EUROPA-
KOMMISSIONEN

UNIONENS HØJTSTÅENDE
REPRÆSENTANT FOR
UDENRIGSANLIGGENDER
OG SIKKERHEDSPOLITIK

Bruxelles, den 13.9.2017
JOIN(2017) 450 final

FÆLLES MEDDELELSE TIL EUROPA-PARLAMENTET OG RÅDET

Modstandsdygtighed, afskrækkelse og forsvar: opbygning af en stærk cybersikkerhed for EU

1. INDLEDNING

Cybersikkerhed er afgørende både for vores velstand og sikkerhed. Efterhånden som vores dagligdag og økonomier bliver mere og mere afhængige af den digitale teknologi, bliver vi mere og mere sårbare. Cybersikkerhedshændelser er forskelligartede, både med hensyn til hvem der er ansvarlig, og hvad de ønsker at opnå. Ondsindede cyberaktiviteter truer ikke kun vores økonomier og indsatsen for at gennemføre det digitale indre marked, men også selve den måde, vores demokratier, friheder og værdier fungerer på. Vores fremtidige sikkerhed afhænger af vores evne til at beskytte EU mod cybertrusler. Både den civile infrastruktur og den militære kapacitet er afhængige af sikre digitale systemer. Dette blevet anerkendt af Det Europæiske Råd i juni 2017[1], samt i den globale strategi for udenrigs- og sikkerhedspolitikken for Den Europæiske Union.[2]

Risikoen vokser eksponentielt. Undersøgelser viser, at den økonomiske indvirkning af cyberkriminalitet blev femdoblet fra 2013 til 2017 og kan være firedoblet senest i 2019.[3] Der har især været en stigning i forekomsten af ransomware[4], og de seneste angreb[5] afspejler den dramatiske stigning i cyberkriminelle aktiviteter. Ransomware er imidlertid langt fra den eneste trussel.

Cybertrusler kommer både fra ikkestatslige og statslige aktører. De er ofte kriminelle, og motivet er penge, men kan også have politiske og strategiske mål. De kriminelle trusler forstærkes af, at grænsen mellem cyberkriminalitet og "traditionel" kriminalitet udviskes, idet kriminelle gør brug af internettet både som en måde til at opskalere deres aktiviteter på, men også som en kilde til at finde nye metoder og værktøjer til at begå kriminalitet[6]. I langt de fleste tilfælde er chancerne for at opspore de kriminelle minimale, og chancerne for retsforfølgning er endnu mindre.

Samtidig opfylder statslige aktører i stigende grad deres geopolitiske mål ikke alene ved hjælp af traditionelle redskaber såsom militær magt, men også gennem mere diskrete cyberredskaber, herunder gennem indblanding i interne demokratiske processer. Det er nu almindeligt anerkendt, at cyberspace kan bruges til krigsførelse, enten alene eller som del af en hybrid tilgang. Misinformationskampagner, falske nyheder og cyberoperationer, der er målrettet kritisk infrastruktur, bliver mere og mere almindelige og kræver en fælles reaktion. Derfor fremhævede Kommissionen i sit oplæg om fremtiden for det europæiske forsvar[7] betydningen af cyberforsvarssamarbejde.

Medmindre vi forbedrer cybersikkerheden markant, vil risikoen vokse i takt med den digitale omstilling. Milliarder af apparater på "tingenes internet" forventes at være tilsluttet internettet i 2020, men cybersikkerhed prioriteres endnu ikke ved udformningen af disse apparater[8]. Manglende beskyttelse af apparater, som vil kontrollere vore elnet, biler og transportnet, fabrikker, finanser, hospitaler og hjem, kan have ødelæggende virkninger og forårsage stor

---

1 http://www.consilium.europa.eu/da/press/press-releases/2017/06/23-euco-conclusions/.

2 http://europa.eu/globalstrategy/.

3 Se f.eks. McAfee & Centre for Strategic and International Studies "Net losses: Estimating the Global Cost of Cybercrime" 2014.

4 Ransomware er en form for malware, der forhindrer eller begrænser brugernes adgang til deres system enten ved at låse systemets skærm eller brugernes filer, medmindre der betales en løsesum.

5 I maj 2017 ramte ransomware-angrebet WannaCry over 400 000 computere i over 150 lande. En måned senere ramte ransomware-angrebet "Petya" Ukraine og en lang række virksomheder i hele verden.

6 Europols Serious and Organised Crime Threat Assessment 2017.

7 https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_da.pdf.

8 IDC og TXT Solutions (2014), SMART 2013/0037, "Cloud and IoT combination", undersøgelse gennemført for Kommissionen.

skade på forbrugernes tillid til nye teknologier. Risikoen for politisk motiverede angreb på civile mål og mangler i det militære cyberforsvar øger risikoen yderligere.

Den tilgang, der redegøres for i denne fælles meddelelse, vil gøre EU bedre rustet til at håndtere disse trusler. Den vil skabe større robusthed og strategisk autonomi, hvilket vil styrke kapaciteten med hensyn til teknologi og færdigheder samt bidrage til at skabe et stærkt indre marked. Dette kræver, at der findes de rette strukturer, således at der kan opbygges en stærk cybersikkerhed og reageres, når det er nødvendigt, med fuld inddragelse af alle centrale aktører. Denne tilgang vil også bedre kunne afværge cyberangreb, idet arbejdet med at opdage, spore og stille de ansvarlige til regnskab intensiveres. Den vil også anerkende den globale dimension ved at skabe et internationalt samarbejde, som skal være platform for EU's lederskab inden for cybersikkerhed. Disse tiltag bygger på tilgangene for det digitale indre marked, den globale strategi, den europæiske dagsorden om sikkerhed[9], den fælles ramme for imødegåelse af hybride trusler[10] og Kommissionens meddelelse om oprettelse af Den Europæiske Forsvarsfond[11][12].

EU arbejder allerede nu med mange af disse spørgsmål. Nu er tiden kommet til at samle de forskellige indsatsområder. I 2013 fastlagde EU en strategi for cybersikkerhed med en række vigtige indsatsområder for at forbedre cyberrobustheden[13]. De vigtigste mål og principper om at fremme et pålideligt, sikkert og åbent cyberøkosystem, er stadig gyldige. Men trusselsbilledet, der hele tiden udvikler sig og forværres, stiller krav om en øget indsats for at modstå og afværge angreb i fremtiden[14].

EU har på baggrund af rækkevidden af sine politikker og de værktøjer og strukturer og den kapacitet, der er til rådighed, gode forudsætninger for at tackle cybersikkerhed. Selv om medlemsstaterne fortsat har ansvaret for den nationale sikkerhed, er truslens omfang og grænseoverskridende karakter et stærkt argument for aktioner på EU-plan, der tilskynder til og støtter medlemsstaternes udvikling og opretholdelse af større og bedre national cybersikkerhedskapacitet, mens der samtidig opbygges kapacitet på EU-niveau. Denne tilgang har til formål at anspore alle aktører — EU, medlemsstaterne, erhvervslivet og enkeltpersoner — til at give den nødvendige prioritering til cybersikkerhed for at skabe robusthed og sikre en bedre reaktion på cyberangreb i EU. Den vil indebære konkrete skridt til at hjælpe med at opdage og efterforske enhver form for cyberhændelser mod EU og dets medlemsstater og til at reagere hensigtsmæssigt, herunder ved at retsforfølge kriminelle. Den vil muliggøre EU's indsats udadtil, således at cybersikkerhed fremmes på en effektiv måde på globalt plan. Resultatet vil være et skift i EU fra en reaktiv til en proaktiv tilgang til beskyttelse af Europas velstand, samfund og værdier såvel som af de grundlæggende rettigheder og friheder, idet der reageres på både eksisterende og kommende trusler.

2. OPBYGNING AF EU'S ROBUSTHED OVER FOR CYBERANGREB

---

9 COM(2015) 185 final.

10 JOIN(2016) 18 final.

11 COM(2017) 295.

12 Tilgangen underbygges også af uafhængig videnskabelig rådgivning ydet af Europa-Kommissionens gruppe af videnskabelige rådgivere på højt plan for mekanismen for videnskabelig rådgivning (se referencer nedenfor).

13 JOIN(2013) 1 final. En vurdering af denne strategi findes i SWD(2017) 295.

14 Forslagene i denne meddelelse er budgetneutrale, medmindre andet er angivet. Initiativer, der har budgetmæssige virkninger, vil nøje følge de årlige budgetprocedurer og kan ikke foregribe den næste flerårige finansielle ramme for perioden efter 2020.

Det er nødvendigt med en fælles og omfattende tilgang for at opnå stor cyberrobusthed. Det kræver mere robuste og effektive strukturer at fremme cybersikkerhed og reagere på cyberangreb ikke kun i medlemsstaterne, men også i EU's egne institutioner, agenturer og organer. Det kræver også en mere omfattende, tværpolitisk tilgang til opbygning af cyberrobusthed og strategisk autonomi med et stærkt indre marked, betydelige fremskridt i EU's teknologiske kapacitet og et langt større antal kvalificerede eksperter. Kernen i dette er en bredere accept af, at cybersikkerhed er en fælles samfundsmæssig udfordring, hvilket betyder, at flere lag af regeringen, økonomien og samfundet bør inddrages.

2.1 Styrkelse af Den Europæiske Unions Agentur for Net- og Informationssikkerhed

Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA) spiller en vigtig rolle med hensyn til at styrke EU's cyberrobusthed og reaktion på cyberhændelser, men er begrænset af sit nuværende mandat. Kommissionen fremlægger derfor et ambitiøst forslag til en reform, herunder **et permanent mandat til agenturet**[15]. Dette vil sikre, at ENISA kan yde støtte til medlemsstaterne, EU-institutionerne og erhvervslivet på centrale områder, bl.a. gennemførelsen af direktivet om sikkerhed ved net- og informationssystemer[16] ("NIS-direktivet") og den foreslåede ramme for cybercertificering.

