EUROPA-
KOMMISSIONEN

Bruxelles, den 5.7.2016
COM(2016) 410 final

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET, RÅDET, DET EUROPÆISKE ØKONOMISKE OG SOCIALE UDVALG OG REGIONSUDVALGET

Styrkelse af Europas system for modstandsdygtighed over for cyberangreb og fremme af en konkurrencedygtig og innovativ cybersikkerhedsindustri

1. INDLEDNING/BAGGRUND

Hver dag forårsager cybersikkerhedshændelser store økonomiske skader for europæiske virksomheder og økonomien som helhed. Sådanne hændelser undergraver borgernes og virksomhedernes tillid til det digitale samfund. Tyveri af forretningshemmeligheder, forretningsoplysninger og personoplysninger, forstyrrelse af tjenester, herunder vigtige tjenester, og infrastrukturer medfører økonomiske tab på flere hundrede milliarder euro hvert år[1]. De kan også have konsekvenser for borgernes grundlæggende rettigheder og for samfundet som helhed.

Den Europæiske Unions strategi for cybersikkerhed fra 2013[2] (EU-strategien for cybersikkerhed) og dens vigtigste resultat, nemlig direktivet om net- og informationssikkerhed (NIS-direktivet)[3], der snart vil blive vedtaget, samt direktiv 2013/40/EU om angreb på informationssystemer udgør indtil videre Den Europæiske Unions vigtigste politiske reaktion på disse cybersikkerhedsudfordringer. Derudover råder EU også over specialiserede enheder såsom Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA), Det Europæiske Center til Bekæmpelse af IT-Kriminalitet (EC3) ved Europol og IT-beredskabsenheden (CERT-EU). Der er for nylig også blevet iværksat en række sektorspecifikke initiativer (f.eks. på energi- og transportområdet) med henblik på at øge cybersikkerheden i forskellige kritiske sektorer.

Til trods for disse positive resultater er EU fortsat sårbar over for cyberhændelser. Dette kunne undergrave det digitale indre marked og det økonomiske og sociale liv som helhed. Deres virkninger kan også have konsekvenser for andet end økonomien. I tilfælde af hybride trusler[4] kan anvendelsen af cyberangreb også koordineres med andre aktiviteter til at destabilisere et land eller udfordre de politiske institutioner.

På den baggrund kunne håndteringen af en omfattende cyberhændelse, der involverer flere medlemsstater samtidigt, udgøre en stor udfordring for EU. I synergi med meddelelsen om bekæmpelse af hybride trusler samt meddelelsen om gennemførelse af den europæiske dagsorden om sikkerhed[5] undersøger Kommissionen, hvordan man kan tackle den nye virkelighed på cybersikkerhedsområdet og vurdere de yderligere foranstaltninger, der kan være nødvendige for at forbedre EU's modstandsdygtighed over for cyberangreb og beredskabet i forbindelse med sådanne hændelser.

Derudover tager Kommissionen også fat på de industrielle kapaciteter på cybersikkerhedsområdet i EU. Selv om hele værdikæden af digitale teknologier ikke beherskes fuld ud i Europa, er der behov for i det mindste at bevare og udvikle visse væsentlige kapaciteter. Levering af produkter og tjenester, der sikrer det højeste niveau for cybersikkerhed, rummer muligheder for cybersikkerhedsindustrien i Europa og kunne give en

[1] *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II; Center for Strategic and International Studies; June 2014* (Nettotab: Vurdering af de samlede omkostninger ved cyberkriminalitet. Den økonomiske virkning af cyberkriminalitet II. Centret for strategiske og internationale studier, juni 2014).
[2] JOIN(2013) 1.
[3] COM(2013) 48.
[4] JOIN(2016) 18.
[5] COM(2016) 230.

stærk konkurrencefordel. Det globale marked for cybersikkerhed forventes at blive blandt de hurtigst voksende segmenter i IKT-sektoren[6]. Forudsætningen for, at EU kan blive en førende aktør på dette område, er en stærk tradition for datasikkerhed, herunder i forbindelse med personoplysninger, og et effektivt beredskab i forbindelse med hændelser. Dette vil blive set som et stærkt argument for at investere i EU og dermed bidrage til at nå de ambitiøse mål for det digitale indre marked om skabelse af vækst og beskæftigelse.

Der er behov for et stærkt engagement for at opnå ovennævnte, navnlig gennem:

i) Styrkelse af samarbejdet om forbedring af beredskabet og håndtering af cyberhændelser

De eksisterende og aftalte samarbejdsmekanismer skal styrkes for at øge EU's modstandsdygtighed og beredskab, herunder med henblik på en eventuel paneuropæisk cybersikkerhedskrise. Disse samarbejdsmekanismer bør være omfattende og dække hele en hændelses livscyklus fra forberedelse til retsforfølgning. Et effektivt samarbejde mellem medlemsstaterne og praktisk gennemførelse af sikkerhedskrav for kritiske operatører vil også kræve robuste tekniske løsninger fra cyberindustriens side.

