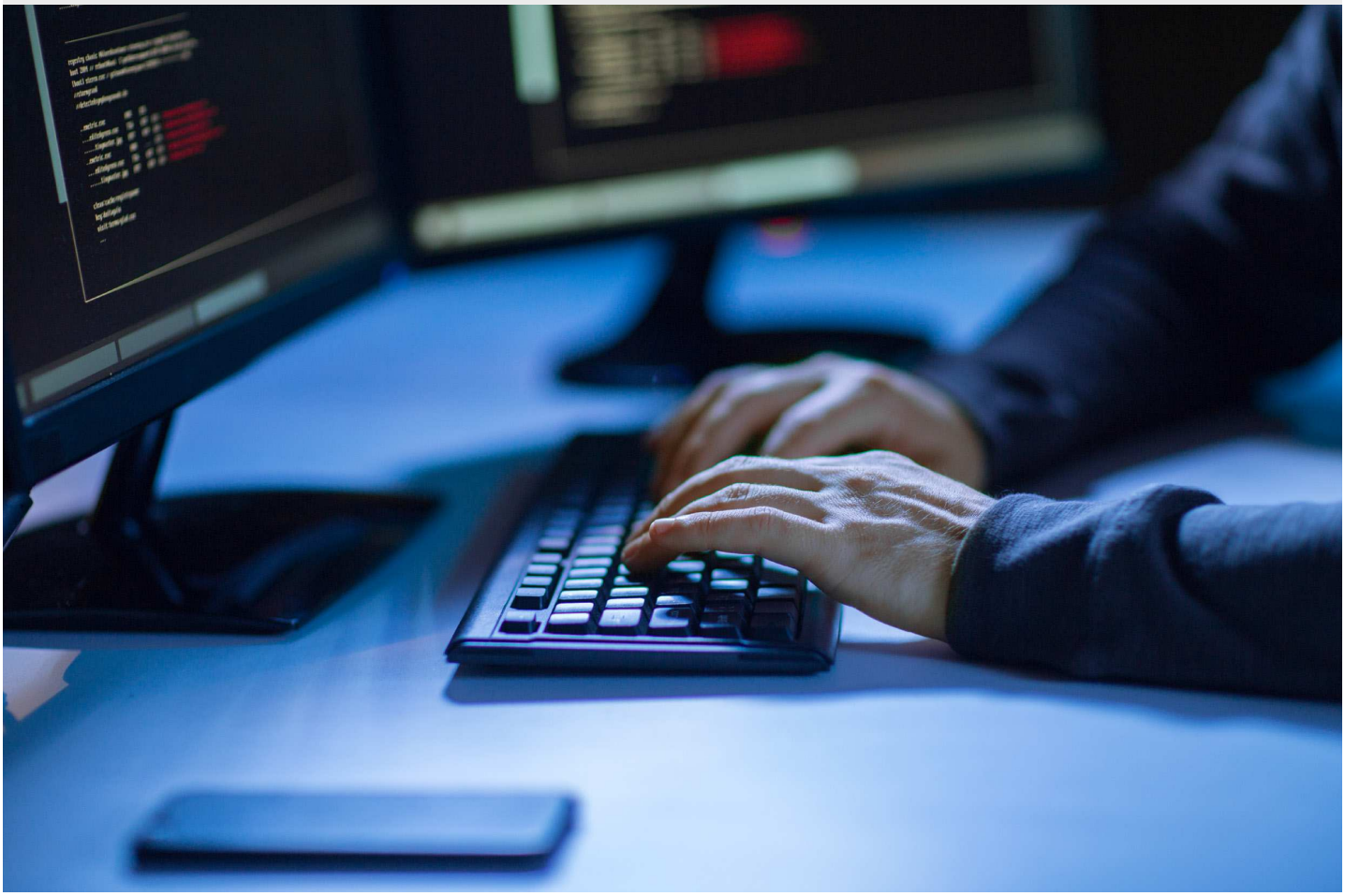
DEN EUROPÆISKE REVISIONSRET

DA 2019

Udfordringer for en effektiv cybersikkerhedspolitik i EU

Briefingpapir

Marts 2019



Om briefingpapiret:

Formålet med dette briefingpapir, som ikke er en revisionsberetning, er at give et overblik over EU's komplekse politiske landskab for cybersikkerhed og identificere de vigtigste udfordringer for en effektiv politikgennemførelse. Briefingpapiret omhandler net- og informationssikkerhed, cyberkriminalitet, cyberforsvar og desinformation. Det indeholder også oplysninger om det fremtidige revisionsarbejde på området.

Vi baserede vores analyse på dokumentgennemgang af offentligt tilgængelige oplysninger i officielle dokumenter, positionspapirer og tredjepartsundersøgelser. Vores arbejde i marken blev udført mellem april og september 2018, og der er taget højde for udviklingen frem til december 2018. Vi supplerede vores arbejde med en spørgeundersøgelse henvendt til medlemsstaternes overordnede revisionsorganer og interview med centrale interessenter fra EU-institutionerne og repræsentanter for den private sektor.

De udfordringer, vi identificerede, er opdelt i fire brede klynger: i) den politiske ramme, ii) finansiering og udgifter, iii) opbygning af cyberrobusthed og iv) effektiv reaktion på cyberhændelser. Det er bydende nødvendigt at opnå et højere cybersikkerhedsniveau i EU. Derfor afslutter vi hvert kapitel med en række ideer til yderligere refleksion blandt politiske beslutningstagere, lovgivere og aktører.

Vi vil gerne takke for den konstruktive feedback, vi har modtaget fra Kommissionens tjenestegrene, Tjenesten for EU's Optræden Udadtil, Rådet for Den Europæiske Union, ENISA, Europol, den europæiske organisation for cybersikkerhed og medlemsstaternes overordnede revisionsorganer.

Indhold

Resumé

I Teknologien åbner en helt ny verden af muligheder, og nye produkter og tjenester bliver integrerede dele af vores dagligdag. Til gengæld stiger risikoen for at blive offer for cyberkriminalitet eller et cyberangreb, og de dermed forbundne samfundsmæssige og økonomiske konsekvenser fortsætter med at vokse. Den indsats, som EU siden 2017 har gjort for at fremskynde bestræbelserne på at styrke cybersikkerheden og sin egen digitale autonomi, kommer derfor på et afgørende tidspunkt.

II Dette briefingpapir, som ikke er en revisionsberetning, men er baseret på offentligt tilgængelige oplysninger, tager sigte på at give et overblik over et komplekst og broget politisk landskab og identificere de vigtigste udfordringer for en effektiv politikgennemførelse. Vores briefingpapir omhandler EU's cybersikkerhedspolitik såvel som cyberkriminalitet og cyberforsvar og beskriver også bestræbelser på at bekæmpe desinformation. De udfordringer, vi identificerede, er opdelt i fire brede klynger: i) den politiske og lovgivningsmæssige ramme, ii) finansiering og udgifter, iii) opbygning af cyberrobusthed og iv) effektiv reaktion på cyberhændelser. Hvert kapitel indeholder en række refleksionspunkter vedrørende de gennemgåede udfordringer.

Den politiske og lovgivningsmæssige ramme

III Udvikling af tiltag, der er på linje med de brede mål i EU's strategi for cybersikkerhed om at blive verdens sikreste digitale miljø, er en udfordring, da der mangler målbare målsætninger og kun findes sparsomme pålidelige oplysninger. Resultater måles sjældent, og kun få politikområder er blevet evalueret. En central udfordring er derfor at **sikre fornuftig ansvarliggørelse og evaluering** ved at foretage et skift i retning af en resultatorienteret kultur med etablerede evalueringspraksis.

IV Den lovgivningsmæssige ramme er fortsat ufuldstændig. **Huller i og uensartet gennemførelse af EU-retten** kan gøre det vanskeligt for lovgivningen at nå sit fulde potentiale.

Finansiering og udgifter

V Det er en udfordring at **tilpasse investeringsniveauerne til målene**: Dette kræver ikke blot opskalering af de samlede investeringer i cybersikkerhed - som har været lave og fragmenterede på EU-plan - men også opskalering af deres virkninger, navnlig ved at udnytte resultaterne af forskningsudgifter bedre og sikre en effektiv målretning mod og finansiering af nystartede virksomheder.