Det reformerede ENISA vil have en stærk rådgivende rolle i udformningen og gennemførelsen af politikker, herunder fremme sammenhængen mellem sektorspecifikke initiativer og NIS-direktivet og bidrage til at oprette centre for informationsudveksling- og -analyse i kritiske sektorer. ENISA vil hæve niveauet og forstærke EU's beredskab ved at afholde årlige fælleseuropæiske cybersikkerhedsøvelser, der kombinerer reaktion på forskellige niveauer. Det vil også yde støtte til EU's politikudvikling inden for informations- og kommunikationsteknologi (IKT) og cybersikkerhedscertificering samt spille en vigtig rolle i forhold til at intensivere både det operationelle samarbejde og krisestyringen i hele EU. Agenturet vil også fungere som et knudepunkt for information og viden i cybersikkerhedsmiljøet.

En hurtig og fælles forståelse af trusler og hændelser, i takt med at de udvikler sig, er en forudsætning for at afgøre, om det er nødvendigt med en fælles afbødnings- og reaktionsindsats med støtte fra EU. En sådan informationsudveksling kræver inddragelse af alle relevante aktører – EU-organer og -agenturer samt medlemsstater — på teknisk, operationelt og strategisk plan. ENISA vil i samarbejde med de relevante organer i medlemsstaterne og på EU-plan, navnlig netværket af enheder, der håndterer IT-sikkerhedshændelser,[17] CERT-EU, Europol og EU's Efterretningsanalysecenter (INTCEN), også bidrage til situationsbevidsthed på EU-plan. Dette kan indgå i trusselsefterretningerne og politikudformningen i forbindelse med regelmæssig overvågning af trusselsbilledet og effektivt operationelt samarbejde samt som reaktion på væsentlige grænseoverskridende hændelser.

2.2 På vej mod et indre marked for cybersikkerhed

[15] COM(2017) 477.

[16] Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen.

[17] Som fastsat i artikel 9 i NIS-direktivet.

Væksten på markedet for cybersikkerhed i EU — for så vidt angår produkter, tjenester og processer — bremses på en række forskellige måder. Et vigtigt aspekt er manglen på ordninger for cybersikkerhedscertificering, der er anerkendt i hele EU, og som kan tilføre produkter højere standarder for robusthed og underbygge markedstilliden i hele EU. Kommissionen fremsætter derfor et forslag til **en EU-ramme for cybersikkerhedscertificering**[18]. Rammen vil fastsætte proceduren for fastlæggelse af EU-dækkende ordninger for cybersikkerhedscertificering, som omfatter produkter, tjenester og/eller systemer, og som tilpasser sikringsniveauet til den anvendelse, det drejer sig om (det være sig kritiske infrastrukturer eller forbrugerapparater)[19]. Det vil medføre klare fordele for virksomhederne, som undgår at skulle gå igennem flere godkendelsesprocedurer, når de handler på tværs af grænserne, hvilket således begrænser de administrative og finansielle omkostninger. Anvendelsen af ordninger, der udvikles i henhold til denne ramme, vil også bidrage til at opbygge forbrugernes tillid med indførelsen af et overensstemmelsescertifikat, som skal informere og overbevise køberne og brugerne om de sikkerhedsmæssige egenskaber ved de produkter og tjenester, de køber og bruger. Dette vil bevirke, at høje standarder for cybersikkerhed bliver en kilde til konkurrencemæssige fordele. Resultatet vil skabe øget robusthed, eftersom IKT-produkter og -tjenester vil blive formelt bedømt ud fra et fastsat sæt standarder for cybersikkerhed, som kan udarbejdes i tæt sammenhæng med det generelle igangværende arbejde vedrørende IKT-standarder[20].

Ordningerne inden for rammen vil være frivillige og vil ikke pålægge forhandlere eller tjenesteudbydere nogen umiddelbare reguleringsforpligtelser Ordningerne vil ikke være i modstrid med gældende lovkrav som f.eks. EU's lovgivning om databeskyttelse.

Når rammen er oprettet, vil Kommissionen opfordre de relevante interessenter til at fokusere på tre prioriterede områder:

- Sikkerheden i forbindelse med kritiske anvendelser eller højrisikoanvendelser[21]: Systemer, som vi er afhængige af i forbindelse med vores daglige aktiviteter, lige fra biler til maskiner på fabrikker og fra de største systemer såsom fly eller kraftværker til de mindste, f.eks. medicinsk udstyr, bliver mere og mere digitale og indbyrdes forbundne. Derfor vil centrale IKT-komponenter i sådanne produkter og systemer kræve strenge sikkerhedsvurderinger.

- Cybersikkerhed i forbindelse med bredt anvendte digitale produkter, net, systemer og tjenester, som anvendes både i den private og den offentlige sektor for at forsvare sig mod angreb og overholde reguleringsmæssige krav[22] — såsom kryptering af mail, firewalls og virtuelle private netværk. Det er afgørende, at udbredelsen af sådanne værktøjer ikke fører til nye risici eller nye sårbarheder.

- Brugen af "indbygget sikkerhed" i billige, digitale, indbyrdes forbundne masseforbrugsapparater, der udgør tingenes internet. Ordninger i henhold til rammen vil kunne anvendes til at tilkendegive, at produkterne er fremstillet ved hjælp af de nyeste

[18] COM(2017) 477.

[19] Et sikringsniveau angiver graden af strenghed i sikkerhedsvurderingen og svarer normalt til det risikoniveau, der er forbundet med disse anvendelsesområder eller funktioner (dvs. der kræves et højere sikringsniveau for IKT-produkter eller -tjenester, der anvendes på højrisikoanvendelsesområder eller i højrisikofunktioner).

[20] COM(2016) 176.

[21] Der vil være en undtagelse, hvis obligatorisk eller frivillig certificering er reguleret ved andre EU-retsakter.

[22] F.eks. direktiv (EU) 2016/1148, forordning (EU) 2016/679, direktiv (EU) 2015/2366 og andre forslag til lovgivning såsom den europæiske kodeks for elektronisk kommunikation, som hver især kræver, at organisationer indfører passende sikkerhedsforanstaltninger til håndtering af relevante cybersikkerhedsrisici.

metoder til sikker udvikling, har gennemgået passende sikkerhedstestning, og at forhandlerne har forpligtet sig til at opdatere deres software i tilfælde af nye sårbarheder eller trusler.

Disse prioriterede områder bør tage særligt hensyn til udviklingen i trusselsbilledet på cybersikkerhedsområdet samt betydningen af væsentlige tjenester som f.eks. transport, energi, sundhed, bankvæsen, finansielle markedsinfrastrukturer, drikkevand eller digital infrastruktur[23].

Selv om det ikke kan garanteres, at IKT-produkter, systemer eller tjenester er "100 %" sikre, er der en række velkendte og veldokumenterede mangler i designet af IKT-produkter, der kan udnyttes til angreb. Den tilgang med "indbygget sikkerhed", som producenter af forbundne apparater, IT-software og udstyr har valgt, vil sikre, at der tages hensyn til cybersikkerhed, inden nye produkter bringes på markedet. Dette kunne indgå i princippet om "rettidig omhu", der skal videreudvikles i samarbejde med industrien, og som kan mindske sårbarheder ved produkter/software ved at anvende en række metoder, fra design til testning og kontrol, herunder formel kontrol, hvis det er relevant, langsigtet vedligeholdelse og anvendelse af sikre udviklingsprocesser i hele produktets livscyklus samt ved at udvikle opdateringer og patches til håndtering af hidtil uopdagede sårbarheder og hurtig opdatering og reparation[24]. Dette vil også øge forbrugernes tillid til digitale produkter.

Desuden bør den vigtige rolle, som tredjeparters sikkerhedsforskere spiller med hensyn til at opdage sårbarhed ved eksisterende produkter og tjenester, anerkendes, og der bør i alle medlemsstater skabes betingelser, der muliggør koordineret offentliggørelse af sårbarheder[25], som bygger på bedste praksis[26] og relevante standarder[27].

Samtidig er der **specifikke sektorer**, der står over for særlige problemer, og som bør tilskyndes til at udvikle deres egen tilgang. Generelle cybersikkerhedsstrategier vil således blive suppleret af sektorspecifikke cybersikkerhedsstrategier på områder som finansielle tjenester[28], energi, transport og sundhed[29].

Kommissionen har allerede fokuseret på de specifikke spørgsmål vedrørende **ansvar**, som de nye digitale teknologier rejser[30], og der arbejdes på at analysere konsekvenserne; de næste skridt vil være afsluttet senest i juni 2018. Cybersikkerhed rejser spørgsmål vedrørende erstatningsansvar for erhvervslivet og forsyningskæderne, og manglende løsning af disse

---

[23] Sektorer omfattet af Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen.

[24] Cybersecurity in the European Digital Single Market – Gruppen af videnskabelige rådgivere på højt plan, marts 2017.

[25] Koordineret offentliggørelse af sårbarheder er en form for samarbejde, som gør det lettere og muligt for sikkerhedsforskere at rapportere om sårbarheder til ejeren eller forhandleren af informationssystemet, og gør det muligt for organisationen at diagnosticere og afhjælpe sårbarheden på en korrekt og rettidig måde, inden mere detaljerede oplysninger om sårbarhed videregives til tredjepart eller offentligheden.

[26] F.eks. Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations, ENISA, 2016.

[27] ISO/IEC 29147: 2014 Informationsteknologi — Sikkerhedsteknikker — Sårbarhedsbeskrivelse.

[28] Kommissionens kommende arbejde med finansiel teknologi vil omfatte cybersikkerhed i den finansielle sektor.

[29] I energisektoren f.eks. ved at kombinere meget gamle teknologier og avancerede informationsteknologier, navnlig med elnettets realtidskrav.

[30] COM(2017) 228.

spørgsmål vil hæmme udviklingen af et stærkt indre marked for cybersikkerhedsprodukter og -tjenester.