Samtidig vil sikring af kritiske cyberaktivers modstandsdygtighed i hele EU kræve løbende bestræbelser på at finde synergier på tværs af sektorer og integrere cybersikkerhedskrav i alle relevante EU-politikker. Kommissionen vil overveje behovet for at opdatere EU's cybersikkerhedsstrategi fra 2013 i den nærmeste fremtid.

ii) Tackling af de udfordringer, som Europas indre marked for cybersikkerhed står over for

Det anerkendes i strategien for et digitalt indre marked[7], at der fortsat er specifikke mangler i teknologierne og løsningerne i relation til onlinenetværkssikkerhed, der er et område i hastig udvikling. Samtidig viser markedsundersøgelser, at EU's indre marked stadig er geografisk fragmenteret for så vidt angår cybersikkerhedsprodukter og -tjenester[8]. I denne meddelelse redegøres der for en række markedsorienterede politiske foranstaltninger med henblik på at afhjælpe disse mangler og udfordringer i det indre marked.

iii) Udvikling af industrielle kapaciteter på cybersikkerhedsområdet

Kommissionen har i forbindelse med både EU's cybersikkerhedsstrategi og strategien for et digitalt indre marked givet tilsagn om at fremme levering af produkter og tjenester fra EU's cybersikkerhedsindustri. Derfor er Kommissionen også i færd med at vedtage en afgørelse, der skal bane vej for en aftale om offentligt-private partnerskaber (OPP'er) om cybersikkerhed, som vil søge at fremme en europæisk dagsorden for avanceret forskning og innovation på cybersikkerhedsområdet med henblik på at forbedre konkurrenceevnen.

[6] Se SWD(2016) 216.
[7] COM(2015) 192.
[8] Se SWD(2016) 216.

2. VIDEREUDVIKLING AF SAMARBEJDE, VIDEN OG KAPACITET

EU's cybersikkerhedsstrategi og navnlig det kommende NIS-direktiv[9] vil bane vej for et forbedret samarbejdet på EU-plan mellem medlemsstaterne. Den hurtige og effektive gennemførelse af direktivet vil være afgørende for udbygningen af digitaliseringen af det økonomiske og sociale liv (også under hensyntagen til cloud computing, tingenes internet og kommunikation mellem maskiner), den stigende sammenkobling på tværs af grænserne og det cybertrusselsbillede, der er i hastig udvikling[10]. I den forbindelse skal EU forberede sig på muligheden for en omfattende cyberkrise[11], herunder f.eks. store samtidige angreb på kritiske informationssystemer i flere medlemsstater[12].

Samarbejdet på EU-plan er derfor vigtigt for håndteringen af både cyberhændelser i mindre målestok, som kan brede sig, og et mulig omfattende cyberangreb i flere medlemsstater. EU skal integrere cyberaspekterne i de eksisterende krisestyringsmekanismer. Det skal også sikre et effektivt samarbejde og hurtige mekanismer til udveksling af oplysninger mellem sektorer og medlemsstater for at reagere på og inddæmme sådanne hændelser. Disse mekanismer bør endvidere fungere i sammenhæng og dermed bidrage til bekæmpelsen af terrorisme, organiseret kriminalitet og cyberkriminalitet. Dette ville også forbedre EU's mulighed for at koordinere sin indsats med sine internationale partnere med hensyn til effektivt at reagere på globale trusler og hændelser.

2.1. Størst mulig udnyttelse af NIS-samarbejdsmekanismerne og udviklingen hen imod ENISA 2.0

En væsentlig del af de nationale kapaciteter, der kræves i NIS-direktivet, er de enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er), som er ansvarlige for hurtig reaktion mod cybertrusler og cyberhændelser. De vil indgå i CSIRT-nettet med henblik på at fremme et effektivt operationelt samarbejde om specifikke cybersikkerhedshændelser og dele oplysninger om risici. Med direktivet vil der endvidere blive oprettet en samarbejdsgruppe for at støtte og lette det strategiske samarbejde mellem medlemsstaterne og opbygge tillid mellem dem.

På grund af cybertruslernes karakter og mangfoldighed opfordrer Kommissionen medlemsstaterne til at få mest muligt ud af NIS-samarbejdsmekanismerne og forbedre det grænseoverskridende samarbejde om beredskabet med hensyn til en omfattende cyberhændelse. Et sådant yderligere samarbejde med henblik på en større cyberhændelse ville drage fordel af en koordineret tilgang til krisesamarbejdet på tværs af de forskellige elementer i cyberøkosystemet. En sådan tilgang kan uddybes i en "model", der også bør sikre synergier og sammenhæng med eksisterende krisestyringsmekanismer[13]. Den bør så regelmæssigt testes ved cyber- og andre krisestyringsøvelser. Den ville omfatte en rolle for organer på EU-plan

[9] NIS-direktivet vil kræve, at medlemsstaterne identificerer en række operatører, der udbyder vigtige tjenester på områder som energi, transport, finansielle tjenesteydelser og sundhed, med henblik på at tackle cybersikkerhedsrisici og sikre, at visse udbydere af digitale tjenester træffer passende foranstaltninger til tackling af sådanne risici.

[10] Se SWD(2016) 216.

[11] Se f.eks. ENISA-rapporten: Common practices of EU-level crisis management and applicability to cyber crises (April 2016) (Fælles praksis for krisestyring på EU-plan og dens anvendelse på cyberkriser (april 2016)).

[12] Se SWD(2016) 216.

[13] Navnlig de integrerede ordninger for politisk kriserespons, herunder afgørelsen om ordninger for EU's gennemførelse af solidaritetsbestemmelsen (24. juli 2014) og beslutningsprocessen vedrørende den fælles sikkerheds- og forsvarspolitik.

såsom ENISA, CERT-EU og det europæiske center for IT-kriminalitet (EC3) ved Europol samt benytte de værktøjer, der er udviklet inden for rammerne af CSIRT-nettet. Kommissionen vil i første halvdel af 2017 fremlægge en sådan samarbejdsmodel for samarbejdsgruppen, CSIRT-nettet og andre relevante aktører med henblik på nærmere overvejelse.