VI Det er afgørende for EU og dets medlemsstater at **have et klart overblik over EU's udgifter** for at vide, hvilke huller der skal lukkes for at nå de fastsatte mål. Da der ikke er et særligt EU-budget til at finansiere strategien for cybersikkerhed, er der ikke et tydeligt billede af, hvilke midler der anvendes, og hvor de anvendes.

VII I en tid med øgede politiske prioriteter på sikkerhedsområdet, kan **ressourcemæssige begrænsninger i EU's agenturer for cyberspørgsmål** forhindre EU i at nå sit ambitionsniveau. For at tackle denne udfordring må der findes metoder til at tiltrække og fastholde talenter.

Opbygning af cyberrobusthed

VIII Der er mange svagheder i forvaltningen af cybersikkerhed i såvel den offentlige som den private sektor i EU samt på internationalt plan. Dette vanskeliggør det internationale samfunds evne til at reagere på og begrænse cyberangreb og underminerer en sammenhængende tilgang på EU-plan. Udfordringen består derfor i at **styrke forvaltningen af cybersikkerhed**.

IX Det er vigtigt at **øge kompetence- og bevidsthedsniveauet** i alle sektorer og på alle niveauer i samfundet, da der i stigende grad mangler cybersikkerhedskompetencer på verdensplan. Omfanget af EU-dækkende standarder for uddannelse, certificering og cyberrisikovurdering er på nuværende tidspunkt begrænset.

X Et tillidsgrundlag er afgørende for at styrke den overordnede cyberrobusthed. Kommissionen har vurderet, at koordineringen generelt stadig er utilstrækkelig. Det er fortsat en udfordring at **forbedre informationsudvekslingen og koordineringen** mellem den offentlige og den private sektor.

Effektiv reaktion på cyberhændelser

XI De digitale systemer er blevet så komplekse, at det er umuligt at forhindre alle angreb. Denne udfordring tackles gennem **hurtig detektering og reaktion**. Cybersikkerhed er imidlertid endnu ikke fuldt ud integreret i de nuværende koordineringsmekanismer for kriseberedskab på EU-plan, hvilket potentielt begrænser EU's kapacitet til at reagere på væsentlige, grænseoverskridende cyberhændelser.

XII **Beskyttelse af kritisk infrastruktur og kritiske samfundsmæssige funktioner** er afgørende. Risikoen for indblanding i valgprocesser og for desinformationskampagner er en stor udfordring.

XIII De nuværende udfordringer, som EU og det internationale samfund står over for i forbindelse med cybertrusler, kræver et fortsat engagement i og en vedvarende loyalitet over for EU's kerneværdier.

Indledning

01 Teknologien åbner en helt ny verden af muligheder. Efterhånden som nye produkter og tjenester kommer til, bliver de integrerede dele af vores dagligdag. Vores teknologiske afhængighed stiger imidlertid med hver ny udvikling, og det samme gør vigtigheden af cybersikkerhed. Jo flere personoplysninger, vi lægger ud online, og jo mere forbundne vi bliver elektronisk, jo større er sandsynligheden for at blive offer for en form for cyberkriminalitet eller cyberangreb.

Hvad er cybersikkerhed?

02 Der er ikke nogen universelt anerkendt standarddefinition af cybersikkerhed[1]. Groft sagt er det alle de sikkerhedsforanstaltninger, der er truffet for at beskytte informationssystemer og deres brugere mod uautoriseret adgang, angreb og skader for at sikre oplysningernes fortrolighed, integritet og tilgængelighed.

03 Cybersikkerhed omfatter forebyggelse og detektering af cyberhændelser, reaktion på dem og efterfølgende genopretning. Hændelser kan være tilsigtede eller utilsigtede og f.eks. spænde fra hændelig spredning af oplysninger til angreb på virksomheder og kritisk infrastruktur, tyveri af personoplysninger og endog indblanding i demokratiske processer. De kan alle få vidtrækkende skadelige konsekvenser for enkeltpersoner, organisationer og samfund.

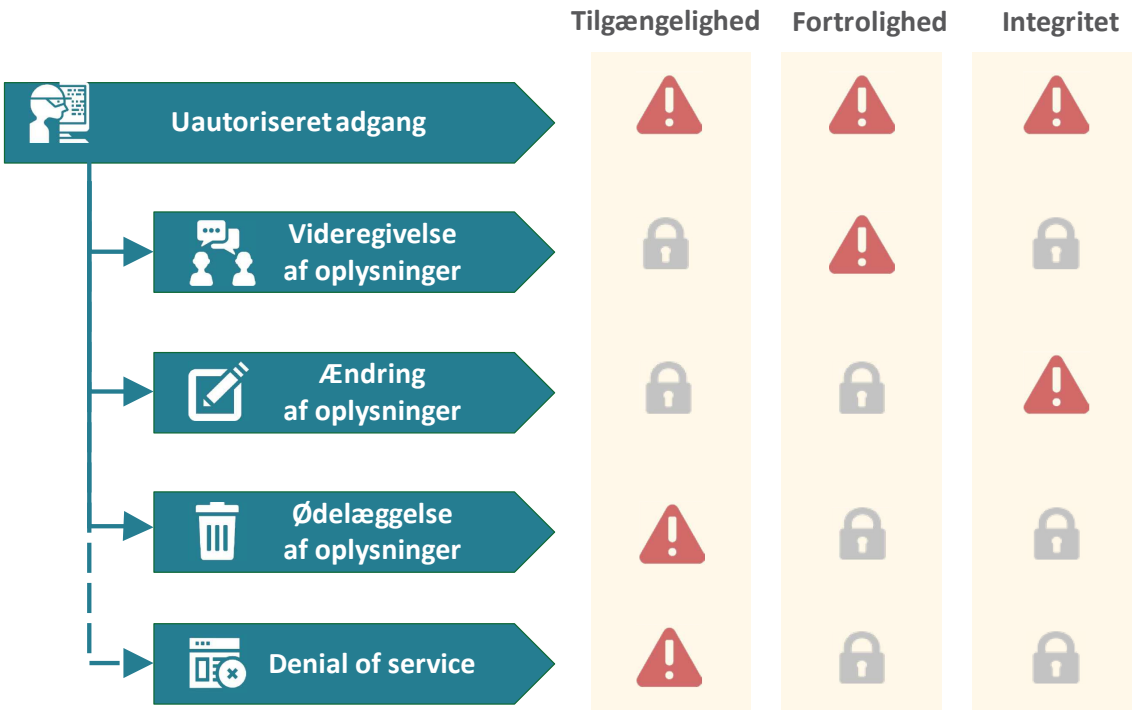
04 Som begreb anvendt i forbindelse med EU-politik er cybersikkerhed ikke begrænset til net- og informationssikkerhed. Det omfatter enhver ulovlig aktivitet, der indebærer brug af digitale teknologier i cyberspace. Det kan derfor dække cyberkriminalitet, f.eks. angreb med computervirus og svig med kontantløse betalinger, og omfatte både systemer og indhold - som det er tilfældet med udbredelsen af materiale online om seksuelt misbrug af børn. Det kan også omfatte desinformationskampagner, der har til formål at påvirke onlinedebatter, og formodet indblanding i valg. Ifølge Europol er der endvidere konvergens mellem cyberkriminalitet og terrorisme[2].

05 Forskellige aktører - herunder stater, kriminelle grupper og hacktivister - står bag cyberhændelser og er drevet af forskellige motiver. Konsekvenserne af disse hændelser mærkes på nationalt, europæisk og endog globalt plan. Internettets immaterielle og stort set grænseløse karakter og de anvendte værktøjer og taktikker

gør det imidlertid ofte vanskeligt at definere, hvem der står bag et angreb (det såkaldte "placeringsproblem").

06 De mange former for cybersikkerhedstrusler kan klassificeres i henhold til, hvad de gør ved oplysninger - videregivelse, ændring, ødelæggelse eller nægtet adgang - eller de grundlæggende informationssikkerhedsprincipper, de overtræder, jf. ***figur 1*** nedenfor. Nogle eksempler på angreb gives i ***tekstboks 1***. Efterhånden som angrebene på informationssystemer bliver mere sofistikerede, bliver vores forsvarsmekanismer mindre effektive[3].