Endelig er udviklingen af EU's indre marked også afhængig af, at cybersikkerhed indregnes som en faktor i politikker vedrørende handel og investeringer. Effekten af udenlandske erhvervelser på kritiske teknologier — som cybersikkerhed er et vigtigt eksempel på — er et centralt aspekt i forbindelse med **overvågning af udenlandske direkte investeringer i Den Europæiske Union**[31], som har til formål muliggøre overvågning af investeringer fra tredjelande af hensyn til sikkerheden og den offentlige orden. Cybersikkerhedskrav har allerede skabt handelshindringer for EU-varer og -tjenester i vigtige sektorer i en række tredjelandsøkonomier. EU's ramme for cybersikkerhedscertificering vil yderligere styrke Europas internationale position og bør suppleres af en fortsat indsats for udvikling af globale standarder for høj sikkerhed og gensidige anerkendelsesordninger.

2.3 Fuld gennemførelse af direktivet om sikkerheden ved net- og informationssystemer

De vigtigste redskaber til bekæmpelse af cyberkriminalitet i dag er på nationale hænder, og EU har anerkendt behovet for at fremme højere standarder. Væsentlige cybersikkerhedshændelser berører sjældent kun en enkelt medlemsstat, hvilket skyldes, at nøglesektorer som f.eks. bankvæsen, energi eller transport bliver stadig mere globaliserede, digitalt afhængige og indbyrdes forbundne.

Direktivet om sikkerheden ved net- og informationssystemer ("NIS-direktivet") er den første cybersikkerhedslovgivning, der omfatter hele EU[32]. Formålet er at opbygge robusthed ved at forbedre den nationale cybersikkerhedskapacitet, fremme et bedre samarbejde mellem medlemsstaterne og stille krav om, at virksomheder i vigtige økonomiske sektorer indfører en effektiv praksis for risikostyring og indberetter alvorlige hændelser til de nationale myndigheder. Disse forpligtelser gælder også for de tre typer af udbydere af centrale internettjenester: cloud computing, søgemaskiner og onlinemarkedspladser. Målet er en stærkere og mere systematisk tilgang og en bedre informationsstrøm.

Det er afgørende for EU's cyberrobusthed, at direktivet er fuldstændigt gennemført i alle medlemsstater senest i maj 2018. Processen støttes af en fælles indsats fra medlemsstaterne, som senest i efteråret 2017 vil munde ud i retningslinjer for at støtte en mere harmoniseret gennemførelse, navnlig for så vidt angår operatører af væsentlige tjenester. Kommissionen offentliggør som led i denne pakke om cybersikkerhed også en meddelelse[33] for at støtte denne indsats gennem eksempler på bedste praksis fra medlemsstaterne, som er relevant for gennemførelsen af direktivet, og vejledning om, hvordan direktivet bør fungere i praksis.

Informationsstrøm er et område, hvor det vil være nødvendigt at supplere direktivet. For eksempel omfatter direktivet kun de vigtigste strategiske sektorer — men det er logisk, at alle interessenter, der rammes af cyberangreb, vil skulle anvende en ensartet tilgang for at opnå en systematisk vurdering af sårbarheder og indgangssteder for cyberangribere. Hertil kommer, at samarbejde og udveksling af oplysninger mellem den private og offentlige sektor støder på en række hindringer. Regeringer og offentlige myndigheder er tilbageholdende med at ville dele cybersikkerhedsrelevante oplysninger af frygt for at skade den nationale sikkerhed eller konkurrenceevne. Private virksomheder er tilbageholdende med at udveksle oplysninger om deres cybersårbarheder og deraf følgende tab af frygt for at afsløre følsomme

[31] COM(2017) 478.

[32] Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen.

[33] COM(2017) 476.

forretningsoplysninger, skade deres omdømme eller overtræde reglerne om beskyttelse af personoplysninger[34]. Der er behov for at styrke tilliden, således at offentlig-private partnerskaber kan understøtte bredere samarbejde og informationsudveksling mellem et større antal sektorer. Den rolle, som centrene for informationsudveksling og -analyse spiller, er særlig vigtig for skabelsen af den nødvendige tillid til informationsudveksling mellem den private og offentlige sektor. Der er taget nogle første initiativer for særlige kritiske sektorer som f.eks. luftfart, med oprettelsen af European Center for Cybersecurity in Aviation[35], og energi, med udviklingen af informationsudvekslings- og analysecentre[36]. Kommissionen vil bidrage fuldt ud til denne tilgang med støtte fra ENISA for at fremskynde udviklingen navnlig i sektorer, der leverer væsentlige tjenester som fastlagt i NIS-direktivet.

2.4 Robusthed gennem hurtig reaktion i nødsituationer

Når et cyberangreb finder sted, kan en hurtig og effektiv reaktion afbøde virkningerne heraf. Dette kan også vise, at offentlige myndigheder ikke er magtesløse over for cyberangreb, og bidrage til at skabe tillid. For så vidt angår EU-institutionernes egen reaktion bør cyberaspekterne i første omgang integreres i EU's eksisterende krisestyringsmekanismer: EU's integrerede ordninger for politisk kriserespons, der koordineres af formandskabet for Rådet[37], og EU's generelle systemer for hurtig varsling[38]. Behovet for at reagere på særligt alvorlige cyberhændelser eller -angreb bør være tilstrækkelig grund til, at en medlemsstat kan påberåbe sig EU's solidaritetsbestemmelse[39].

En hurtig og effektiv reaktion afhænger også af en hurtig informationsudvekslingsmekanisme mellem alle centrale aktører på nationalt plan og EU-plan, hvilket igen kræver klarhed om deres respektive roller og ansvarsområder. Kommissionen har hørt institutionerne og medlemsstaterne om en plan for indførelsen af en effektiv proces for operationel reaktion på EU-plan og på medlemsstatsplan på væsentlige cyberhændelser. Den **plan**, der fremlægges i en henstilling[40] i denne pakke, forklarer, hvordan cybersikkerhed integreres i eksisterende krisestyringsmekanismer på EU-plan og fastlægger målene og formerne for samarbejde mellem medlemsstaterne og EU's relevante institutioner, tjenester, agenturer og organer[41], når der skal reageres på væsentlige cybersikkerhedshændelser og -kriser. I henstillingen opfordres medlemsstaterne og EU-institutionerne også til at etablere en EU-krisereaktionsramme for cybersikkerhed for at gøre planen operationel. Planen vil jævnlig blive testet i forbindelse med cyberøvelser og andre krisestyringsøvelser[42] og opdateret, når det er nødvendigt.

---

[34] Cybersecurity in the European Digital Single Market – Gruppen af videnskabelige rådgivere på højt plan, marts 2017. Et særligt problem vedrører forretningshemmeligheder, hvor man i meddelelsen fra juli 2016 "Styrkelse af Europas system for modstandsdygtighed over for cyberangreb" konstaterede en tilbageholdenhed med at indberette cybertyveri af forretningshemmeligheder, og at det derfor er vigtigt med sikre indberetningskanaler, der garanterer fortroligheden.

[35] https://www.easa.europa.eu/newsroom-and-events/news/implementation-european-centre-cyber-security-aviationeccsa.

[36] Disse er medlemsdrevne nonprofitorganisationer, der er oprettet af private og offentlige enheder, med henblik på udveksling af oplysninger om cybertrusler, risici, forebyggelse, afbødning og reaktion. Se f.eks. European Energy Information Sharing and Analysis Centres (http://www.ee-isac.eu).

[37] Dette muliggør koordinerede reaktioner på store tværsektorielle kriser på højeste politiske plan.

[38] Disse muliggør intern informationsudveksling og koordinering i forbindelse med nye multisektorale kriser eller en forudseelig eller umiddelbar trussel, der kræver aktioner på EU-plan.

[39] I henhold til artikel 222 i traktaten om Den Europæiske Unions funktionsmåde.

[40] C(2017) 6100.

[41] Herunder Europol, ENISA, EU's IT-beredskabsenhed for EU's institutioner, organer og agenturer (CERT-EU) og for EU's Efterretningsanalysecenter (INTCEN).

[42] F.eks. øvelser, der afholdes af ENISA: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

Eftersom cybersikkerhed kan have væsentlig indvirkning på økonomiernes funktion og menneskers dagligdag, kunne det være en mulighed at undersøge, om der kan etableres en **beredskabsfond for cybersikkerhed**, i lighed med andre sådanne krisemekanismer på andre EU-politikområder. Dette ville give medlemsstaterne mulighed for at søge hjælp på EU-plan under eller efter en større hændelse, forudsat at medlemsstaten har indført et fornuftig system for cybersikkerhed forud for hændelsen, herunder fuld gennemførelse af NIS-direktivet, veludviklet risikostyring og tilsynsrammer på nationalt plan. En sådan fond, der supplerer eksisterende krisestyringsmekanismer på EU-plan, kan benytte sig af en hurtig reaktionskapacitet af hensyn til solidariteten og finansiere specifikke beredskabsaktioner som f.eks. udskiftning af kompromitteret udstyr eller anvendelse af afbødnings- eller reaktionsværktøjer, idet der trækkes på national ekspertise ligesom det er tilfældet med EU-civilbeskyttelsesmekanismen.

2.5 Kompetencenetværk for cybersikkerhed med et europæisk forsknings- og kompetencecenter for cybersikkerhed

De teknologiske redskaber for cybersikkerhed er strategiske aktiver og samtidig vigtige vækstteknologier for fremtiden. Det er i EU's strategiske interesse at sikre, at EU bevarer og udvikler afgørende kapaciteter til at sikre den digitale økonomi, samfundet og demokratiet, beskytte kritisk hardware og software og tilvejebringe vigtige cybersikkerhedstjenester.

Det offentlig-private partnerskab om cybersikkerhed[43], som blev oprettet i 2016, var et vigtigt første skridt og mobiliserer investeringer på op til 1,8 mia. EUR frem til 2020. Dog viser omfanget af investeringer, der er undervejs i andre dele af verden[44], at EU skal gøre mere med hensyn til investeringer og for at overvinde fragmenteringen af kapaciteter spredt ud over hele EU.