EU råder på nuværende tidspunkt over viden og ekspertise, men på en spredt og ustruktureret måde. For at støtte NIS-samarbejdsmekanismerne bør oplysningerne samles i et "informationsknudepunkt", for at de nemmere kan stilles til rådighed for alle medlemsstater efter anmodning. Dette "knudepunkt" vil være en central ressource, som gør det muligt for EU-institutionerne og medlemsstaterne at udveksle oplysninger, når det er relevant. Lettere adgang til bedre strukturerede oplysninger om cybersikkerhedsrisici og potentielle måder at afhjælpe dem på bør hjælpe medlemsstaterne med at øge deres kapaciteter og tilpasse deres praksis og dermed forbedre den samlede modstandsdygtighed over for angreb. Kommissionen vil med støtte fra ENISA, CERT-EU og med Det Fælles Forskningscenters ekspertise lette oprettelsen af og sikre knudepunktets bæredygtighed.

Endvidere bør der på EU-plan oprettes en rådgivende gruppe på højt plan[14] vedrørende cybersikkerhed bestående af eksperter og beslutningstagere fra industrien, den akademiske verden, civilsamfundet og andre relevante organisationer, som skal holde møder regelmæssigt. Gruppen ville gøre det muligt for Kommissionen på en åben og gennemsigtig måde at opnå ekstern ekspertise og input vedrørende sine politikker med hensyn til cybersikkerhedsstrategier og potentielle lovgivningsmæssige eller andre offentlige politiske tiltag. Den vil supplere og interagere med andre strukturer, der beskæftiger sig med cybersikkerhed[15].

Kommissionen skal endvidere foretage en evaluering af ENISA senest den 20. juni 2018, og den eventulle ændring eller fornyelse af ENISA's mandat skal være vedtaget senest den 19. juni 2020[16]. I betragtning af det nuværende cybersikkerhedslandskab sigter Kommissionen mod at fremskynde evalueringen og med forbehold af resultaterne heraf fremlægge et forslag snarest muligt.

Ved vurderingen af det mulige behov for at ændre ENISA's mandat vil Kommissionen tage hensyn til de cybersikkerhedsmæssige udfordringer, der er beskrevet ovenfor, og de generelle bestræbelser på at styrke samarbejde og vidensdeling. Denne proces vil være en anledning til at se nærmere på den mulige forbedring af agenturets kapaciteter og muligheder for på bæredygtig vis at støtte medlemsstaterne i deres bestræbelser på at opnå modstandsdygtighed over for cyberangreb. Ved overvejelserne om ENISA's mandat skal der endvidere tages hensyn til agenturets nye ansvarsområder inden for rammerne af NIS-direktivet, nye politiske målsætninger om støtte til cybersikkerhedsindustrien (strategien for et digitalt indre marked og det kontraktlige OPP), udviklingen i behovene for sikring af kritiske sektorer og nye

[14] Kommissionens ekspertgrupper er underlagt de horisontale regler i Kommissionens afgørelse C(2016) 3301.
[15] F.eks. platformen for net- og informationssikkerhed, det kontraktlige OPP om cybersikkerhed og sektorplatforme såsom cybersikkerhedsplatformen af energieksperter. Den bør også stå i forbindelse med den rundbordskonference på højt plan, der er bebudet i meddelelsen om digitalisering af EU's industri: COM(2016) 180.
[16] Forordning (EU) nr. 526/2013 om ophævelse af forordning (EF) nr. 460/2004.

udfordringer i relation til grænseoverskridende hændelser, herunder en koordineret reaktion på cyberkriser.

Kommissionen vil:

- foreslå en samarbejdsmodel for tackling af omfattende cyberhændelser på EU-plan i første halvdel af 2017
- fremme etableringen af et "informationsknudepunkt" for at støtte udvekslingen af oplysninger mellem EU-organer og medlemsstater
- oprette en rådgivende gruppe på højt plan vedrørende cybersikkerhed og
- afslutte evalueringen af ENISA inden udgangen af 2017. Ved en sådan evaluering vil der blive taget fat på behovet for at ændre eller udvide ENISA's mandat med henblik på at fremlægge et eventuelt forslag snarest muligt.

2.2. Øget indsats inden for uddannelse, træning og øvelser i cybersikkerhed

Tilstrækkelige færdigheder og tilstrækkelig træning i relation til både forebyggelse af cybersikkerhedshændelser og håndtering og afbødning af deres virkninger er nogle af de vigtigste aspekter ved opnåelsen af modstandsdygtighed over for cyberangreb.

På nuværende tidspunkt spiller ENISA, Den Europæiske Uddannelsesgruppe vedrørende Cyberkriminalitet (ECTEG) i samarbejde med det europæiske center for IT-kriminalitet ved Europol og Det Europæiske Politiakademi (Cepol) alle en vigtig rolle gennem ydelse af støtte til kapacitetsopbygning – bl.a. inden for cyberkriminalteknik – ved at udvikle manualer og tilrettelægge træning og øvelser i cybersikkerhed.

Samtidig er cyberspace et område i hastig udvikling, hvor mulighederne for dobbelt anvendelse spiller en vigtig rolle. Det er derfor nødvendigt at udvikle samarbejde og synergier mellem det civile og det militære område med hensyn til træning og øvelser for at øge EU's modstandsdygtighed og muligheder for at reagere på hændelser.

For at imødekomme dette behov og som opfølgning på vedtagelsen af NIS-direktivet og rammen for EU's cyberforsvarspolitik[17] vil Kommissionens tjenestegrene samarbejde med medlemsstaterne, EU-Udenrigstjenesten, ENISA og andre relevante EU-organer[18] om etablering af en platform for uddannelse, øvelser og træning i cybersikkerhed, der skal fremme synergier mellem civil og forsvarsmæssig træning.