Figur 1 - Trusselstyper og de sikkerhedsprincipper, der bringes i fare



Kilde: Revisionsretten. Tilpasset fra en undersøgelse i Europa-Parlamentet[4]. Hængelås = ingen konsekvenser for sikkerheden, udråbstegn = sikkerheden i fare

Tekstboks 1

Former for cyberangreb

Hver gang en ny enhed tilsluttes internettet eller forbindes til andet udstyr, vokser den såkaldte "angrebsflade" inden for cybersikkerhed. Den eksponentielle vækst i tingenes internet, skyen, big data og digitaliseringen af industrien ledsages af en øget risiko for sårbarhed, hvilket giver ondsindede aktører mulighed for at gå efter flere ofre. De mange forskellige former for angreb og deres stigende sofistikeringsgrad gør det virkelig svært at følge med[5].

Malware (skadelig software) er udviklet til at skade udstyr eller net. Det kan omfatte virus, trojanske heste, ransomware, orme, adware og spyware. **Ransomware** krypterer data for at forhindre brugerne i at få adgang til deres filer, indtil der betales en løsesum, typisk i kryptovaluta, eller der udføres en bestemt handling. Ifølge Europol dominerer angreb med ransomware over hele linjen, og antallet af ransomwaretyper er eksploderet i de seneste år. **Distribueret Denial of Service**-angreb (DDoS-angreb), der gør tjenester eller ressourcer utilgængelige ved at overbelaste dem med flere forespørgsler, end de kan håndtere, stiger også, og i 2017 var en tredjedel af alle organisationer udsat for denne form for angreb[6].

Brugere kan manipuleres til ubevidst at udføre en handling eller videregive fortrolige oplysninger. Denne metode kan anvendes til datatyveri eller cyberspionage og er kendt som **social engineering**. Dette kan foregå på forskellige måder, men der anvendes oftest **phishing**, hvor e-mail, der ser ud til at komme fra pålidelige kilder, narrer brugerne til at afsløre oplysninger eller klikke på link, der vil inficere deres udstyr med downloadet malware. Mere end halvdelen af medlemsstaterne rapporterede om efterforskninger af netangreb[7].

Den mest ondsindede af alle truslerne er nok **avancerede vedholdende trusler**. Sofistikerede angribere foretager langsigtet overvågning og tyveri af data og har somme tider også ødelæggende mål for øje. Formålet er at forblive under radaren så længe som muligt uden at blive opdaget. Avancerede vedholdende trusler er ofte statstilknyttede og rettet navnlig mod følsomme sektorer som f.eks. teknologi, forsvar og kritisk infrastruktur. Cyberspionage anslås at tegne sig for mindst en fjerdedel af alle cyberhændelser og størstedelen af omkostningerne[8].

Hvor alvorligt er problemet?

07 Da der mangler pålidelige oplysninger, er det vanskeligt at måle virkningen af at være dårligt forberedt på at cyberangreb. De økonomiske konsekvenser af cyberkriminalitet er femdoblet mellem 2013 og 2017[9] og har ramt regeringer og både store og små virksomheder. Den forventede stigning i forsikringspræmier på cyberområdet fra 3 milliarder euro i 2018 til 8,9 milliarder euro i 2020 afspejler denne tendens.

08 De finansielle konsekvenser af cyberangreb bliver fortsat større, men der er en alarmerende forskel mellem omkostningerne ved at iværksætte et angreb og omkostningerne ved at forebygge, efterforske og udbedre skaderne. Et DDoS-angreb kan f.eks. koste så lidt som 15 EUR om måneden at udføre, men de tab, som den ramte virksomhed lider, herunder af omdømmemæssig karakter, er betydeligt højere[10].

09 Selv om 80 % af virksomhederne i EU oplevede mindst én cybersikkerhedshændelse i 2016[11], er anerkendelsen af risici stadig alarmerende lav. Blandt virksomheder i EU har 69 % ingen eller kun en grundlæggende forståelse af deres eksponering over for cybertrusler[12], og 60 % har aldrig anslået det potentielle økonomiske tab[13]. Ifølge en global undersøgelse vil en tredjedel af organisationerne desuden hellere betale løsesum til hackeren end investere i informationssikkerhed[14].

10 De verdensomspændende angreb med ransomwaren *Wannacry* og wipermalwaren *NotPetya* i 2017 berørte tilsammen mere end 320 000 personer i omkring 150 lande[15]. Disse angreb førte til en slags global opvågning til det trusselsbillede, som cyberangreb udgør, og skabte nyt momentum for at integrere cybersikkerhed i den generelle politikudformning. Endvidere mener 86 % af EU's borgere nu, at risikoen for at blive offer for cyberkriminalitet er stigende[16].

EU's indsats på cybersikkerhedsområdet

11 I 2001 blev EU observatør i Europarådets komité for konventionen om IT-kriminalitet[17] (Budapestkonventionen). Siden da har EU udformet politikker, vedtaget lovgivning og brugt penge med henblik på at styrke sin cyberrobusthed. På baggrund af det stigende antal væsentlige cyberangreb og -hændelser er aktiviteterne taget til siden 2013, jf. ***figur 2***. Samtidig har medlemsstaterne vedtaget (og i nogle tilfælde allerede ajourført) deres første nationale strategier for cybersikkerhed.

12 De vigtigste EU-aktører med ansvar for cybersikkerhed er beskrevet i ***tekstboks 2*** og ***bilag I***.

Tekstboks 2

Hvem er involveret?

Europa-Kommissionen ønsker at øge cybersikkerhedskapaciteten og samarbejdet, styrke EU som cybersikkerhedsaktør og integrere cybersikkerhed i andre EU-politikker. De vigtigste generaldirektorater (GD'er), der er ansvarlige for cybersikkerhed, er GD **CNECT** (cybersikkerhed) og GD **HOME** (cyberkriminalitet), som er ansvarlige for henholdsvis det digitale indre marked og sikkerhedsunionen. GD **DIGIT** er ansvarligt for IT-sikkerheden i Kommissionens egne systemer.

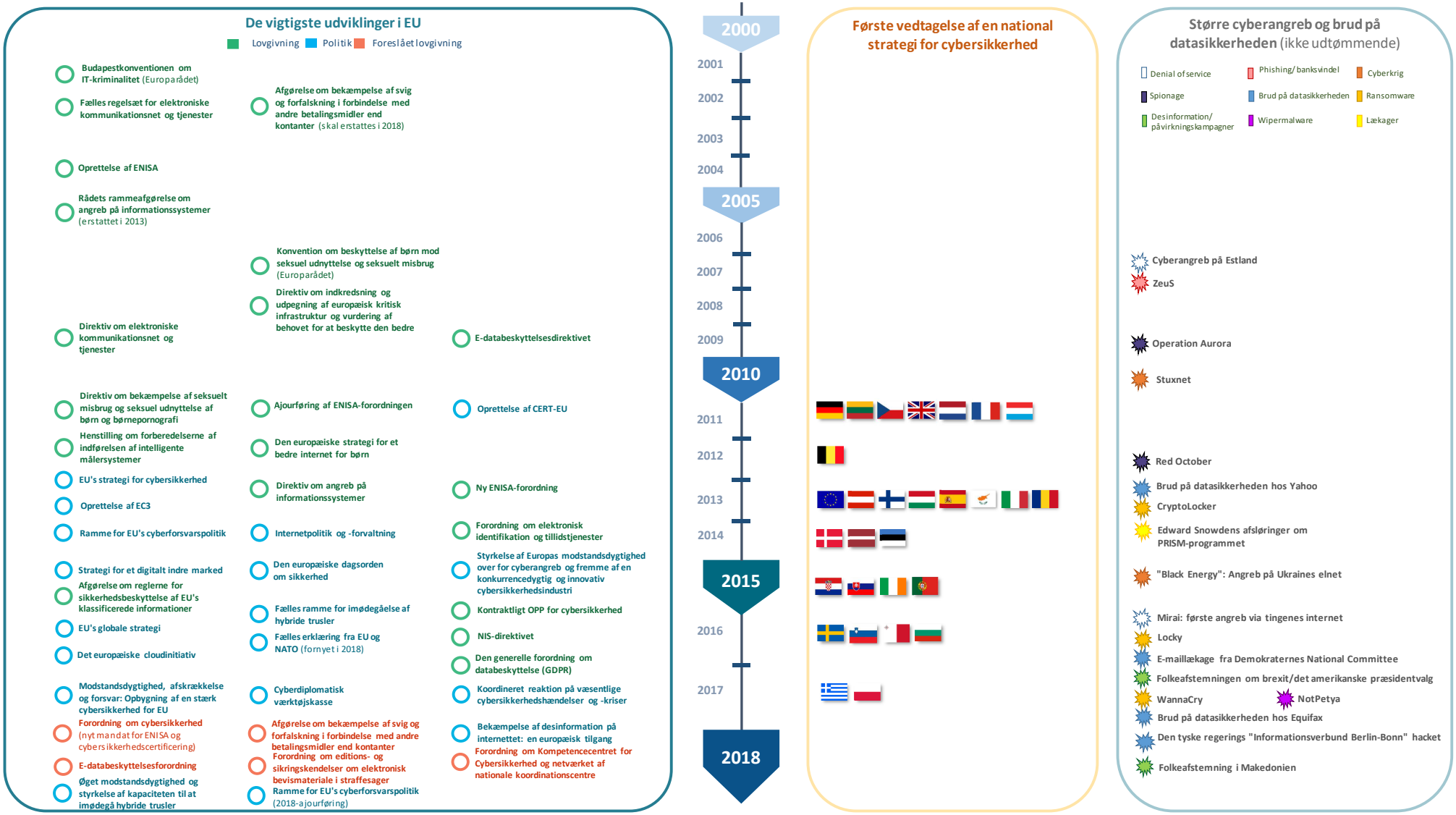
En række EU-agenturer støtter Kommissionen, navnlig **ENISA** (Den Europæiske Unions Agentur for Net- og Informationssikkerhed), som er EU's agentur for cybersikkerhed - et overvejende rådgivende organ, der støtter politikudvikling, kapacitetsopbygning og bevidstgørelse. Europols Europæiske Center for Bekæmpelse af Cyberkriminalitet (**EC3**) blev oprettet for at styrke EU's retshåndhævelsesindsats på cyberkriminalitetsområdet. Hos Kommissionen er der en IT-beredskabsenhed (**CERT-EU**), der støtter alle Unionens institutioner, organer og agenturer.