EU kan skabe merværdi som følge af cybersikkerhedsteknologiens kompleksitet, de nødvendige omfattende investeringer og behovet for løsninger, der fungerer i hele EU. Med udgangspunkt i medlemsstaternes og det offentlig-private partnerskabs arbejde vil et yderligere skridt bestå i at styrke EU's cybersikkerhedskapacitet ved hjælp af et **netværk af kompetencecentre for cybersikkerhed**[45] med et **europæisk forsknings- og kompetencecenter for cybersikkerhed** i centrum. Netværket og dets center vil stimulere udviklingen og anvendelsen af teknologi inden for cybersikkerhed og supplere kapacitetsopbygningsbestræbelserne på dette område på EU-plan og på nationalt plan. Kommissionen vil gennemføre en konsekvensanalyse for at undersøge de tilgængelige muligheder – herunder muligheden af at oprette et fællesforetagende – med henblik på indførelsen af denne struktur i 2018.

Som et første skridt og for at bidrage til den fremtidige tankegang vil Kommissionen foreslå, at der iværksættes en pilotfase under Horizon 2020 for at hjælpe nationale centre med at gå sammen i netværk, som vil skabe ny fremdrift inden for cybersikkerhedskompetence og teknologiudvikling. Den har planer om at foreslå en kortsigtet tilførsel af midler på 50 mio. EUR til dette formål. Denne aktivitet vil supplere det igangværende offentlig-private partnerskab om cybersikkerhed.

---

[43] C(2016) 4400 final.

[44] USA vil investere 19 mia. USD i cybersikkerhed alene i 2017, hvilket er en stigning på 35 % i forhold til 2016. The White House, Office of the Press Secretary: "Fact Sheet: Cybersecurity National Action Plan", 9. februar 2016.

[45] Netværket vil omfatte eksisterende og fremtidige cybersikkerhedscentre i medlemsstaterne, hvis medlemmer typisk vil være offentlige forskningsorganisationer og laboratorier.

Sammenlægning og udformning af forskningsindsatsen vil være kernen i netværket og centrets indledende fokus. For at støtte udviklingen af industrielle kapaciteter vil centret kunne fungere som en kapacitetsprojektleder, der kan håndtere multinationale projekter. Dette vil også sætte yderligere skub i EU-industriens innovation og konkurrenceevne på den globale scene med udvikling af digitale næstegenerationsteknologier, herunder kunstig intelligens, kvantedatabehandling, blockchain og sikre digitale identiteter, samt sikre EU-baserede selskaber adgang til massedata, hvilket alt sammen er nøglen til fremtidens cybersikkerhed. Centret vil også trække på EU's arbejde med at opskalere højtydende databehandlingsinfrastruktur. Dette har afgørende betydning for analyse af store mængder data, hurtig kryptering og dekryptering af data, kontrol af identitet, simulering af cyberangreb og analyse af videomateriale[46].

Netværket af kompetencecentre vil også kunne have kapacitet til at støtte industrien gennem testning og simulering for at understøtte den cybersikkerhedscertificering, der er beskrevet i afsnit 2.2. Dets inddragelse i alle EU's cybersikkerhedsaktiviteter vil sikre en løbende ajourføring af målretning efter behov. Centret vil sigte mod at fremme høje standarder for cybersikkerhed ikke kun i forbindelse med teknologi og cybersikkerhedssystemer, men også i forbindelse med udvikling af avancerede færdigheder for fagfolk gennem tilvejebringelse af løsninger og modeller for nationale tiltag til udbredelse af digitale færdigheder. Det vil derfor også forbedre cybersikkerhedskapaciteter på EU-plan og bygge på synergier navnlig med ENISA, CERT-EU, Europol, den eventuelle fremtidige beredskabsfond for cybersikkerhed og nationale CSIRT'er.

Kompetencenetværket skal have særlig fokus på den manglende europæiske kapacitet til at vurdere **krypteringen** af de produkter og tjenester, der anvendes af borgere, virksomheder og myndigheder på det digitale indre marked. Stærk kryptering er grundlaget for sikre digitale identifikationssystemer, som spiller en afgørende rolle for effektiv cybersikkerhed[47]; Stærk kryptering sikrer også folks intellektuelle ejendom og gør det muligt at beskytte grundlæggende rettigheder som f.eks. ytringsfrihed og beskyttelse af personoplysninger og sikrer sikker nethandel[48].

Eftersom EU's markeder for civil og militær cybersikkerhed har fælles udfordringer[49] og teknologi med dobbelt anvendelse, der kræver tæt samarbejde på kritiske områder, kan anden fase af netværket og dets center videreudvikles med en cyberforsvarsdimension under fuld overholdelse af traktatbestemmelserne om fælles sikkerheds- og forsvarspolitik. Forsvarsdimensionen og dens teknologiske fokus kan bidrage til samarbejdet mellem medlemsstaterne på cyberforsvarsområdet, herunder informationsdeling, situationsbevidsthed, ekspertiseopbygning og koordinerede reaktioner, og støtte medlemsstaternes udvikling af fælles kapaciteter. Dimensionen kan også fungere som en platform, der sætter medlemsstaterne i stand til at fastlægge prioriteterne for EU's cyberforsvar, udforsker fælles løsninger, bidrager til udvikling af fælles strategier, fremmer fælles uddannelse inden for cyberforsvar, øvelser og testning på EU-plan og støtter arbejdet med cyberforsvarstaksonomier og -standarder, hvor centret har en rådgivende rolle. For at udøve ovennævnte aktiviteter vil centret skulle arbejde tæt sammen med og i fuld komplementaritet med Det Europæiske Forsvarsagentur på cyberforsvarsområdet samt med ENISA på

[46] COM(2012) 45 final og COM(2016) 178 final.

[47] Kommissionen vil allerede under Horisont 2020 lancere en ny Horizon-challengepris, som er på 4 mio. EUR til den bedste innovative løsning for sømløse elektroniske autentificeringsmetoder.

[48] Cybersecurity in the European Digital Single Market – Gruppen af videnskabelige rådgivere på højt plan, marts 2017.

[49] "Study on synergies between the civilian and the defence cybersecurity markets"(Optimity; SMART 2014-0059).

cyberrobusthedsområdet. Denne forsvarsdimension vil tage hensyn til den proces, der blev igangsat i oplægget om fremtiden for Europas forsvar.

Den høje grad af robusthed, der kræves inden for cyberforsvar, fordrer specifik målretning af forsknings- og teknologiressourcer. De cyberforsvarsprojekter eller -teknologier, som virksomheder har udviklet, kan få gavn af finansiering fra Den Europæiske Forsvarsfond både i forsknings- og udviklingsfasen[50]. Specifikke områder såsom kryptering baseret på kvanteteknologier, cybersituationsbevidsthed, biometriske adgangskontrolsystemer, opdagelse af avancerede vedholdende trusler eller datamining kunne være særlig relevante i denne sammenhæng. Den højtstående repræsentant, Det Europæiske Forsvarsagentur og Kommissionen vil hjælpe medlemsstaterne med at identificere områder, hvor fælles cybersikkerhedsprojekter kan komme på tale til finansiering af Den Europæiske Forsvarsfond.

2.6 Opbygning af en stærk EU-base for cyberfærdigheder

Cybersikkerhed har en stærk uddannelsesdimension. Effektiv cybersikkerhed er stærkt afhængig af de berørte personers færdigheder. Det forudses dog, at der vil mangle 350 000 fagfolk med færdigheder inden for cybersikkerhed i den private sektor i Europa i 2022[51]. Uddannelse inden for cybersikkerhed bør udvikles på alle niveauer, startende med regelmæssig uddannelse af en cyberarbejdsstyrke, yderligere cybersikkerhedsuddannelse for alle IKT-specialister og nye specifikke cybersikkerhedsundervisningsplaner. Der skal etableres stærke akademiske ekspertisecentre for at tilfredsstille efterspørgslen efter fremskyndet uddannelse, som kan trække på rådgivning fra et europæisk forsknings- og kompetencecenter for cybersikkerhed og ENISA. Målet bør være, at det bliver naturligt at designe IKT-produkter og -systemer, som fra begyndelsen inkorporerer sikkerhedsprincipper. Uddannelse inden for cybersikkerhed bør ikke være begrænset til IT-fagfolk, men bør integreres i undervisningsplanerne for andre område, f.eks. ingeniørvidenskab, virksomhedsledelse og jura, samt for specifikke uddannelsesspor. Endelig bør lærere og elever i grundskolen og på ungdomsuddannelserne bevidstgøres om cyberkriminalitet og cybersikkerhed, når de tilegner sig digitale kompetencer i skolerne.

EU bør sammen med medlemsstaterne også bidrage ved at bygge videre på det arbejde, som koalitionen for digitale færdigheder og job[52] har gennemført, og ved f.eks. at indføre lærlingeordninger inden for cybersikkerhed i SMV'er.

2.7 Fremme af cyberhygiejne og -bevidsthed

Det siges, at ca. 95 % af alle hændelser skyldes "en eller anden form for menneskelige fejl — bevidst eller ej"[53], og der er således en stærk menneskelig faktor, der spiller ind. Cybersikkerhed er således et fælles ansvar. Dette er ensbetydende med, at enkeltpersoners, virksomheders og offentlige myndigheders adfærd må ændres for at sikre, at alle forstår truslen og er udstyret med de nødvendige værktøjer og færdigheder til hurtigt at opdage og aktivt beskytte sig selv mod angreb. Folk har behov for at udvikle gode vaner inden for cyberhygiejne, og virksomheder og organisationer skal indføre passende risikobaserede cybersikkerhedsprogrammer og ajourføre dem regelmæssigt for at tage højde for udviklingen i risikosituationen.

---

[50] Allerede nu vil den europæiske forsvarsindustris udviklingsprogram prioritere projekter vedrørende cyberforsvar, og cyberforsvar bliver et af emnerne i den indkaldelse af forslag, som vil blive iværksat i 2018.

[51] Global Information Security Workforce Study 2017. På globalt plan er tallet 1,8 mio.