Kommissionen vil:

- arbejde tæt sammen med medlemsstaterne, ENISA, EU-Udenrigstjenesten og andre EU-organer om etableringen af en træningsplatform for cybersikkerhed.

[17] Vedtaget af Den Europæiske Unions Udenrigsråd den 18. november 2014, dok. 15585/14.
[18] Såsom Det Europæiske Sikkerheds- og Forsvarsakademi, EC3, Cepol og Det Europæiske Forsvarsagentur (EDA).

2.3. Håndtering af indbyrdes afhængighed mellem forskellige sektorer og vigtige offentlige netinfrastrukturers modstandsdygtighed

En vigtig faktor ved vurderingen af risikoen i forbindelse med og virkningen af en omfattende cyberhændelse er graden af grænseoverskridende og tværsektoriel indbyrdes afhængighed. En alvorlig cyberhændelse i én sektor eller i én medlemsstat kan direkte eller indirekte indvirke på – eller brede sig til – andre sektorer eller til andre medlemsstater.

Grænseoverskridende og tværsektorielt samarbejde letter udvekslingen af oplysninger og ekspertise og øger dermed beredskabet og modstandsdygtigheden. Kommissionen har støttet arbejdet i forskellige sektorer for bedre at forstå den indbyrdes afhængighed gennem vedtagelse af det europæiske program for beskyttelse af kritisk infrastruktur[19].

Samtidig er det en nødvendig forudsætning for håndteringen af tværsektorielle risici, at den enkelte sektor er i stand til at identificere, træffe beredskabsforanstaltninger og reagere på cyberhændelser. Kommissionen vil vurdere den risiko, der følger af cyberhændelser i stærkt forbundne sektorer inden for og på tværs af de nationale grænser, navnlig i de sektorer, der er omfattet af NIS-direktivet, også under hensyntagen til udviklingen på nationalt plan[20]. Efter denne vurdering vil Kommissionen overveje, om der er behov for yderligere specifikke regler og/eller vejledning om cyberrisikoberedskabet for sådanne kritiske sektorer.

På europæisk plan kan sektoropdelte informationsudvekslings- og analysecentre[21] og de tilsvarende CSIRT'er spille en vigtig rolle for beredskabet i forbindelse med og reaktionen på cyberhændelser. For at sikre en effektiv informationsstrøm om trusler i konstant udvikling og lette reaktionen på cyberhændelser bør informationsudvekslings- og analysecentrene tilskyndes til at samarbejde med CSIRT-nettet under NIS-direktivet og det europæiske center for IT-kriminalitet ved Europol, CERT-EU samt med de relevante retshåndhævende myndigheder.

Informationsudvekslingen mellem interessenter og med myndigheder i hele cyberrisicienes livscyklus kræver, at deltagerne har tillid til, at det ikke indebærer, at de ifalder ansvar. Kommissionen har bemærket en række sådanne bekymringer, der forhindrer virksomhederne i at dele værdifulde trusselsefterretninger med deres ligestillede på tværs af sektorer eller med myndigheder, navnlig i en grænseoverskridende sammenhæng. Kommissionen vil bestræbe sig på at tage fat på og dæmpe sådanne bekymringer af hensyn til en forbedret udveksling af oplysninger om cybertrusler.

Sikre rapporteringskanaler, der garanterer fortrolighed, er også afgørende for, at man kan tilskynde virksomhederne til at indberette cybertyveri af forretningshemmeligheder. Dette ville gøre det muligt at overvåge og vurdere skaderne for europæisk industri (med tab af salg og arbejdspladser til følge) og forskningsorganer. Dette ville også bidrage til udformningen af en afstemt politisk reaktion. Med støtte fra ENISA vil Den Europæiske Unions Kontor for Intellektuel Ejendomsret (EUIPO) og EC3 ved Europol vil Kommissionen – i dialog med

[19] SWD(2013) 318.
[20] F.eks. den køreplan for cybersikkerhed, der blev vedtaget af Det Europæiske Luftfartssikkerhedsagentur, og arbejdet i Organisationen for International Civil Luftfart og Den Internationale Søfartsorganisation.
[21] Se f.eks. det europæiske informationsudvekslings- og analysecenter på energiområdet (http://www.ee-isac.eu).

private interessenter – oprette sikre kanaler for frivillig indberetning af cybertyveri af forretningshemmeligheder. Dette burde også gøre det muligt at indsamle anonymiserede og aggregerede data på EU-plan. Disse data kan deles med medlemsstaterne som grundlag for diplomatiske bestræbelser og oplysningskampagner for at bidrage til at beskytte EU's immaterielle aktiver mod cyberangreb.

For at støtte cybersikkerheden i de enkelte sektorer vil Kommissionen også bidrage til at gøre cybersikkerhed til en fast bestanddel af udviklingen af forskellige EU-sektorpolitikker med en cybersikkerhedsdimension.

Sidst, men ikke mindst, spiller de offentlige myndigheder en rolle med hensyn til at kontrollere integriteten af vigtige internetinfrastrukturer med henblik på at opdage problemer, underrette den part, der er ansvarlig for disse net, og – når der er behov for det – yde bistand med at afhjælpe kendte sårbarheder. De nationale tilsynsmyndigheder kunne anvende CSIRT'ernes kapaciteter til at udføre regelmæssige skanninger af offentlige netinfrastrukturer. På grundlag heraf kunne de tilskynde aktørerne til at afhjælpe de mangler eller tage fat på de sårbarheder, som sådanne skanninger måtte afsløre.