Tjenesten for EU's Optræden Udadtil (EU-Udenrigstjenesten) er førende hvad angår cyberforsvar, cyberdiplomati og strategisk kommunikation og har efterretnings- og analysecentre. **Det Europæiske Forsvarsagentur** (EDA) har til formål at udvikle cyberforsvarskapaciteten.

Medlemsstaterne er primært ansvarlige for deres egen cybersikkerhed og handler på EU-plan gennem **Rådet**, der har mange koordinations- og informationsudvekslingsorganer (heriblandt Den Horisontale Gruppe vedrørende Cyberspørgsmål). **Europa-Parlamentet** er medlovgiver.

Organisationer i den private sektor, herunder industrien, internetforvaltningsorganer og akademiske kredse, er både partnere og bidragydere til politikudvikling og -gennemførelse - herunder gennem et kontraktligt offentlig-privat partnerskab (**cPPP**).

Figur 2 - Øget politikudvikling og lovgivning (pr. 31. december 2018)



Kilde: Revisionsretten.

Politik

13 EU's cyberøkosystem er komplekst og består af mange lag, og det spænder over en lang række interne politiske områder, f.eks. retlige og indre anliggender, det digitale indre marked og forskningspolitik. I udenrigspolitikken indgår cybersikkerhed i diplomatiet og er i stigende grad en del af EU's nye forsvarspolitik.

14 Hjørnestenen i EU's politik er **strategien for cybersikkerhed fra 2013**[18]. Formålet med strategien er at gøre EU's digitale miljø til det sikreste i verden, samtidig med at de grundlæggende værdier og frihedsrettigheder forsvares. Den har fem centrale mål: i) bedre cyberrobusthed, ii) mindskelse af cyberkriminalitet, iii) udvikling af cyberforsvarspolitik og -kapacitet, iv) udvikling af industrielle og teknologiske cybersikkerhedsressourcer og v) fastlæggelse af en international cyberspacepolitik, der er tilpasset centrale EU-værdier.

15 Strategien for cybersikkerhed er tæt forbundet med tre andre strategier, der er vedtaget efterfølgende:

— Den **europæiske dagsorden om sikkerhed** (2015) har til formål at forbedre retshåndhævelsen og den juridiske respons på cyberkriminalitet, navnlig ved at revidere eller ajourføre eksisterende politikker og lovgivning[19]. Den har også til hensigt at identificere hindringer for strafferetlig efterforskning af cyberkriminalitet og styrke cyberkapacitetsopbygning.

— **Strategien for et digitalt indre marked**[20] (2015) tager sigte på at skabe bedre adgang til digitale varer og tjenester ved at skabe de rette betingelser for at maksimere den digitale økonomis vækstpotentiale. I denne sammenhæng er det afgørende at styrke onlinesikkerhed, tillid og inklusion.

— Den **globale strategi**[21] fra 2016 skal styrke EU's rolle i verden. Cybersikkerheden er et centralt fundament, der bygger på et fornyet engagement i cyberspørgsmål, samarbejde med nøglepartnere og en vilje til at tackle cyberspørgsmål på alle politikområder, herunder ved tilbagevisning af desinformation gennem strategisk kommunikation.

16 I de seneste år er cyberspace i stigende grad blevet militariseret[22] og brugt som våben[23], og det anses for at være det femte område for krigsførelse[24]. Formålet med cyberforsvar er at beskytte cyberspacesystemer, net og kritisk infrastruktur mod angreb med militære midler og andre midler. En **ramme for cyberforsvarspolitikken** blev vedtaget i 2014 og ajourført i 2018[25]. 2018-ajourføringen fastsætter seks

prioriteter, herunder udvikling af cyberforsvarskapacitet og beskyttelse af det kommunikations- og informationsnetværk, der hører under EU's fælles sikkerheds- og forsvarspolitik (FSFP). Cyberforsvar indgår også i rammerne for det permanente strukturerede samarbejde (PESCO) og EU-NATO-samarbejdet.

17 EU's **fælles ramme for imødegåelse af hybride trusler** (2016) imødegår cybertrusler mod både kritisk infrastruktur og private brugere og understreger, at cyberangreb kan gennemføres gennem desinformationskampagner på de sociale medier[26]. Den fremhæver også, at der er behov for at øge bevidstheden og styrke samarbejdet mellem EU og NATO, hvilket blev underbygget i de fælles erklæringer fra EU og NATO i 2016 og 2018[27].

18 I 2017 fremlagde Kommissionen en ny cybersikkerhedspakke i lyset af det stadig mere påtrængende behov for digital beskyttelse. Den omfattede en ny meddelelse fra Kommissionen om ajourføring af strategien for cybersikkerhed fra 2013[28], en plan for en hurtig og koordineret reaktion på væsentlige angreb og hurtig gennemførelse af direktivet om sikkerhed for net- og informationssystemer (NIS-direktivet)[29]. Pakken omfattede endvidere en række lovgivningsforslag (jf. punkt ***22***).

Lovgivning

19 Siden 2002 er der vedtaget lovgivning med forskellige grader af relevans for cybersikkerheden.

20 Den vigtigste søjle i strategien for cybersikkerhed fra 2013 er dens juridiske kerne, **direktivet om net- og informationssikkerhed (NIS)**[30] fra 2016; den første EU-lovgivning om cybersikkerhed. Formålet med direktivet, som skulle være gennemført senest i maj 2018, er at opnå et minimumsniveau af harmoniseret kapacitet ved at forpligte medlemsstaterne til at vedtage nationale NIS-strategier og oprette centrale kontaktpunkter og enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er)[31]. Det fastsætter også sikkerheds- og underretningskrav for operatører af væsentlige tjenester i kritiske sektorer og for udbydere af digitale tjenester.

21 Samtidig trådte den **generelle forordning om databeskyttelse**[32] (GDPR) i kraft i 2016 og fandt anvendelse fra maj 2018. Forordningens formål er at beskytte europæiske borgeres personoplysninger ved at fastsætte regler om behandling og udbredelse af personoplysninger. Den giver registrerede visse rettigheder og pålægger dataansvarlige (udbydere af digitale tjenester) visse forpligtelser vedrørende anvendelse og videregivelse af oplysninger. Den indfører også underretningskrav i

tilfælde af brud på datasikkerheden og pålægger i nogle tilfælde bøder. ***Figur 3*** viser, hvordan NIS-direktivet og GDPR supplerer hinanden for så vidt angår deres mål om at styrke cybersikkerheden og garantere databeskyttelsen.