[52] https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition.

[53] IBM "Cybersecurity Intelligence indeks" 2014, omhandlet i Securitymagazine.com, 19. juni 2014.

NIS-direktivet fastlægger ikke blot medlemsstaternes forpligtelser til at udveksle oplysninger om cyberangreb på EU-plan, men også til at indføre avancerede nationale cybersikkerhedsstrategier og -rammer for sikkerheden ved net og informationssystemer. Offentlige myndigheder på EU-plan og nationalt plan bør i højere grad spille en ledende rolle med hensyn til at sætte skub i dette arbejde.

For det første bør medlemsstaterne maksimere tilgængeligheden af cybersikkerhedsværktøjer for virksomheder og enkeltpersoner. Navnlig bør der gøres mere for at forebygge og afbøde virkningerne af cyberkriminalitet for slutbrugerne. Et eksempel findes allerede i Europols arbejde med kampagnen "NoMoreRansom"[54], som er bygget op gennem et tæt samarbejde mellem retshåndhævende myndigheder og cybersikkerhedsvirksomheder for at hjælpe brugerne med at forebygge infektioner med ransomware og dekryptere data, hvis de er ofre for et angreb. Sådanne ordninger bør indføres for andre typer skadelig software inden for andre områder, og EU bør udvikle en **enkelt portal, der samler alle disse værktøjer hos en kvikskranke**, der tilbyder rådgivning til brugerne om forebyggelse og opdagelse af malware og links til rapporteringsmekanismer.

For det andet bør medlemsstaterne fremskynde **brugen af flere cybersikre redskaber i udviklingen af e-forvaltning** og også drage fuld nytte af kompetencenetværket. Indførelsen af sikre identifikationsmidler bør fremmes, idet der bygges videre på EU-rammerne for elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked, der har været gældende siden 2016 og giver et forudsigeligt lovgivningsmiljø, således at der åbnes mulighed for sikker og ubesværet elektronisk interaktion mellem virksomheder, enkeltpersoner og de offentlige myndigheder[55]. Desuden bør offentlige institutioner, navnlig dem, der leverer grundlæggende tjenesteydelser, sikre, at deres personale modtager uddannelse inden for cybersikkerhed.

For det tredje bør medlemsstaterne prioritere cyberbevidsthed **inden for rammerne af oplysningskampagner**, herunder kampagner, der er rettet mod skoler, universiteter, erhvervslivet og forskningsorganer. Cybersikkerhedsmåneden, der finder sted hvert år i oktober under koordination af ENISA, vil blive intensiveret for at opnå større rækkevidde som en fælles kommunikationsindsats på EU-plan og nationalt plan. Oplysning om online**misinformationskampagner og falske nyheder** på sociale medier, der er specifikt rettet mod underminering af demokratiske processer og europæiske værdier, er lige så vigtig. Selv om det primære ansvar stadig ligger på nationalt plan — herunder for valg til Europa-Parlamentet — har sammenlægning af ekspertise og udveksling af erfaringer på europæisk plan vist sig at være af merværdi ved at tilvejebringe et fokus for indsatsen[56].

Der er også en fremtrædende rolle for **industrien** generelt, men med særlig vægt på udbydere af digitale tjenester og fabrikanterne. Den skal støtte brugerne (enkeltpersoner, virksomheder og offentlige forvaltninger) med redskaber, som sætter dem i stand til at tage ansvar for deres egne handlinger på nettet, og gøre det klart, at opretholdelse af cyberhygiejne er en

---

54 https://www.nomoreransom.org/.

55 Forordning (EU) nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked (eIDAS-forordningen), der blev vedtaget den 23. juli 2014. Endvidere sørger Europa-Kommissionen for grundelementer og værktøjer til e-ID- og e-signaturinteroperabilitet (f.eks. Trusted Lists Browsers) gennem programmet for Connecting Europe-faciliteten.

56 Et eksempel herpå er East StratCom Task Force, som medlemsstaterne og den højtstående repræsentant oprettede i 2015 for at imødegå Ruslands igangværende misinformationskampagner. Gruppen er i gang med at udvikle kommunikationsprodukter og kampagner med fokus på at redegøre for EU-politikkerne i østpartnerskabsregionen.

uundværlig del af tilbuddene til forbrugerne[57]. For at opdage og fjerne svagheder bør industrien bestræbe sig på at få etableret interne processer for undersøgelse, kategorisering og fjernelse af sårbarheder, uanset om kilden til potentiel sårbarhed er uden for eller inden for den pågældende virksomhed.

Nøgleaktioner

- Fuld gennemførelse af direktivet om sikkerheden ved net og informationssystemer.
- En hurtig vedtagelse fra Europa-Parlamentets og Rådets side af forordningen om et nyt mandat for ENISA og en europæisk ramme for certificering[58].
- Et fælles initiativ mellem Kommissionen og branchen om at definere et "princip om rettidig omhu" for at mindske sårbarheder i produktet/softwaren og fremme "indbygget sikkerhed".
- En hurtig gennemførelse af planen for en grænseoverskridende reaktion på større hændelser.
- Iværksættelse af en konsekvensanalyse for at undersøge muligheden for et forslag fra Kommissionen i 2018 om oprettelse af et netværk af kompetencecentre for cybersikkerhed og et europæisk forsknings- og kompetencecenter for cybersikkerhed, der bygger på en pilotfase, der gennemføres umiddelbart inden.
- Støtte til medlemsstaternes indsats for at udpege områder, hvor fælles cybersikkerhedsprojekter kunne komme i betragtning til støtte fra Den Europæiske Forsvarsfond.
- En EU-dækkende kvikskranke, hvor ofre for cyberangreb kan få hjælp, og som giver oplysninger om de seneste trusler og samler praktisk rådgivning og cybersikkerhedsværktøjer.
- Tiltag fra medlemsstaternes side for at integrere cybersikkerhed i færdighedsprogrammer, e-forvaltning og oplysningskampagner.
- Tiltag fra industriens side for at intensivere cybersikkerhedsrelateret uddannelse af deres personale og indføre en tilgang med "indbygget sikkerhed" for deres produkter, tjenester og processer.

3. ETABLERING AF ET EFFEKTIVT CYBERFORSVAR MED AFSKRÆKKENDE VIRKNING PÅ EU-PLAN

En effektiv afskrækkende virkning indebærer etablering af en ramme med foranstaltninger, der både er troværdige og har en afskrækkende virkning for potentielle cyberkriminelle og -terrorister. Så længe gerningsmændene til cyberangreb — både stater og andre — intet har at frygte ud over fiasko, vil de have et meget begrænset incitament til at stoppe med at prøve. En mere effektiv retshåndhævelsesindsats, der fokuserer på opdagelse, sporing og retsforfølgelse af cyberkriminelle, er af afgørende betydning for at opbygge en effektiv afskrækkende virkning. Hertil kommer behovet for, at EU støtter medlemsstaterne i udviklingen af cybersikkerhedskapacitet med dobbelt anvendelse. Vi vil først begynde at vende udviklingen med hensyn til cyberangreb, når vi øger chancerne for at fange og straffe dem, der begår dem. Cyberangreb bør efterforskes omgående, og gerningsmændene skal retsforfølges, eller der skal træffes foranstaltninger for at muliggøre en passende politisk eller diplomatisk reaktion. I

[57] Visse fabrikanter er allerede vant til dette koncept, da dele af den europæiske produktlovgivning (f.eks. maskindirektivet (2006/42/EF)) fastsætter principper for "sikker udformning".

[58] COM(2017) 477.

tilfælde af en større krise med en betydelig international og forsvarsmæssig dimension kan den højtstående repræsentant fremsætte forslag til en passende reaktion til Rådet.

Der er allerede taget et skridt i retning af at forbedre den strafferetlige reaktion på cyberangreb med vedtagelsen af direktivet om angreb på informationssystemer i 2013[59]. Direktivet indeholder bestemmelser om minimumsregler vedrørende definitionen af strafbare handlinger og sanktioner i forbindelse med angreb på informationssystemer samt operationelle foranstaltninger for at forbedre samarbejdet mellem forskellige myndigheder. Direktivet har medført store fremskridt med hensyn til kriminalisering af cyberangreb på et sammenligneligt niveau i alle medlemsstater, hvilket letter det grænseoverskridende samarbejde mellem retshåndhævende myndigheder, der efterforsker denne type strafbare handlinger. Der er dog stadig muligheder for at udnytte direktivets potentiale fuldt ud, hvis medlemsstaterne gennemfører alle bestemmelserne i fuldt omfang[60]. Kommissionen vil fortsat yde støtte til medlemsstaterne i forbindelse med deres gennemførelse af direktivet og ser i øjeblikket ikke nogen grund til at foreslå ændringer til det.

3.1 Identificering af ondsindede aktører

For at øge vores chancer for at retsforfølge gerningsmændene er vi nødt til hurtigst muligt at forbedre vores kapacitet til at identificere dem, der er ansvarlige for cyberangreb. At finde anvendelige oplysninger med henblik på efterforskning af cyberkriminalitet, hovedsagelig i form af digitale spor, er en stor udfordring for de retshåndhævende myndigheder. Vi er derfor nødt til at øge vores teknologiske kapacitet til at efterforske effektivt, herunder ved at forstærke Europols cyberkriminalitetsenhed med cybersikkerhedseksperter. Europol er blevet en central aktør med hensyn til støtte til medlemsstaternes efterforskning på tværs af jurisdiktioner. Det bør blive et ekspertisecenter for medlemsstaternes retshåndhævende myndigheder i forbindelse med efterforskning på nettet og cyberkriminalteknik.