Kommissionen vil derfor undersøge de nødvendige retlige og organisatoriske betingelser for, at de nationale tilsynsmyndigheder – i samarbejde med de nationale cybersikkerhedsmyndigheder – kan anmode CSIRT'erne om at udføre regelmæssige sårbarhedstjek af offentlige netinfrastrukturer. De nationale CSIRT'er bør opfordres til at samarbejde inden for CSIRT-nettet om bedste praksis ved overvågning af netværk og således lette forebyggelsen af omfattende hændelser.

Kommissionen vil:

- fremme udviklingen af europæisk samarbejde mellem sektoropdelte informationsudvekslings- og analysecentre, støtte deres samarbejde med CSIRT'er og søge at tackle de barrierer, der kan forhindre markedsdeltagerne i at udveksle oplysninger
- undersøge den strategiske/systemiske risiko som følge af cyberhændelser i stærkt indbyrdes afhængige sektorer inden for og på tværs af nationale grænser
- vurdere behovet for og eventuelt overveje supplerende regler og/eller vejledning om cyberrisikoberedskabet for kritiske sektorer
- i samarbejde med ENISA, EUIPO og EC3 oprette sikre kanaler for frivillig indberetning af cybertrusler mod forretningshemmeligheder
- arbejde for at gøre cybersikkerhedsforanstaltninger til en fast bestanddel af europæiske sektorpolitikker og
- undersøge de nødvendige betingelser for, at de nationale myndigheder kan anmode CSIRT'erne om at udføre regelmæssige tjek af vigtige netinfrastrukturer.

3. IMØDEGÅELSE AF DE UDFORDRINGER, SOM EUROPAS INDRE MARKED FOR CYBERSIKKERHED STÅR OVER FOR

Europa har behov for interoperable og økonomisk overkommelige cybersikkerhedsprodukter og løsninger af høj kvalitet. Udbuddet af IKT-sikkerhedsprodukter og -tjenester i det indre marked er fortsat meget fragmenteret rent geografisk. På den ene side gør det det vanskeligt for de europæiske virksomheder at konkurrere på nationalt, europæisk og globalt plan, og på den anden side mindsker det udvalget af levedygtige og brugbare cybersikkerhedsteknologier, som borgere og virksomheder har adgang til[22].

Cybersikkerhedsindustrien i Europa har hovedsagelig udviklet sig med afsæt i den nationale statslige efterspørgsel, herunder til forsvarssektoren. De fleste europæiske forsvarsleverandører har udviklet cybersikkerhedsafdelinger[23]. Sideløbende hermed er der også dukket et væld af innovative SMV'er op både på specialiserede markeder/nichemarkeder (f.eks. krypteringssystemer) og på veletablerede markeder med nye forretningsmodeller (f.eks. antivirussoftware).

Virksomhederne har dog vanskeligt ved at vokse uden for deres indenlandske, nationale marked. Manglen på tillid til løsninger, der tilbydes "på tværs af grænserne", er den væsentlige faktor, der klart fremgik af alle de høringer, som Kommissionen har gennemført[24]. Som følge heraf finder mange udbud fortsat sted i en given medlemsstat, og mange virksomheder kæmper for at opnå stordriftsfordele, der ville sætte dem i stand til at blive mere konkurrencedygtige både i det indre marked og globalt.

Manglen på interoperable løsninger (tekniske standarder), praksisser (processtandarder) og velfungerende certificeringsmekanismer på EU-plan er blandt de andre mangler, der påvirker det indre marked for cybersikkerhed. I den forbindelse blev cybersikkerhed identificeret som en af IKT-standardiseringsprioriteterne for det digitale indre marked[25].

De begrænsede vækstudsigter for cybersikkerhedsvirksomheder i det indre marked fører til talrige fusioner og opkøb fra ikkeeuropæiske investorers side[26]. Denne tendens afspejler de europæiske iværksætteres innovationskapacitet på cybersikkerhedsområdet, men den kan også føre til tab af europæisk knowhow og ekspertise samt hjerneflugt.

Der er behov for en hurtig indsats for at fremme et mere integreret indre marked for cybersikkerhedsprodukter og -tjenester, der vil lette udbredelsen af mere praktiske og økonomisk overkommelige løsninger.

Hindringer for tillid mellem europæiske industrielle og institutionelle aktører kan overvindes ved at fremme samarbejdet på et tidligt stadium af innovationslivscyklussen, nemlig inden for cybersikkerhedsindustrien selv, mellem leverandører og købere og i en tværsektoriel dimension, der involverer industrier, som allerede er eller forventes at blive kunder til cybersikkerhedsløsninger.

[22] Se SWD(2016) 216.
[23] Se SWD(2016) 216.
[24] Se SWD(2016) 215.
[25] COM(2016) 176/2.
[26] Se SWD(2016) 216.

Samtidig får udviklingen af produkter, tjenester og teknologier med dobbelt anvendelse stigende betydning i Europa. Et stigende antal løsninger overgår fra det civile marked til forsvarsmarkedet[27]. Det er Kommissionens hensigt, at den i den kommende europæiske forsvarshandlingsplan vil identificere foranstaltninger med henblik på at sætte yderligere gang i civil-militære synergier på europæisk plan.

3.1. Certificering og mærkning

Certificering spiller en vigtig rolle for styrkelsen af tilliden til og sikkerheden ved produkter og tjenester. Dette gælder også for nye systemer, der i vidt omfang benytter digitale teknologier, og som kræver høj sikkerhed, såsom forbundne og automatiske biler, e-sundhedssystemer, industrielle automationsstyringssystemer eller intelligente net.