22 Blandt de udkast til lovgivning, som drøftes i øjeblikket, kan nævnes den foreslåede forordning om cybersikkerhed, der skal styrke ENISA og oprette en EU-dækkende certificeringsordning[33], den foreslåede forordning om editions- og sikringskendelser om elektronisk bevismateriale[34] og det foreslåede direktiv om elektronisk bevismateriale[35]. 2018-forslaget vedrørende det europæiske industri-, teknologi- og forskningskompetencecenter og netværket af nationale koordinationscentre (i det følgende benævnt "netværket af kompetencecentre for cybersikkerhed og et forskningskompetencecenter") er en del af cybersikkerhedspakken fra 2017[36].

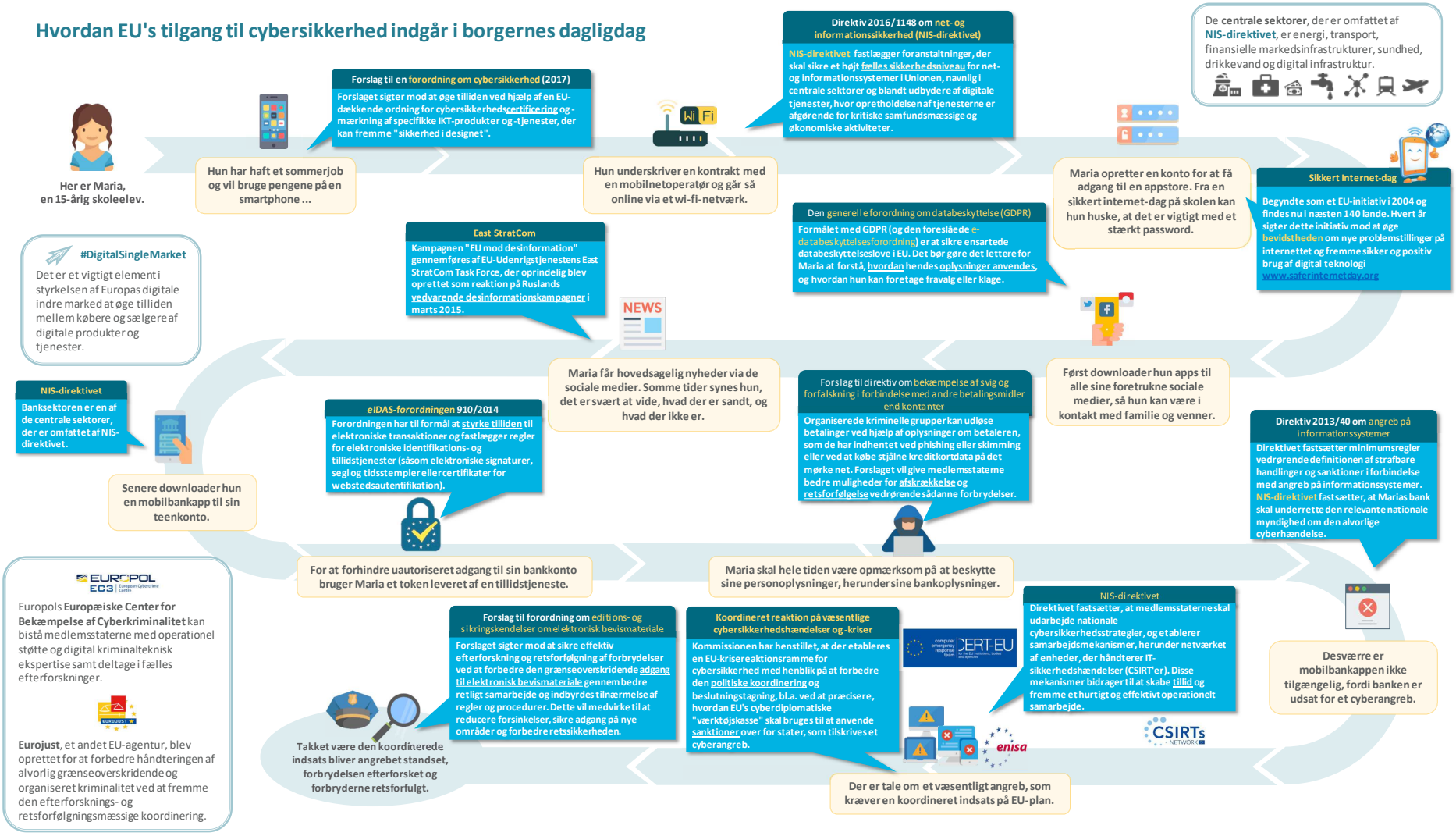
23 Det kan være vanskeligt at overskue bredden af den politiske og lovgivningsmæssige ramme, der vedrører cybersikkerhed, og hvordan den påvirker vores dagligdag.

24 ***Figur 4*** forsøger at beskrive forskellige retsakters og aktiviteters betydning for en fiktiv europæisk borgers tilværelse.

Figur 3 – Hvordan GDPR og NIS-direktivet supplerer hinanden

Kilde: Revisionsretten.

Figur 4 - Hvordan EU's tilgang til cybersikkerhed indgår i borgernes dagligdag



Kilde: Revisionsretten.

Etablering af en politisk og lovgivningsmæssig ramme

25 EU's cyberøkosystem er komplekst og består af mange lag, og det involverer mange aktører (jf. ***bilag I***). Det er en stor udfordring at samle alle cyberøkosystemets forskellige dele. Siden 2013 er der blevet gjort en fælles indsats for at skabe sammenhæng på cybersikkerhedsområdet i EU[37].

Udfordring 1: Fornuftig evaluering og ansvarliggørelse

26 Som Kommissionen har bemærket, er det vanskeligt at fastslå en årsagssammenhæng mellem strategien fra 2013 og eventuelle ændringer. Målene i strategien fra 2013 var meget bredt formuleret og udtrykte snarere en vision end en målbar målsætning[38]. Uden målbare målsætninger er det en udfordring at udarbejde tiltag, der er tilpasset disse brede mål. Den ajourførte ramme for cyberforsvarspolitikken (2018) vil sigte mod at udvikle målsætninger, der fastsætter det mindsteniveau af cybersikkerhed og tillid, der skal opnås. Dette vil imidlertid være begrænset til cyberforsvar og ikke omfatte målsætninger, der fastsætter det ønskede niveau af robusthed for hele EU.

27 Resultater måles sjældent, og kun få politikområder er blevet evalueret[39]. Dette skyldes til dels, at mange foranstaltninger - af lovgivningsmæssig eller andet art - først er blevet gennemført for nylig, hvilket hindrer en fuldstændig vurdering af deres virkning. Udfordringen er at definere relevante vurderingskriterier, som kan bidrage til at måle virkningen. Endvidere er grundig evaluering endnu ikke blevet normen på cybersikkerhedsområdet generelt. Der er derfor behov for et skift i retning af en resultatorienteret kultur med etablerede evalueringspraksis og standardiseret rapportering. ENISA's nuværende mandat omfatter ikke evaluering og overvågning af situationen vedrørende cybersikkerhed og beredskab.

28 Evidensbaseret beslutningstagning kræver, at der foreligger tilstrækkelige pålidelige oplysninger og statistikker, som kan hjælpe med at overvåge og analysere tendenser og behov. Der findes imidlertid kun sparsomme pålidelige oplysninger, fordi der ikke er et obligatorisk og fælles overvågningssystem. Ofte er der ingen indikatorer, og de er vanskelige at definere[40]. Der er dog udviklet specifikke parametre på nogle områder, f.eks. i EU-politikcyklussen for bekæmpelse af grov og organiseret kriminalitet.

29 Kun få medlemsstater indsamler regelmæssigt oplysninger om cyberrelaterede spørgsmål, hvilket hindrer sammenlignelighed. EU har hidtil næsten ikke beskæftiget sig med behovet for at konsolidere statistiske data på europæisk plan[41]. Der foreligger også kun et beskedent antal uafhængige analyser på EU-plan, der omfatter centrale områder såsom[42]: de økonomiske aspekter ved cybersikkerhed, herunder adfærdsmæssige aspekter (misforhold mellem incitamenter, informationsasymmetri), forståelse af konsekvenserne af cybermangler og cyberkriminalitet, makrostatistik vedrørende cybertendenser og forventede udfordringer samt de bedste løsninger til at imødegå trusler.