Den udbredte praksis med at anbringe flere — undertiden tusindvis af — brugere bag en IP-adresse gør det teknisk meget vanskeligt at undersøge ondsindet adfærd på internettet. Det gør det også sommetider nødvendigt, f.eks. i forbindelse med alvorlige forbrydelser såsom seksuelt misbrug, at undersøge et stort antal brugere med henblik på at identificere en ondsindet aktør. EU vil derfor fremme udbredelsen af den nye protokol (IPv6), som giver mulighed for tildeling af en enkelt bruger pr. IP-adresse og dermed bringer klare fordele for retshåndhævelse og cybersikkerhedsundersøgelser. Som et første skridt til at fremme udbredelsen vil Kommissionen indarbejde kravet om at gå over til IPv6 i alle sine politikker, herunder krav i forbindelse med offentlige indkøb, projekt- og forskningsstøtte, samt yde støtte til tilvejebringelse af de nødvendige undervisningsmaterialer. Desuden bør medlemsstaterne overveje frivillige aftaler med internetudbyderne for at fremme indførelsen af IPv6.

Belgien er førende på verdensplan[61] med hensyn til indførelsen af IPv6, bl.a. takket være det offentlig-private samarbejde: Relevante berørte parter har overvejet at begrænse anvendelsen

[59] Europa-Parlamentets og Rådets direktiv 2013/40/EU af 12. august 2013 om angreb på informationssystemer.
[60] COM(2017) 474.
[61] https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption.

af en IP-adresse til højst 16 brugere som en del af en frivillig selvregulerende foranstaltning, der tilskynder til overgang til IPv6[62].

Mere generelt bør onlineansvarlighed fremmes yderligere. Dette indebærer fremme af foranstaltninger med henblik på at forhindre misbrug af domænenavne til distribution af uønskede meddelelser eller phishingangreb. Kommissionen vil derfor arbejde for at forbedre funktionen, tilgængeligheden og nøjagtigheden af oplysningerne i domænenavne og IP WHOIS-systemer[63] i overensstemmelse med den indsats, som ydes af Internet Corporation for Assigned Names and Numbers[64].

3.2 Styrkelse af de retshåndhævende myndigheders indsats

Effektiv **efterforskning** og **retsforfølgning** af cyberkriminalitet er et centralt afskrækkelsesmiddel over for cyberangreb. De aktuelle proceduremæssige rammer skal dog tilpasses bedre til internettets tidsalder[65]. Hastigheden af cyberangreb kan være for høj for vores procedurer og skabe særlige behov for et effektivt samarbejde på tværs af grænserne. Med henblik herpå vil Kommissionen som bebudet i den europæiske dagsorden om sikkerhed i begyndelsen af 2018 fremsætte forslag for **at lette den grænseoverskridende adgang til elektroniske beviser**. Sideløbende hermed er Kommissionen ved at gennemføre praktiske foranstaltninger til forbedring af den grænseoverskridende adgang til elektroniske beviser til strafferetlige efterforskninger, herunder finansiering af uddannelse i grænseoverskridende samarbejde, udvikling af en elektronisk platform for udveksling af oplysninger inden for EU og standardisering af formularer til retligt samarbejde mellem medlemsstaterne.

En anden hindring for effektiv retsforfølgelse er de forskellige kriminaltekniske procedurer for indsamling af elektroniske beviser i forbindelse med efterforskning af cyberkriminalitet i medlemsstaterne. Dette kunne afhjælpes ved at arbejde hen imod etableringen af fælles kriminaltekniske standarder. Desuden skal de kriminaltekniske kapaciteter styrkes for at støtte sporbarhed og tildeling. Det ville være et relevant tiltag at videreudvikle den kriminaltekniske kapacitet i Europol gennem tilpasning af de eksisterende budgetmæssige og menneskelige ressourcer ved Europols europæiske center til bekæmpelse af cyberkriminalitet for at opfylde det voksende behov for operationel støtte til efterforskning af grænseoverskridende cyberkriminalitet. Et andet tiltag ville være at tage det ovenfor beskrevne teknologiske fokus for kryptering i betragtning, når man ser på, hvordan kriminelles misbrug skaber betydelige udfordringer i kampen mod grov kriminalitet, herunder terrorisme og cyberkriminalitet. Kommissionen vil fremlægge resultaterne af de igangværende overvejelser om **betydningen af kryptering i strafferetlige efterforskninger**[66] senest i oktober 2017[67].

---

62 http://bipt.be/public/files/nl/22027/Raadpleging_ipv6.pdf.

63 En protokol for spørgsmål og svar, som er meget udbredt inden for søgning i databaser, der lagrer oplysninger om registrerede brugere eller erhververe af en internetressource.

64 Internet Corporation for Assigned Names and Numbers (ICANN) er en nonprofit-organisation, der har ansvaret for at koordinere vedligeholdelsen og procedurerne for flere databaser med oplysninger om internettets navnerum.

65 For blot at nævne et eksempel blev den (virtuelle) centrale command and control server for Avalanche-botnet flyttet til en ny fysisk server og et nyt domæne hvert femte minut.

66 Formandskabet for Rådet, "Resultat af samlingen i Rådet for Retlige og Indre Anliggender den 8. og 9. december 2016", nr. 15391/16.

67 Ottende statusrapport om indførelsen af en effektiv og ægte sikkerhedsunion af 29. juni 2017 (COM(2017) 354 final).

Eftersom internettet ikke kender nogen grænser, giver de rammer for det internationale samarbejde, som Europarådets **Budapestkonvention om cyberkriminalitet**[68] fastsætter, mulighed for at anvende en optimal juridisk standard for de forskellige nationale lovgivninger vedrørende cyberkriminalitet blandt en forskelligartet gruppe af lande. En mulig tilføjelse af en protokol til konventionen er nu ved at blive undersøgt[69], hvilket også kunne give en kærkommen lejlighed til at behandle spørgsmålet om grænseoverskridende adgang til elektroniske beviser i en international sammenhæng. Frem for, at der skabes nye internationale retlige instrumenter for spørgsmål vedrørende cyberkriminalitet, foretrækker EU at opfordre alle lande til at udforme en passende national lovgivning og fortsætte samarbejdet inden for de eksisterende internationale rammer.

Den udbredte tilgængelighed af anonymiseringsværktøjer gør det lettere for kriminelle at skjule sig. "**Mørkenettet**"[70] har givet kriminelle nye muligheder for at få adgang til materiale, der skildrer seksuelt misbrug af børn, narkotika eller skydevåben, ofte med lav risiko for at blive opdaget[71]. Det er nu også en vigtig kilde til de værktøjer, der anvendes til cyberkriminalitet, f.eks. malware og hackingværktøjer. Kommissionen vil sammen med relevante berørte parter analysere nationale tilgange med henblik på at finde frem til nye løsninger. Europol bør lette og støtte efterforskninger på mørkenettet, vurdere trusler og bidrage til at fastlægge jurisdiktion og prioritere sager med stor risiko, og EU kan spille en ledende rolle ved at koordinere internationale tiltag[72].

Inden for cyberkriminalitet er misbrug af kreditkortoplysninger eller andre elektroniske betalingsmidler et område, som er i vækst. Betalingsoplysninger, der er fremskaffet via cyberangreb mod onlineforhandlere eller andre legitime virksomheder, sælges online og kan bruges af kriminelle til at begå svig[73]. Kommissionen forelægger et forslag om at øge den afskrækkende virkning ved hjælp af et **direktiv om bekæmpelse af svig og forfalskning i forbindelse med andre betalingsmidler end kontanter**[74]. Det tager sigte på at ajourføre de eksisterende regler på dette område og at styrke de retshåndhævende myndigheders evne til at bekæmpe denne form for kriminalitet.

Medlemsstaternes retshåndhævende myndigheders kapacitet til at efterforske cyberkriminalitet samt anklageres og retssystemets forståelse af cyberbaserede forbrydelser og efterforskningsmuligheder skal også forbedres Eurojust og Europol bidrager til opfyldelsen af dette mål og til forbedret koordinering i tæt samarbejde med specialiserede rådgivende grupper i Europols center til bekæmpelse af cyberkriminalitet samt nettene af ledere af

---

[68] Konventionen er den første internationale traktat om kriminalitet begået over internettet og andre computernet, som navnlig sætter ind over for krænkelser af ophavsret, computerrelateret svindel, børnepornografi og brud på netsikkerheden. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. I 2017 havde 55 regeringer enten ratificeret eller tiltrådt Europarådets konvention om cyberkriminalitet.

[69] Mandat for udarbejdelse af et udkast til 2. tillægsprotokol til Budapestkonventionen om cyberkriminalitet, T-CY (2017)3.

[70] Mørkenettet består af indhold i overlay-net, der anvender internettet, men hvortil der kræves specifik software, konfigurationer eller autorisation for at få adgang. Mørkenettet udgør en lille del af det dybe net, som er den del af nettet, der ikke indekseres af søgemaskiner.

[71] En bemærkelsesværdig undtagelse er den seneste fjernelse af to af de største ulovlige markeder på mørkenettet, AlphaBay og Hansa: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

[72] Europol spiller allerede en vigtig rolle på dette område. Et nyere eksempel kan findes her: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

[73] Udbyttet af svig er en vigtig indtægtskilde for organiserede kriminelle og muliggør således anden kriminel aktivitet såsom terrorisme, narkotikahandel og menneskehandel.

[74] COM(2017) 489.

cyberkriminalitetsenheder og anklagere, der er specialiseret i cyberkriminalitet. Kommissionen vil afsætte 10,5 mio. EUR til støtte til bekæmpelse af cyberkriminalitet, primært inden for rammerne af **programmet for Fonden for Intern Sikkerhed – Politi**. Uddannelse er et vigtigt element, og en række nyttige materialer er blevet udarbejdet af Den Europæiske Uddannelsesgruppe vedrørende Cyberkriminalitet. Disse bør nu udbredes til en bred kreds af fagfolk inden for retshåndhævelse med støtte fra Den Europæiske Unions Agentur for Uddannelse inden for Retshåndhævelse (Cepol).