Man er ved at udvikle nationale initiativer til fastsættelse af cybersikkerhedskrav på højt plan til IKT-komponenter i traditionelle infrastrukturer, herunder certificeringskrav. Uanset hvor vigtige disse er, indebærer de en risiko for, at markedet fragmenteres, og at der opstår interoperabilitetsproblemer. Kun i nogle få medlemsstater findes der effektive sikkerhedscertificeringsordninger for IKT-produkter[28]. Det kan være nødvendigt for en IKT-sælger at underkaste sig flere certificeringsprocesser for at sælge i flere medlemsstater. I værste fald kan et IKT-produkt eller en IKT-tjeneste, der er udviklet til at opfylde cybersikkerhedskravene i én medlemsstat, ikke markedsføres i en anden.

For at opnå et velfungerende indre marked for cybersikkerhed bør en mulig ramme for cybersikkerhedscertificering af IKT-produkter og -tjenester søge at nå følgende mål: i) dække en bred vifte af IKT-systemer, -produkter og -tjenester, ii) sikre anvendelse på alle 28 medlemsstater og iii) vedrøre ethvert cybersikkerhedsniveau under hensyntagen til udviklingen på internationalt plan.

Kommissionen vil med henblik herpå nedsætte en særlig arbejdsgruppe vedrørende sikkerhedscertificering af IKT-produkter og -tjenester bestående af eksperter fra medlemsstaterne og industrien. Dens formål vil være – i samarbejde med ENISA og Det Fælles Forskningscenter – inden udgangen af 2016 at fastlægge en køreplan for undersøgelse af muligheden for at udarbejde et forslag til en sådan europæisk IKT-sikkerhedscertificeringsramme, der skal forelægges inden udgangen af 2017. Kommissionen vil i den forbindelse også tage hensyn til forordning 2008/765 og de certificeringsbestemmelser, der er indeholdt i den generelle forordning om databeskyttelse (2016/679)[29].

Processen vil omfatte en bred høring og konsekvensanalyse. Dette vil sætte Kommissionen i stand til at undersøge forskellige muligheder for skabelse af certificeringsrammen for IKT-produkter og -tjenester. Kommissionen vil også undersøge IKT-sikkerhedscertificering i

[27] I 2013 udgjorde eksporten af varer og tjenester med dobbelt anvendelse allerede 20 % af EU's samlede eksport (målt i værdi). Dette tal inkluderer handel inden for EU.

[28] Se SWD(2016) 216 til godkendelse i gruppen af højtstående embedsmænd vedrørende informationssystemer (Rådets afgørelse af 31. marts 1992 (92/242/EØF) og andre eksisterende ordninger, f.eks. Commercial Product Assurance i Det Forenede Kongerige og Certification Sécuritaire de Premier Niveau i Frankrig.

[29] I henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger skal der både indføres adfærdskodekser, der skal bidrage til den korrekte anvendelse af databeskyttelsesreglerne, samt certificeringsmekanismer, der omfatter alle beskyttelsesprincipper, herunder navnlig datasikkerhed i forbindelse med behandlingen af personoplysninger.

infrastruktursektorer (f.eks. inden for luftfart, jernbaner, bilindustrien) og i specifikke certificerings- og valideringsmekanismer for ibrugtagningsklar teknologi (f.eks. cybersikkerhed i forbindelse med automationsstyringssystemer[30], tingenes internet, cloud computing). Den vil også afhjælpe identificerede mangler i ovennævnte europæiske ordning for IKT-sikkerhedscertificering.

Certificeringsbestræbelserne vil så vidt muligt bygge på internationalt anerkendte standarder og blive udviklet i samarbejde med internationale partnere.

Kommissionen vil også undersøge, hvordan man bedst kan integrere IKT-sikkerhedscertificering i fremtidig sektorspecifik lovgivning, også i relation til sikkerhedsaspekterne.

Ud over eventuelle reguleringsmæssige modeller vil Kommissionen også undersøge muligheden for at oprette en europæisk, kommercielt orienteret, frivillig og enkel mærkningsordning vedrørende IKT-produkters sikkerhed. Som supplement til certificering vil den søge at forbedre læsbarheden af cybersikkerhedsmærkningen af kommercielle produkter for at gøre dem mere konkurrencedygtige i det indre marked og globalt. Der vil blive taget behørigt hensyn til igangværende sektorielle og horisontale initiativer, der er iværksat af industrien, både fra udbuds- og efterspørgselssiden.

De offentlige myndigheder vil blive tæt involveret for at gøre det muligt at anvende fælles specifikationer og henvise til certificering i offentlige udbud. Kommissionen vil også overvåge og rapportere om anvendelsen af relevante certificeringskrav i forbindelse med offentlige udbud på nationalt plan, navnlig for så vidt angår sektorspecifikke systemer (energi, transport, sundhed, offentlig administration osv.).

Kommissionen vil:

- inden udgangen af 2016 fastlægge en køreplan for udarbejdelsen af et muligt forslag til en europæisk IKT-sikkerhedscertificeringsramme, der skal forelægges inden udgangen af 2017, og vurdere gennemførligheden og virkningen af en enkel mærkningsordning vedrørende cybersikkerhed
- undersøge og, hvis det er hensigtsmæssigt, tage fat på mangler i IKT-certificeringen inden for de eksisterende sektorspecifikke certificerings-/valideringsmekanismer
- hvor det er hensigtsmæssigt, medtage integrering af sikkerhedscertificering af IKT-produkter i fremtidig sektorspecifik EU-lovgivning
- fremme inddragelsen af de offentlige myndigheder for at lette anvendelsen af certificering og fælles specifikationer i forbindelse med offentlige udbud
- overvåge anvendelsen af relevante certificeringskrav i forbindelse med offentlige og erhvervsmæssige udbudsprocedurer og rapportere om markedssituationen om tre år.