30 Fordi der har manglet specifikke målsætninger og kun foreligget sparsomme pålidelige oplysninger og veldefinerede indikatorer, har vurderingen af strategiens resultater indtil videre været overvejende kvalitativ. Statusrapporter beskriver ofte de aktiviteter, der er gennemført, eller de milepæle, der er nået, uden en grundig måling af resultater. Desuden er der endnu ikke fastsat basislinjer for vurdering af systemers modstandsdygtighed. Da der ikke er en kodificeret definition af cyberkriminalitet, er det endvidere stort set umuligt at finde relevante europæiske indikatorer, der kan støtte overvågningen og evalueringen.

31 Det uafhængige tilsyn med cybersikkerhedspolitikkens gennemførelse varierer mellem medlemsstaterne. Vi spurgte medlemsstaternes overordnede revisionsorganer om deres revisionserfaring på dette område. Halvdelen af alle respondenterne[43] havde aldrig foretaget revisioner på området. De, der havde foretaget revisioner, havde primært fokuseret på: informationsforvaltning, beskyttelse af kritisk infrastruktur, informationsudveksling og koordinering mellem centrale interessenter samt beredskab, underretning og reaktion vedrørende hændelser. Blandt de emner, der blev dækket i mindre grad, var bevidstgørelsesforanstaltninger og kløften for så vidt angår digitale færdigheder. Af hensyn til den nationale sikkerhed offentliggøres resultaterne af disse revisioner eller evalueringer ikke altid. I ***bilag III*** findes en liste over de revisionsberetninger, der er offentliggjort af medlemsstaternes revisionsorganer.

32 Begrænsninger i cyberkompetencer (jf. også punkt ***82-90***) og vanskeligheder med at evaluere fremskridtene inden for cybersikkerhed blev betragtet som de største udfordringer for revisionen af nationale foranstaltninger på dette område.

Udfordring 2: Udbedring af EU-rettens huller og dens uensartede gennemførelse

33 Den hastighed, hvormed nye teknologier og trusler opstår, overgår langt udformningen og gennemførelsen af EU-lovgivning. Unionens procedurer blev ikke udformet med tanke på den digitale tidsalder: Det er af højeste prioritet at udvikle innovative og fleksible procedurer, der kan sikre en politisk og retlig ramme, som er "fit for purpose"[44], og som giver bedre mulighed for at forudse og forme fremtiden[45].

34 Trods bestræbelser på at skabe større sammenhæng er den lovgivningsmæssige ramme for cybersikkerhed fortsat ufuldstændig (jf. eksemplerne i ***tabel 1***). Fragmentering og lovgivningsmæssige huller gør det vanskeligt at nå de overordnede politiske målsætninger og fører til ineffektivitet. De huller, som Kommissionen identificerede i sin vurdering af strategien, omfattede tingenes internet, ansvarsfordelingen mellem brugere og udbydere af digitale produkter, og visse aspekter, der ikke var omfattet af NIS-direktivet. Den foreslåede forordning om cybersikkerhed forsøger delvis at tackle disse spørgsmål ved at fremme indbygget sikkerhed gennem en EU-dækkende certificeringsordning. Nogle interessenter mener, at den fortsatte mangel på en klart defineret cyberpolitik for industrien og en fælles tilgang til cyberspionage er en væsentlig svaghed[46].

Tabel 1 - Huller og uensartet gennemførelse i den lovgivningsmæssige ramme (listen er ikke udtømmende)

Politikområde	Eksempler
Det digitale indre marked	o Det nuværende forbrugerkøbsdirektiv omfatter ikke cybersikkerhed. Formålet med det foreslåede direktiv om digitalt indhold[47] og onlinesalg[48] er at lukke dette hul. o Der er begrænsede og forskellige retlige rammer for rettidig omhu i EU-medlemsstaterne, hvilket skaber retsusikkerhed og vanskeligheder med at anvende retsmidler[49]. o Der udvikles politikker vedrørende afsløring af softwaresårbarheder i forskelligt tempo i medlemsstaterne uden en overordnet EU-retlig ramme, der muliggør en koordineret tilgang[50].
Styrkelse af net- og informationssikkerhed	o Medlemsstaterne kan frit beslutte, om de vil inddrage sektorer, der er udeladt fra NIS-direktivet[51]. Indkvarteringsbranchen, som ikke er omfattet, kan bane vejen for andre forbrydelser, herunder menneske- og narkotikasmugling og ulovlig indvandring[52].
Bekæmpelse af cyberkriminalitet	o Mange medlemsstater har ikke defineret elektronisk bevismateriale i deres nationale lovgivning[53] (jf. også punkt ***22***). o Den nuværende rammeafgørelse om svig i forbindelse med kontantløse betalinger omfatter ikke udtrykkeligt ikkefysiske betalingsinstrumenter såsom virtuelle valutaer, e-penge og mobile penge, og heller ikke handlinger som f.eks. phishing, skimming samt besiddelse og deling af oplysninger om betaleren[54]. o Direktivet om angreb på informationssystemer vedrører ikke direkte ulovlig dataindsamling indefra (f.eks. cyberspionage), hvilket giver udfordringer for de retshåndhævende myndigheder[55]. o I kølvandet på dommen fra Den Europæiske Unions Domstol om opbevaring af data[56] har forskelle i medlemsstaternes anvendelse af den retlige ramme vanskeliggjort retshåndhævelsen, hvilket potentielt kan medføre tab af efterforskningsspor og modvirke en effektiv retsforfølgning af kriminelle onlineaktiviteter[57].

Kilde: Revisionsretten.

35 Det er fortsat frivilligt både for de nationale myndigheder og de private operatører at gennemføre en række aspekter af lovgivningen. Inden for rammerne af samarbejdsgruppen er det f.eks. frivilligt at evaluere de nationale strategier for net- og informationssystemers sikkerhed og effektiviteten af CSIRT'er. I henhold til den foreslåede certificeringsordning i forordningen om cybersikkerhed vil det ligeledes være frivilligt at indføre certificering af IKT-produkter og -tjenester.

36 I EU henhører cybersikkerhed under medlemsstaterne. Ikke desto mindre har EU en afgørende rolle at spille i forbindelse med at skabe vilkårene for, at dets medlemsstaters kapacitet kan forbedres, og at de kan arbejde sammen og skabe tillid. På grund af de store forskelle mellem medlemsstaterne for så vidt angår kapacitet og engagement[58] vil formidlingen af følsomme oplysninger (vedrørende national sikkerhed) dog forblive frivillig.

37 Medlemsstaternes uensartede gennemførelse af EU-retten kan resultere i juridisk og operationel uoverensstemmelse, og den forhindrer lovgivningen i at nå sit fulde potentiale. Medlemsstaterne har f.eks. forskellige fortolkninger af, hvordan kontrol med eksport af produkter med dobbelt anvendelse bør gennemføres[59], hvilket betyder, at nogle EU-baserede virksomheder muligvis eksporterer teknologier og tjenester, der kan bruges til cyberovervågning og menneskerettighedskrænkelser gennem censur eller aflytning. Europa-Parlamentet har udtrykt bekymring over dette[60].

38 Endvidere kræver beskyttelsen af privatlivets fred og ytringsfriheden et skræddersyet lovgivningsmæssigt svar for at sikre den nødvendige balance mellem at beskytte de grundlæggende værdier og tage højde for EU's sikkerhedshensyn. Hvordan sikrer vi f.eks. "end-to-end"-kryptering, samtidig med at vi finder den bedste metode til at støtte retshåndhævelsen? Eller hvordan kan vi opfylde målene i GDPR og samtidig forstå dens konsekvenser for offentligt tilgængelige oplysninger om indehavere af domænenavne og indehavere af blokke af IP-adresser? Og hvordan kan dette have negativ indvirkning på de retshåndhævende myndigheders efterforskninger[61]?

39 Lovgivning alene sikrer ikke cyberrobusthed. Formålet med NIS-direktivet er et nå et højt sikkerhedsniveau i hele EU, men det fokuserer udtrykkeligt på at opnå minimumsharmonisering, ikke maksimumsharmonisering[62]. Der vil fortsat opstå huller, efterhånden som cyberlandskabet udvikler sig.