3.3 Offentlig-privat samarbejde til bekæmpelse af cyberkriminalitet

Traditionelle retshåndhævelsesforanstaltningers effektivitet udfordres på grund af kendetegnene ved den digitale verden, der primært består af privatejet infrastruktur og mange forskellige aktører på tværs af forskellige jurisdiktioner. Som en følge heraf er samarbejde med den private sektor, herunder industrien og civilsamfundet, af grundlæggende betydning for de offentlige myndigheder, når de skal bekæmpe kriminalitet effektivt. I denne forbindelse er finanssektoren også af central betydning, og samarbejdet bør intensiveres. For eksempel bør den rolle, som finansielle efterretningsenheder[75] spiller i forbindelse med cyberkriminalitet, styrkes.

Nogle medlemsstater har allerede taget vigtige skridt. I Nederlandene arbejder finansielle institutioner og retshåndhævende myndigheder side om side for at imødegå onlinesvig og cyberkriminalitet i taskforcen for elektronisk kriminalitet. Det tyske kompetencecenter for bekæmpelse af cyberkriminalitet udgør det operationelle omdrejningspunkt for medlemmernes udveksling af oplysninger i tæt samarbejde med det tyske forbundspoliti og udvikling af foranstaltninger, der tager sigter på at sikre beskyttelse mod cyberkriminalitet. 16 medlemsstater[76] har oprettet ekspertisecentre for cyberkriminalitet for at fremme samarbejdet mellem retshåndhævende myndigheder, den akademiske verden og private partnere om udvikling og udveksling af bedste praksis, uddannelse og kapacitetsopbygning.
Kommissionen støtter oprettelsen af offentlig-private partnerskaber og samarbejdsmekanismer gennem specifikke projekter såsom Online Fraud Cyber Centre and Experts Network[77] og indførelse af en model og en standard for informationsudveksling med henblik på at analysere og mindske risiciene ved elektronisk kriminalitet og onlinesvindel.

I forbindelse med cyberkriminalitet bør private virksomheder kunne udveksle oplysninger om konkrete hændelser, herunder personoplysninger, med de retshåndhævende myndigheder under fuld overholdelse af reglerne for beskyttelse af personoplysninger. EU's databeskyttelsesreform, som vil træde i kraft i maj 2018, fastlægger et sæt fælles regler for de betingelser, hvorunder retshåndhævende myndigheder og private enheder kan samarbejde. Europa-Kommissionen vil samarbejde med Det Europæiske Databeskyttelsesråd og relevante berørte parter med henblik på at fastlægge bedste praksis på dette område og, hvor det er relevant, yde vejledning.

3.4 Intensivering af den politiske reaktion

[75] Finansielle efterretningsenheder fungerer som nationale centre for modtagelse og analyse af underretninger om mistænkelige transaktioner og andre oplysninger af relevans for hvidvaskning af penge, tilknyttede prædikatforbrydelser og finansiering af terrorisme samt for formidling af resultaterne af denne analyse.

[76] Østrig, Belgien, Bulgarien, Cypern, Tjekkiet, Estland, Frankrig, Tyskland, Grækenland, Irland, Litauen, Polen, Rumænien, Slovenien, Spanien og Det Forenede Kongerige.

[77] EU-OF2CEN-initiativet har til formål at muliggøre systematisk, EU-dækkende udveksling af oplysninger om internetsvindel mellem banker og retshåndhævende myndigheder med henblik på forebyggelse af udbetalinger til svindlere og pengekurerer og efterforskning og retsforfølgelse af de involverede gerningsmænd. Det medfinansieres af EU (programmet for Fonden for Intern Sikkerhed – Politi).

De nyligt vedtagne **rammer for EU's fælles diplomatiske reaktion på skadelige cyberaktiviteter**[78](den "cyberdiplomatiske værktøjskasse") fastlægger foranstaltningerne under den fælles udenrigs- og sikkerhedspolitik, herunder restriktive foranstaltninger, som kan anvendes til at styrke EU's reaktion på aktiviteter, der skader de politiske, sikkerhedsmæssige og økonomiske interesser. Rammerne udgør et vigtigt skridt i udviklingen af signalkapaciteten og den reaktive kapacitet på EU-plan og på medlemsstatsplan. De vil øge vores kapacitet til at placere ansvaret for ondsindede cyberaktiviteter med det formål at påvirke adfærden hos potentielle gerningsmænd, samtidig med at der tages hensyn til behovet for at sikre hensigtsmæssige reaktioner. Det er en suveræn politisk afgørelse baseret på efterretning fra alle kilder at tilskrive en statslig eller ikkestatslig aktør ansvar. Rammerne gennemføres for nærværende i samarbejde med medlemsstaterne og vil blive videreført under nøje hensyntagen til planen for reaktion på væsentlige cyberhændelser[79]. Det situationskendskab, der er nødvendigt for anvendelsen af foranstaltninger inden for rammerne, bør samles, analyseres og deles af INTCEN[80] i tæt samarbejde med medlemsstaterne og EU's institutioner.

3.5 Opbygning af afskrækkelsesforanstaltninger inden for cybersikkerhed gennem medlemsstaternes forsvarskapacitet

Medlemsstaterne er allerede i gang med at udvikle cyberforsvarskapacitet. På grund af udviskningen af grænserne mellem cyberforsvar og cybersikkerhed og muligheden for dobbelt anvendelse af værktøjer og teknologier samt de store forskelle mellem medlemsstaternes tilgange er EU godt placeret til at bidrage til at fremme synergieffekter mellem den militære og den civile indsats[81].

De medlemsstater, som har mere avancerede cybersikkerhedskapaciteter og er villige til at samle dem, kunne, med støtte fra den højtstående repræsentant, Kommissionen og Det Europæiske Forsvarsagentur, overveje at lade cybersikkerhed indgå i rammerne for et "permanent struktureret samarbejde" (PESCO). Dette kunne bygge på det arbejde, der er beskrevet ovenfor, for at fremme EU's industrielle kapacitet og strategiske autonomi. EU kan også fremme interoperabilitet, bl.a. ved at lette kapacitetsudvikling, koordinering af uddannelse og standardiseringsarbejde inden for området dobbelt anvendelse.

Der skal også gøres fuld brug af den fælles ramme for at imødegå hybride trusler, som ofte omfatter cyberangreb, navnlig gennem EU's analyseenhed for hybride trusler (EU Hybrid Fusion Cell) og det nyligt oprettede Europæiske Center for Imødegåelse af Hybride Trusler i Helsinki, hvis formål er at tilskynde til strategisk dialog og udføre forskning og analyse.

EU vil igen fokusere på EU's cyberforsvarspolitiske ramme fra 2014[82] som et redskab til yderligere integrering af cybersikkerhed og -forsvar i den fælles sikkerheds- og forsvarspolitik (FSFP). FSFP-missionernes og -operationernes egen cyberrobusthed er af afgørende betydning: Der vil blive udviklet standardiserede procedurer og teknisk kapacitet, der kan støtte både civile og militære missioner og operationer samt deres respektive strukturer for planlægning og gennemførelseskapacitet og EU-Udenrigstjenestens udbydere af informationsteknologi. Med henblik på at fremme medlemsstaternes samarbejde og bedre styre EU's indsats på dette område vil Det Europæiske Forsvarsagentur og EU-

[78] http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/.
[79] C(2017) 6100.
[80] JOIN(2016) 018 final.
[81] EU opfatter cyberspace som et operationsområde i lighed med land, luft og hav. Cyberforsvarsindsatsen omfatter også beskyttelsen og robustheden af rumaktiver og dertil knyttede jordbaserede infrastrukturer.
[82] www.consilium.europa.eu/en/workarea/downloadasset.aspx?id=40802190515.

Udenrigstjenesten i samarbejde med Kommissionens tjenestegrene lette strategisk samarbejde mellem medlemsstaternes beslutningstagere inden for cyberforsvar. EU vil også støtte udviklingen af europæiske cybersikkerhedsløsninger som led i sin indsats til fordel for det europæiske forsvars teknologiske og industrielle basis. Dette omfatter også fremme af regionale kompetenceklynger inden for cybersikkerhed og -forsvar.

Kommissionens tjenestegrene vil i tæt samarbejde med EU-Udenrigstjenesten, medlemsstaterne og andre relevante EU-organer senest i 2018 etablere **en platform for uddannelse inden for cyberforsvar** for at løse de nuværende problemer vedrørende mangel på færdigheder inden for cyberforsvar. Dette vil supplere det arbejde, der udføres af Det Europæiske Forsvarsagentur på dette område, og bidrage til at afhjælpe den nuværende mangel på færdigheder inden for cybersikkerhed og cyberforsvar.

Nøgleaktioner

- Et kommissionsinitiativ om grænseoverskridende adgang til elektroniske beviser (primo 2018).
- Hurtig vedtagelse i Europa-Parlamentet og Rådet af det foreslåede direktiv om bekæmpelse af svig og forfalskning i forbindelse med andre betalingsmidler end kontanter.
- Indførelse af krav om IPv6 inden for offentlige indkøb, forskning og projektfinansiering i EU. Frivillige aftaler mellem medlemsstaterne og internetudbyderne for at øge udbredelsen af IPv6.
- Et revideret/udvidet fokus i Europol på cyberkriminaltektnik og overvågning af mørkenettet.
- Gennemførelsen af rammerne for EU's fælles diplomatiske reaktion på skadelige cyberaktiviteter.
- Øget finansiel støtte til nationale og tværnationale projekter, der styrker strafferetten relateret til cyberspace.
- En cybersikkerhedsrelateret uddannelsesplatform for at gøre noget ved den nuværende mangel på færdigheder inden for cybersikkerhed og cyberforsvar i 2018.

4. STYRKELSE AF INTERNATIONALT SAMARBEJDE OM CYBERSIKKERHED

Med udgangspunkt i EU's kerneværdier og grundlæggende rettigheder såsom ytringsfrihed og retten til privatlivets fred og beskyttelse af personoplysninger samt fremme af et åbent, frit og sikkert cyberspace er EU's cybersikkerhedspolitik udformet til at håndtere udfordringen vedrørende fremme af global cyberstabilitet, som er under stadig udvikling, og til at bidrage til Europas strategiske uafhængighed i cyberspace.

