svaret, at de ingen bemærkninger har til meddelelsen.

By & Havn har meddelt, at By & Havn har noteret sig forslagets indhold og tilslutter sig et tæt samarbejde indenfor EU, men har derudover ikke yderligere bemærkninger.

Dansk Industri, DI/ITEK noterer sig med tilfredshed, at EU Kommissionen med den nye meddelelse sætter fokus på netværks- og informationssikkerhed og erklærer sig enig med stort set alle de tiltag, som nævnes i meddelelsen. DI/ITEK pointerer vigtigheden af samarbejde også med partnere uden for Europa og fremhæver, at USA allerede i årevis har haft fokus på cyber sikkerhed, og lægger vægt på, at EU bør følge de standarder, der allerede er på området, da det vil være til skade for europæiske virksomheders konkurrenceevne, hvis der er flere sæt standarder, virksomhederne skal efterleve. Det nævnes endvidere, at grænsen mellem cyberkriminalitet og cyberkrig er ved at blive udvisket. DI/ITEK anbefaler, at NATO inddrages i fremtiden og at det afklares, i hvilket omfang eksisterende internationale regler for krig kan overføres til cyberkrig.

Finansrådet bemærker, at der er steder i strategien, hvor der er et særligt fokus på den private sektor, og at det er væsentligt at gøre opmærksom på en mindst ligeså stor risiko, som ligger hos den enkelte bruger, der ikke nødvendigvis er teknisk kyndig. Derfor findes det væsentligt at sikre initiativer i offentlig regi, der fokuserer på borgerens viden om it-sikkerhed og oplysning herom. Finansrådet støtter op om initiativet fra Kommissionens side vedr. et pilotprojekt til bekæmpelse af botnets og malware.

Landbrug & Fødevarer betoner vigtigheden af netværkssikkerhed, og hilser ensartede sikkerhedsnormer i EU-landene velkommen, og udtrykker samtidig et ønske om fokus på parter udenfor EU.

Rådet for Digital Sikkerhed ser positivt på tiltagene fra Kommissionen til at øge sikkerheden og beskyttelsen af den kritiske infrastruktur, som er helt essentiel. Rådet savner dog en indsats for at kortlægge det komplicerede samspil mellem forskellige typer infrastruktur. Rådet for Digital Sikkerhed opfordrer til, at arbejdet med udvikling af en strategi for cybersikkerhed ikke begrænser sig til europæiske organer, men også inddrager den viden, organisationer i andre dele af verden har udviklet. Strategien nævner Awareness Raising som et indsatsområde, der skal bidrage til at sikre, at borgerne har den fornødne viden til at vurdere deres risiko, når de færdes i cyberspace. Rådet for Digital Sikkerhed vil gerne understrege behovet for bedre oplysning af borgerne i forhold til risici, herunder både i forbindelse med angreb og om forebyggende adfærd og valg. Denne opgave kan med fordel placeres hos den nationale CERT, som Kommissionens udspil lægger op til.

9. Generelle forventninger til andre landes holdninger

Der er ikke kendskab til andre landes holdninger.

10. Regeringens foreløbige generelle holdning

Regeringen hilser meddelelsen velkommen. Der er behov for en fælles EU-indsats til beskyttelse af den fælles internationale kommunikations- og informationsstruktur.

Derudover afventer regeringen de konkrete udspil, som måtte komme fra Kommissionen med henblik på en implementering af denne strategi.

Et første direktivforslag blev offentliggjort samtidig med denne strategi. Dette direktiv, som vedrører net- og informationssikkerhed (NIS-direktivet), bliver behandlet i et særskilt grundnotat.

11. Tidligere forelæggelse for Folketingets Europaudvalg

Sagen har ikke tidligere været forelagt for Folketingets Europaudvalg.