Refleksionspunkter - Den politiske ramme

- Hvilke vigtige skridt er nødvendige for, at både politiske beslutningstagere og lovgivere foretager et skift i retning af en mere resultatorienteret kultur på cybersikkerhedsområdet og bl.a. definerer generel cyberrobusthed?
- Hvordan kan forskningen i højere grad bidrage til at generere de oplysninger og statistikker, der er nødvendige for at muliggøre en fornuftig evaluering?
- Hvordan kan EU's lovgivningsprocedurer tilpasses, så de bliver mere fleksible og tager bedre hensyn til, at teknologien og truslerne udvikler sig hurtigt?
- Hvordan kan praksis med hensyn til udvikling af parametre (indikatorer, mål) i EU-politikcyklussen tilpasses, opskaleres og overføres til cybersikkerhedsområdet som helhed?
- Hvad kan medlemsstaternes overordnede revisionsorganer lære af hinandens tilgange til revision af cybersikkerhedspolitikker og -foranstaltninger?
- Hvilke uoverensstemmelser i gennemførelsen og anvendelsen af EU's retlige ramme underminerer en mere effektiv reaktion på huller i cybersikkerheden og cyberkriminalitet, og hvordan kan dette bedst løses af medlemsstaterne og EU-institutionerne?
- Hvor effektiv er EU's eksportkontrol med cybervarer og -tjenester med hensyn til at forebygge menneskerettighedskrænkelser uden for EU?

Finansiering og udgifter

40 EU tilstræber at blive verdens sikreste onlinemiljø. Det kræver en markant indsats fra alle interessenters side at opfylde denne ambition, herunder et solidt og velordnet finansielt grundlag.

Udfordring 3: Tilpasning af investeringsniveauerne til målene

Opskalering af investeringerne

41 De samlede globale udgifter til cybersikkerhed som procentdel af BNP anslås til omkring 0,1 %. I USA[63] ligger de på ca. 0,35 % (inkl. den private sektor). Som procentdel af BNP udgør den amerikanske forbundsregerings udgifter ca. 0,1 %, eller omkring 21 milliarder USD budgetteret for 2019[64].

42 Til sammenligning har udgifterne i EU været lave, fragmenterede og ofte ikke bakket op af samordnede regeringsledede programmer. Det er vanskelige at komme i besiddelse af tal, men de offentlige udgifter til cybersikkerhed i EU anslås til mellem én og to milliarder euro om året[65]. Visse medlemsstaters udgifter som procentdel af BNP er en tiendedel af det amerikanske niveau, eller endda lavere[66]. EU og dets medlemsstater er nødt til at vide, hvor meget de tilsammen investerer, for at kunne finde ud af, hvilke huller der skal lukkes.

43 Det er vanskeligt at danne sig et samlet billede, da der mangler klare oplysninger som følge af cybersikkerhedens tværgående karakter, og fordi cybersikkerhed og generelle IT-udgifter ofte ikke kan skelnes fra hinanden[67]. Vores undersøgelse har bekræftet, at det er vanskeligt at opnå pålidelige statistikker om udgifterne i både den offentlige og den private sektor. Tre fjerdedele af medlemsstaternes overordnede revisionsorganer meddelte, at de ikke havde et centraliseret overblik over de cyberrelaterede offentlige udgifter, og ikke én eneste medlemsstat pålagde offentlige enheder at angive udgifter til cybersikkerhed separat i deres finansieringsplaner.

44 Det er en særlig udfordring at opskalere de offentlige og private investeringer i Europas cybersikkerhedsfirmaer. Offentlig kapital er ofte tilgængelig i de indledende faser, men sjældnere i vækst- og ekspansionsfaserne[68]. Der findes mange EU-finansieringsinitiativer, men de bliver ikke udnyttet, hovedsagelig på grund af bureaukrati[69]. Generelt klarer EU's cybersikkerhedsfirmaer sig dårligt i forhold til virksomheder i andre lande: De er færre i antal, og den gennemsnitlige

finansieringskapital, de rejser, er betydeligt lavere[70]. Det er derfor afgørende at sikre en effektiv målretning og finansiering af nystartede virksomheder for at nå EU's politiske målsætninger på det digitale område.

Opskalering af virkningerne

45 Bestræbelserne på at lukke cyberinvesteringskløften er nødt til at give konkrete resultater. F.eks. har EU en stærk forsknings- og innovationssektor, men dens resultater bliver ikke patenteret, markedsført og opskaleret tilstrækkeligt med henblik på at styrke cyberrobustheden, konkurrenceevnen og den digitale autonomi[71]. Dette er navnlig tilfældet, når der sammenlignes med EU's globale konkurrenter. Sparsomheden af korrekt udnyttede resultater skyldes en række faktorer[72], bl.a.:

- manglen på en sammenhængende transnational strategi til at opskalere tilgangen, så den matcher EU's bredere digitale mål for så vidt angår konkurrenceevne og øget autonomi
- varigheden af værdikædecyklussen, som medfører, at værktøjer hurtigt bliver forældede
- den manglende bæredygtighed, da projekter typisk afsluttes med opløsningen af projektteamet og indstillingen af al support, herunder opdateringer og patchløsninger.

46 Kommissionens forslag om at oprette et netværk af kompetencecentre for cybersikkerhed og et forskningskompetencecenter er et forsøg på at fjerne fragmenteringen på området for cybersikkerhedsforskning og fremme investeringer i stor skala[73]. Der findes i alt ca. 665 ekspertisecentre i hele EU.

Udfordring 4: Et klart overblik over EU's budgetudgifter

47 Et centraliseret overblik over udgifterne er vigtigt for gennemsigtigheden og en bedre koordinering. Uden dette overblik er det vanskeligt for de politiske beslutningstagere at se, om udgifterne er tilpasset til de behov, der skal dækkes, for at de prioriterede mål kan nås.

48 Intet særskilt budget finansierer strategien for cybersikkerhed. På EU-plan afholdes udgifterne til cybersikkerhed i stedet over EU's almindelige budget og via medlemsstaternes medfinansiering. Vores analyse afslører en kompleks struktur, der består af mindst ti forskellige instrumenter under EU's almindelige budget, men den

giver intet tydeligt billede af, hvilke midler der anvendes, og hvor de anvendes (jf. ***bilag 2***).

49 Det er derfor en stor udfordring at få et klart overblik over udgifterne vedrørende dette emne, der går på tværs af mange politikområder. Udgiftsprogrammerne forvaltes af forskellige dele af Kommissionen, der alle har deres egne mål, regler og tidsplaner. Billedet kompliceres yderligere, når medlemsstaternes medfinansiering tages i betragtning, f.eks. i forbindelse med Fonden for Intern Sikkerhed (Politi)[74].

Identificerbare udgifter til cybersikkerhed

50 Kommissionen brugte i perioden 2014-2018 mindst 1,4 milliarder euro på at gennemføre strategien[75] og tildelte den største del af midlerne til Horisont 2020[76]. Midlerne fra Horisont 2020 kanaliseres primært gennem programmet vedrørende udfordringen "Sikre samfund" og projekter under programmet "Lederskab inden for støtte- og industriteknologi"[77]. Vi identificerede 279 indgåede kontrakter om cybersikkerhedsrelaterede projekter frem til september 2018 med en samlet EU-finansiering på 786 millioner euro[78]. ***Figur 5*** viser, hvordan disse projekter ifølge vores analyse fordeler sig på typer.

Figur 5 – Indgåede kontrakter om forskningsprojekter vedrørende cybersikkerhed under Horisont 2020 (millioner euro)

Kilde: Revisionsretten.

51 Et kontraktligt offentlig-privat partnerskab (cPPP) blev oprettet i 2016 for at styrke den europæiske cybersikkerhedsindustri. Målet var at kanalisere 450 millioner euro fra Horisont 2020-programmet til cPPP og tiltrække yderligere 1,8 milliarder euro fra den private sektor senest i 2020. I perioden på 18 måneder frem til den 31. december 2017 var der kanaliseret 67,5 millioner euro fra Horisont 2020 til cPPP, og den private sektor havde investeret 1 milliard euro[79].

52 Bekæmpelsen af cyberkriminalitet støttes også af Fonden for Intern Sikkerhed - Politi (FIS-P). FIS-P støtter undersøgelser, ekspertmøder og kommunikationsaktiviteter; disse beløb sig til næsten 62 millioner euro mellem 2014 og 2017. Medlemsstaterne kan endvidere få tilskud til udstyr, uddannelse, forskning og dataindsamling under delt forvaltning. 19 medlemsstater har modtaget 42 millioner euro i sådanne tilskud.