4.1 Cybersikkerhed og eksterne forbindelser

Der findes dokumentation, der tyder på, at mennesker i hele verden peger på cyberangreb fra andre lande som nogle af de største trusler mod den nationale sikkerhed[83]. Da der er tale om en global trussel, er opbygning og vedligeholdelse af robuste alliancer og partnerskaber med tredjelande afgørende for forebyggelse af og afskrækkelse fra cyberangreb, som er af stadig mere central betydning for den internationale stabilitet og sikkerhed. EU vil prioritere udarbejdelsen af en strategisk ramme for konfliktforebyggelse og stabilitet i cyberspace i sine bilaterale, regionale og multilaterale kontakter med mange forskellige aktører.

[83] Spring 2017 Global Attitudes Survey, Pew Research Centre.

EU går stærkt ind for holdningen om, at folkeretten og FN-pagten skal gælde for cyberspace. Som et supplement til bindende folkeret støtter EU de frivillige ikke-bindende standarder, regler og principper for ansvarlig statslig adfærd, som er blevet formuleret af FN's gruppe af regeringseksperter[84]. EU tilskynder også til udvikling og gennemførelse af regionale tillidsskabende foranstaltninger, både i Organisationen for Sikkerhed og Samarbejde i Europa og andre fora.

På bilateralt plan vil cyberrelaterede dialoger[85] blive videreudviklet og suppleret med bestræbelser på at fremme samarbejde med tredjelande med henblik på at styrke principperne om fornøden omhu og staternes ansvarlighed i cyberspace. EU vil prioritere internationale sikkerhedsspørgsmål i cyberspace i sine internationale forbindelser, samtidig med at det sikres, at cybersikkerhed ikke bliver et påskud for markedsbeskyttelse og begrænsning af de grundlæggende rettigheder og friheder, herunder ytringsfrihed og adgang til information. En samlet tilgang til cybersikkerhed kræver respekt for menneskerettighederne, og EU vil fortsat værne om sine grundlæggende værdier på globalt plan med udgangspunkt i EU's retningslinjer vedrørende menneskerettigheder med hensyn til frihed på nettet[86]. I den forbindelse understreger EU betydningen af, at alle berørte parter inddrages i forvaltningen af internettet.

Kommissionen har også fremsat forslag[87] om at modernisere EU's eksportkontrol, herunder indførelse af kontrol af eksport af kritisk cyberovervågningsteknologi, som kunne føre til overtrædelse af menneskerettighederne eller misbruges mod EU's egen sikkerhed, og vil intensivere dialogerne med tredjelande om at fremme global konvergens og ansvarlig adfærd inden for dette område.

4.2 Kapacitetsopbygning inden for cybersikkerhed

Global cyberstabilitet afhænger af evnen på lokalt og nationalt plan til at forebygge og reagere på cyberhændelser samt efterforske og retsforfølge i sager om cyberkriminalitet. Støtte til de nationale bestræbelser på at opbygge modstandsdygtighed i tredjelande vil øge cybersikkerhedsniveauet på globalt plan, med positive virkninger for EU. Imødegåelse af cybertrusler under hastig udvikling vil forudsætte uddannelse, en indsats for at udvikle politikker og lovgivning samt effektive IT-beredskabsenheder og cyberkriminalitetsenheder i alle lande i verden.

Siden 2013 har Unionen været førende med hensyn til kapacitetsopbygning inden for cybersikkerhed og har systematisk skabt sammenhæng mellem denne indsats og dens udviklingssamarbejde. EU vil fortsat fremme en rettighedsbaseret kapacitetsopbygningsmodel i overensstemmelse med tilgangen i Digital4Development[88]. Kapacitetsopbygning vil være højest prioriteret i EU's nabolande og udviklingslande, der oplever hastigt voksende konnektivitet og en hurtig udvikling i trusselssituationen. EU's indsats vil være et supplement til EU's udviklingsdagsorden i lyset af 2030-dagsordenen for bæredygtig udvikling og den overordnede indsats for opbygning af institutionel kapacitet.

For at forbedre EU's evne til at mobilisere sin kollektive ekspertise til støtte for denne kapacitetsopbygning bør der etableres et særligt cyberkapacitetsopbygningsnet på EU-plan,

---

84 A/68/98 og A/70/174.

85 I september 2017 gennemførte EU cyberrelaterede dialoger med USA, Kina, Japan, Republikken Korea og Indien.

86 EU Human Rights Guidelines on Freedom of Expression Online and Offline.

87 COM(2016) 616.

88 SWD(2017) 157.

som samler EU-Udenrigstjenesten, medlemsstaternes cybermyndigheder, EU-agenturerne, Kommissionens tjenestegrene, den akademiske verden og civilsamfundet. Der vil blive udarbejdet retningslinjer for cyberkapacitetsopbygningsnettet på EU-plan for at bidrage til bedre politisk vejledning og prioritering af EU's indsats i tredjelande.

EU vil også arbejde sammen med andre donorer på dette område for at undgå dobbeltarbejde og fremme en mere målrettet kapacitetsopbygning i forskellige regioner.

4.3 Samarbejde mellem EU og NATO

Med udgangspunkt i de betydelige fremskridt, der allerede er opnået, vil EU uddybe EU's og NATO's samarbejde om cybersikkerhed, hybride trusler og forsvar som omhandlet i den fælles erklæring af 8. juli 2016[89]. Prioriteterne omfatter fremme af interoperabilitet gennem sammenhængende cyberforsvarskrav og -standarder, styrket samarbejde om uddannelse og øvelser samt harmonisering af uddannelseskrav.

EU og NATO vil også fremme forsknings- og innovationssamarbejde om cyberforsvar og bygge videre på den eksisterende tekniske ordning om udveksling af oplysninger om cybersikkerhed mellem deres respektive cybersikkerhedsorganer[90]. De seneste fælles bestræbelser på at imødegå hybride trusler, navnlig samarbejdet mellem EU's analyseenhed for hybride trusler og NATO's afdeling for analyse af hybride trusler, bør udvikles yderligere for at styrke modstandsdygtigheden og reaktionen på cyberkriser. Yderligere samarbejde mellem EU og NATO vil blive fremmet gennem cyberforsvarsøvelser med inddragelse af EU-Udenrigstjenesten og andre EU-organer og NATO's relevante modstykker, herunder NATO's cyberforsvarscenter i Tallinn. For første gang vil NATO og EU gennemføre parallelle og koordinerede øvelser som reaktion på et hybridscenarie med NATO i spidsen i 2017 og EU i spidsen på tilsvarende vis i 2018. Den næste rapport om samarbejdet mellem EU og NATO, som skal forelægges de respektive råd i december 2017, vil give mulighed for at overveje mulighederne for at udvide samarbejdet yderligere, navnlig ved at sikre fælles, sikre og robuste kommunikationsmidler mellem alle relevante institutioner og aktører, herunder ENISA.

Nøgleaktioner

- Fremme af den strategiske ramme for konfliktforebyggelse og stabilitet i cyberspace.
- Udvikling af et nyt kapacitetsopbygningsnet for at støtte tredjelandenes evne til at imødegå cybertrusler og retningslinjer for cybersikkerhedskapacitetsopbygningsnettet på EU-plan for bedre at kunne prioritere EU's indsats.
- Yderligere samarbejde mellem EU og NATO, herunder deltagelse i parallelle og koordinerede øvelser og styrket interoperabilitet mellem cybersikkerhedsstandarderne.

5. KONKLUSION

EU's cyberberedskab er af central betydning for både det digitale indre marked og vores sikkerheds- og forsvarsunion. At styrke den europæiske cybersikkerhed og imødegå trusler mod både civile og militære mål er en nødvendighed.

Det kommende digitale topmøde, som arrangeres af det estiske rådsformandskab den 29. september 2017, vil være en lejlighed til at vise en fælles vilje til at give cybersikkerhed en central placering i EU som et digitalt samfund. Som en del af denne fælles forpligtelse

[89] http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/.
[90] CERT-EU og NATO's Computer Incident Response Capability (NCIRC).

opfordrer Kommissionen medlemsstaterne til at give tilsagn om, hvordan de agter at handle på områder, hvor de har det primære ansvar. Dette bør omfatte styrkelse af cybersikkerhed gennem:

- Sikring af fuld og effektiv gennemførelse af NIS-direktivet senest den 9. maj 2018 samt de ressourcer, som er nødvendige for, at de offentlige myndigheder med ansvar for cybersikkerhed kan udføre deres opgaver effektivt.
- Anvendelse af de samme regler på offentlige myndigheder i betragtning af den rolle, de spiller i samfundet og økonomien som helhed.
- Cybersikkerhedsrelateret uddannelse i den offentlige administration.
- Prioritering af cyberovervågning i oplysningskampagner og herunder cybersikkerhed som en del af akademiske og erhvervsfaglige uddannelsesprogrammer.
- Anvendelse af initiativer vedrørende det "permanente strukturerede samarbejde" (PESCO) og Den Europæiske Forsvarsfond til støtte for udvikling af cyberforsvarsprojekter.

Denne fælles meddelelse har beskrevet omfanget af udfordringen og den række af foranstaltninger, som EU kan træffe. Vi har brug for et Europa, der er modstandsdygtigt, og som kan beskytte borgerne effektivt ved at foregribe mulige cybersikkerhedshændelser gennem opbygning af en stærk beskyttelse i sine strukturer og sin adfærd og gennem hurtig overvindelse af eventuelle cyberangreb samt hurtig afskrækkelse af de ansvarlige. I denne meddelelse beskrives der målrettede foranstaltninger, som yderligere vil styrke EU's cybersikkerhedsstrukturer og -kapacitet på koordineret vis i fuldt samarbejde med medlemsstaterne og de berørte EU-strukturer og under hensyntagen til disses kompetencer og ansvarsområder. Gennemførelsen heraf vil give et klart signal om, at EU og medlemsstaterne vil arbejde sammen om at indføre en standard for cybersikkerhed modsvarende de stadig større udfordringer, som Europa står over for i dag.