[30] Se ERNCIP's tematiske gruppe om cybersikkerhed i forbindelse med industrielle styringssystemer, tilgængelig påhttps://erncip-project.jrc.ec.europa.eu/download-area/category/16-case-studies-for-industrial-automation-and-control-systems

3.2. Øgede investeringer i cybersikkerhed i Europa og støtte til SMV'er

Selv om der er stærk vækst i innovation i cybersikkerhedssektoren i Europa, har EU fortsat ikke tilstrækkelig tradition for investering i cybersikkerhed. Der er mange innovative SMV'er på dette område, men de er ofte ikke i stand til at øge deres aktiviteter. Dette skyldes bl.a. mangel på lettilgængelig finansiering til at støtte dem i de tidlige udviklingsfaser. Virksomhederne har også begrænset adgang til venturekapital i Europa, og deres markedsføringsbudget til forbedring af deres synlighed eller håndtering af forskellige sæt standardiserings- og overholdelseskrav er utilstrækkeligt.

Samtidig er samarbejdet mellem aktørerne på cybersikkerhedsområdet ret mangelfuldt, og der er behov for yderligere bestræbelser på at øge den økonomiske koncentration og udvikle nye værdikæder[31].

For at øge investeringerne i cybersikkerhed i Europa og støtte SMV'erne er det nødvendigt at lette adgangen til finansiering. Der skal også være støtte til udviklingen af cybersikkerhedsklynger og ekspertisecentre, der er konkurrencedygtige på globalt plan, i regionale økosystemer, der er fremmende for digital vækst. Denne støtte skal være kædet sammen med gennemførelsen af intelligente specialiseringsstrategier og andre EU-instrumenter, sådan at cybersikkerhedsindustrien i Europa kan få større fordel af dem.

Kommissionens tilgang vil gå ud på at maksimere bevidstheden i cybersikkerhedsmiljøet om finansieringsmulighederne på europæisk, nationalt og regionalt plan (i relation til både horisontale instrumenter og specifikke indkaldelser[32]) ved at anvende eksisterende instrumenter og kanaler som f.eks. Enterprise Europe-netværket.

Kommissionen vil supplere disse bestræbelser ved sammen med Den Europæiske Investeringsbank (EIB) og Den Europæiske Investeringsfond (EIF) at undersøge, hvordan man kan lette adgangen til finansiering. Dette kan være i form af egenkapital- samt kvasiegenkapitalinvesteringer, lån og garantier til projekter eller modgarantier til formidlere, f.eks. gennem oprettelse af en platform for investering i cybersikkerhed under Den Europæiske Fond for Strategiske Investeringer[33].

Derudover vil Kommissionen også se på mulighederne for sammen de interesserede medlemsstater og regioner at udvikle en intelligent specialiseringsplatform for cybersikkerhed[34]. Dette ville bidrage til at koordinere og planlægge cybersikkerhedsstrategier og oprette et strategisk samarbejde mellem interesserede parter inden for regionale økosystemer. Denne fremgangsmåde bør også bidrage til at udnytte de eksisterende europæiske struktur- og investeringsfondes potentiale til gavn for cybersikkerhedssektoren.

Mere generelt vil Kommissionen fremme metoden med indbygget sikkerhed. Den vil bestræbe sig på at sikre, at kravene til cybersikkerhed konsekvent tages op i forbindelse med

[31] Se SWD(2016) 216.

[32] Se f.eks. indkaldelsen af forslag i 2016, der omfatter flere sektorer, under programmet for Connecting Europe-faciliteten, og indkaldelser under Cosme 2016 vedrørende programmet for internationalisering af klynger.

[33] Inden for rammerne af Den Europæiske Fond for Strategiske Investeringer kan der ydes støtte til individuelle projekter enten direkte eller indirekte gennem investeringsplatforme. Sådanne platforme kan bidrage til at finansiere mindre projekter og samle midler fra forskellige kilder for at muliggøre forskelligartede investeringer med et geografisk eller tematisk fokus.

[34] Se intelligente specialiseringsinstrumenter (RIS3): http://s3platform.jrc.ec.europa.eu/

alle større infrastrukturinvesteringer med en digital komponent, der medfinansieres af de europæiske fonde. Den vil gøre dette ved gradvist at indføre relevante krav i reglerne for offentlige udbud og programmer.

Kommissionen vil:

- anvende eksisterende SMV-støtteværktøjer til at øge opmærksomheden omkring eksisterende finansieringsmekanismer i cybersikkerhedsmiljøet
- yderligere øge anvendelsen af EU-værktøjer og -instrumenter for at støtte innovative SMV'er, således at de kan undersøge synergier mellem civile og militære cybersikkerhedsmarkeder[35]
- sammen med EIB og EIF undersøge muligheden for at lette adgangen til investeringer, f.eks. gennem en specialiseret platform for investering i cybersikkerhed eller andre værktøjer
- udvikle en platform intelligent specialisering vedrørende cybersikkerhed for at hjælpe medlemsstater og regioner, der er interesserede i at investere i cybersikkerhedssektoren (RIS3), og
- fremme metoden med indbygget sikkerhed i forbindelse med større infrastrukturinvesteringer med en digital komponent, der medfinansieres af EU-fonde.

4. FREMME OG UDVIKLING AF DEN EUROPÆISKE CYBERSIKKERHEDSINDUSTRI GENNEM INNOVATION – ETABLERING AF DET KONTRAKTLIGE OPP OM CYBERSIKKERHED

For at fremme den europæiske cybersikkerhedsindustris konkurrenceevne og innovation vil der blive indgået et kontraktligt offentligt-privat partnerskab (OPP) om cybersikkerhed. Det kontraktlige OPP vil samle industrielle og offentlige ressourcer med henblik på at tilvejebringe ekspertise inden for forskning og innovation.

Det kontraktlige OPP har til formål at opbygge tillid blandt medlemsstaterne og de industrielle aktører ved at fremme samarbejdet på de tidlige stadier af forsknings- og innovationsprocessen. Det har også til formål at skabe overensstemmelse mellem efterspørgsels- og udbudssektorerne. Dette burde gøre det muligt for industrien at opnå fremtidige krav fra slutbrugere og sektorer, der er vigtige kunder til cybersikkerhedsløsninger (f.eks. energi-, sundheds-, transport- og finanssektoren). Det vil gøre det lettere for dem at deltage i fastsættelsen af fælles krav vedrørende digital sikkerhed, beskyttelse af privatlivets fred og databeskyttelse for deres sektorer.

Det kontraktlige OPP om cybersikkerhed vil også bidrage til at maksimere anvendelsen af disponible midler. Dette vil først og fremmest ske gennem stærkere koordinering med medlemsstaterne. For det andet vil der være et større fokus på nogle få tekniske prioriteter for

[35] F.eks. vil Entreprise Europe-netværket og det europæiske netværk af forsvarsrelaterede regioner åbne nye muligheder for regionerne for at udforske det grænseoverskridende samarbejde inden for dobbelt anvendelse, herunder cybersikkerhed, og for SMV'er for at indlede partnersøgningsaktiviteter.

at hjælpe cybersikkerhedsindustrien med at opnå tekniske gennembrud og beherske fremtidige cybersikkerhedsteknologier. I den forbindelse kan udviklingen af open source-software og åbne standarder bidrage til at fremme tillid, gennemsigtighed samt disruptiv innovation og bør derfor også indgå i de investeringer, der foretages som led i dette kontraktlige OPP.

Det arbejde, der udføres inden for rammerne af det kontraktlige OPP om cybersikkerhed, vil også nyde godt af synergier med andre europæiske projekter, navnlig når disse vedrører sikkerhedsaspekter. Disse omfatter fabrikker for fremtiden, energieffektive bygninger, 5G- og big data-OPP'er[36] og andre sektorspecifikke OPP'er[37] samt initiativet vedrørende tingenes internet[38]. Endvidere vil der blive fremmet en tæt tilpasning til den europæiske åbne videnskabscloud og det europæiske supercomputinginitiativ for kvantecyberteknologier (f.eks. innovation i kvantenøgledistribution og forskning i kvantecomputing).

Det kontraktlige OPP om cybersikkerhed lanceres under Horisont 2020[39], EU's rammeprogram for forskning og innovation for perioden 2014-2020. Det vil trække på finansiering fra to søjler i programmet, nemlig lederskab inden for støtte- og industriteknologi (LEIT-ICT) og samfundsmæssige udfordringer og sikre samfund (SC7). Det samlede budget for det kontraktlige OPP vil være på op til 450 mio. EUR med en tredobbelt løftestangsfaktor for industriens vedkommende. Cybersikkerhed bør også tages op og koordineres med andre relevante dele af Horisont 2020 (f.eks. energi, transport og samfundsmæssige udfordringer på sundhedsområdet og ekspertisedelen af Horisont 2020). Dette vil bidrage til målsætningerne for det kontraktlige OPP om cybersikkerhed. Denne koordinering bør også finde sted på forhånd ved udformningen af sektorspecifikke strategier.

Det kontraktlige OPP vil blive gennemført på gennemsigtig vis med en åben og fleksibel forvaltning, der er tilpasset et cybersikkerhedsmiljø i hastig udvikling. Det vil også tage hensyn til medlemsstaternes behov for at drøfte, hvordan teknologiske ændringer påvirker den sikre drift af nationale og grænseoverskridende infrastrukturer. På tilsvarende måde skal resultatet af partnerskabet være bæredygtigt i en periode på flere år for at sikre, at dets målsætninger kan opfyldes.

Det kontraktlige OPP vil blive understøttet af Den Europæiske Cybersikkerhedsorganisation (ECSO), hvis medlemskab vil afspejle mangfoldigheden af markedet for cybersikkerhed i Europa. Det vil også omfatte nationale, regionale og lokale offentlige administrationer, forskningscentre, den akademiske verden og andre interesserede parter.

Kommissionen vil:

- indgå et kontraktligt offentligt-privat partnerskab om cybersikkerhed med industrien, så det bliver operationelt i tredje kvartal 2016
- iværksætte Horisont 2020-indkaldelser af forslag i relation til det kontraktlige OPP om cybersikkerhed i første kvartal 2017 og

[36] Det offentligt-private partnerskab om 5G-infrastruktur og det offentligt-private værdipartnerskab om big data.
[37] F.eks. SESAR eller det offentligt-private partnerskab om overgang til jernbanetransport.
[38] Alliancen for innovation i relation til tingenes internet (AIOTI).
[39] http://ec.europa.eu/programmes/horizon2020/en/official-documents

– sikre koordinering af det kontraktlige OPP om cybersikkerhed med relevante sektorspecifikke strategier, Horisont 2020-instrumenter og sektorspecifikke OPP'er.

5. KONKLUSION

I denne meddelelse fremlægges der foranstaltninger til styrkelse af Europas system for modstandsdygtighed over for cyberangreb og fremme af en konkurrencedygtig og innovativ cybersikkerhedsindustri i Europa som bebudet i EU's strategi for cybersikkerhed og i strategien for et digitalt indre marked. Kommissionen opfordrer Europa-Parlamentet og Rådet til at støtte denne fremgangsmåde.