53 Midlerne til støtte for det retlige samarbejde og den funktion, som traktater om gensidig retshjælp har, med særligt fokus på udveksling af elektroniske data og finansielle oplysninger, udgjorde 9 millioner euro under programmet for retlige anliggender, der forvaltes af GD JUST.

54 I NIS-direktivet er det udtrykkeligt angivet, at CSIRT'erne skal have de fornødne ressourcer til effektivt at udføre deres opgaver[80]. Mellem 2016 og 2018 var der årligt 13 millioner euro til rådighed fra Connecting Europe-faciliteten, hvorfra medlemsstaterne kunne ansøge om midler til at støtte opfyldelsen af direktivets krav. Der er ikke foretaget nogen undersøgelse for at kortlægge de konkrete finansielle behov, der skal dækkes, for at CSIRT-netværket og samarbejdsgruppen har en indvirkning.

55 Flere af agenturernes operationelle omkostninger er specifikt blevet afsat til cybersikkerhed eller bekæmpelse af cyberkriminelle aktiviteter. Det er dog vanskeligt at udtrække nøjagtige tal fra de offentligt tilgængelige oplysninger.

56 Budapestkonventionen (jf. punkt ***11***) har dannet grundlaget for EU's eksterne udgifter til cybersikkerhed. EU brugte ca. 50 millioner euro på at styrke cybersikkerheden uden for sine grænser i perioden 2014-2018. Næsten halvdelen af dette beløb kom fra instrumentet til fremme af stabilitet og fred, hvor ét vigtigt projekt - GLACY+ til 13,5 millioner euro - tager sigte på at styrke den globale kapacitet inden for udvikling og gennemførelse af lovgivning om cyberkriminalitet og øge det internationale samarbejde[81]. Ellers fokuserede midlerne fra EU's andre finansielle instrumenter hovedsagelig på det vestlige Balkan[82] samt det europæiske nærområde, f.eks. tager Cybercrime@EaP-projektet med landene i det østlige partnerskab sigte på at forbedre det internationale samarbejde om cyberkriminalitet og elektronisk bevismateriale.

Andre udgifter til cybersikkerhed

57 Det er ikke altid muligt at identificere specifikke udgifter til cybersikkerhed inden for EU-programmer:

- Finansieringen under Horisont 2020 er også blevet kanaliseret til cyberfysiske systemer gennem fællesforetagendet for elektronikkomponenter og -systemer for europæisk lederskab (ECSEL).- Vi var dog ikke i stand til at fastlægge, hvad der specifikt vedrørte cybersikkerhed i de 27 projekter til i alt 437 millioner euro mellem 2015 og 2016.

- Der er op til 400 millioner euro til rådighed til udgifter vedrørende cybersikkerhed og tillidstjenester under de europæiske struktur- og investeringsfonde. Dette omfatter investeringer i sikkerhed og databeskyttelse til fremme af interoperabilitet og sammenkobling mellem digitale infrastrukturer, elektronisk identifikation, beskyttelse af privatlivets fred og tillidstjenester.

58 Den Europæiske Investeringsbank bebudede i sin operationelle plan for 2018, at den agtede at øge sin finansiering af teknologi med dobbelt anvendelse, cybersikkerhed og civil sikkerhed til op til 6 milliarder euro over en treårig periode[83].

Fremtidsperspektiver

59 Cybersikkerhedskomponenten til 2 milliarder euro i det foreslåede nye program for et digitalt Europa[84] for 2021-2027 har til formål at styrke EU's cybersikkerhedsindustri og samfundets overordnede beskyttelse, bl.a. ved at støtte gennemførelsen af NIS-direktivet. Det foreslåede netværk af kompetencecentre for cybersikkerhed og et forskningskompetencecenter, som skal føre til en mere strømlinet tilgang, forventes at udgøre den vigtigste gennemførelsesmekanisme for EU-udgifterne under programmet for et digitalt Europa.

60 Forsvarsudgifterne fra EU-budgettet er for nylig steget på grund af programmet for udvikling af den europæiske forsvarsindustri, hvorfra der skal tildeles 500 millioner euro i 2019 og 2020[85]. Der vil blive lagt vægt på at forbedre koordineringen og effektiviteten af medlemsstaternes forsvarsudgifter gennem incitamenter til fælles udvikling. Målet er at generere et samlet beløb på 13 milliarder euro til investering i forsvarskapacitet efter 2020, herunder til cyberforsvar, gennem Den Europæiske Forsvarsfond[86].

Udfordring 5: Tilstrækkelige ressourcer til EU's agenturer

61 De tre organer, der udgør kernen i EU's cybersikkerhedspolitik - ENISA, Europols EC3 og CERT-EU (jf. ***tekstboks 2***) - står over for ressourcemæssige udfordringer i en tid med særlig stærke politiske prioriteter med fokus på sikkerhed. Med den nuværende tildeling af menneskelige og finansielle ressourcer er det fortsat en udfordring for EU-agenturerne at leve op til forventningerne[87].

62 Agenturernes anmodninger om yderligere ressourcer for at matche den stigende efterspørgsel er ikke blevet fuldt ud efterkommet, og det kan potentielt forhindre, at de politiske målsætninger nås (rettidigt). Følgende kan nævnes som eksempler:

- Begrænsede ressourcer var en faktor, der bidrog til at forhindre ENISA i fuldt ud at nå sine målsætninger i 2017[88]. Der blev foreslået yderligere ressourcer i 2017-pakken for at sikre, at ENISA kan opfylde sit nye mandat.

- Tilrådighedsstillelsen af analysepersonale og investeringerne i IKT-kapacitet hos Europols EC3 er ikke fulgt med efterspørgslen[89]. Endvidere er Europols fælles aktionsgruppe vedrørende cyberkriminalitet (J-CAT) bemandet med personale fra medlemsstaterne og tredjelandseksperter, der støtter efterretningsbaserede undersøgelser. Omkostningerne afholdes dog primært af udsenderstaterne, hvilket afholder dem fra at udsende eksperter i stort antal. Der er planlagt en ordning med midlertidig udsendelse fra sag til sag, som i nogen grad kan finansieres via Europol eller EU-politikcyklussen for at gøre det muligt for flere lande at deltage.

63 En række begrænsninger er selvforskyldte. Mange ansatte i CERT-EU og ENISA er kontraktansatte, og procedurerne for ansættelse af disse er generelt langsomme. Andre begrænsninger, f.eks. med hensyn til at tiltrække nye talenter og holde på dem, skyldes, at agenturerne ikke er i stand til at konkurrere med den private sektors lønninger, eller at karrieremulighederne er dårlige. Derfor outsourcede ENISA en stor del af sit arbejde mellem 2014 og 2016[90].

64 Manglen på personale og de nødvendige værktøjer kan medføre betydelige risici, navnlig med hensyn til indsamling af efterretningsoplysninger om trusler. Mængden af data fra åbne og lukkede kilder fortsætter med at vokse og risikerer at belaste analysepersonalets kapacitet til at udføre grundige trusselsanalyser. Uden den nødvendige kapacitet og de rette værktøjer til med vellykket resultat at integrere og sammenkoble disse data vil de ikke effektivt kunne omsættes til brugbare efterretningsoplysninger om trusler, der kan deles og analyseres i hele EU[91].

Refleksionspunkter - Finansiering og udgifter

- Hvordan kan Kommissionen og lovgiverne strømline EU's udgifter til cybersikkerhed og mere eksplicit tilpasse dem til klart fastsatte mål?
- Hvordan kan manglerne i ressourcetildelingen til EU's agenturer tackles på en overordnet måde, der tager hensyn til Unionens behov og mål?
- Hvilke foranstaltninger er ved at blive identificeret på EU-plan og i medlemsstaterne med henblik på at mindske hindringerne for, at SMV'er kan optage investeringslån for at opskalere deres aktiviteter?
- Hvilke konkrete og vedvarende resultater har midlerne under Horisont 2020 leveret med hensyn til cybersikkerhedsløsninger?
- Hvordan styrker EU's kapacitetsopbygning kapaciteten uden for EU's grænser i overensstemmelse med EU's værdier?

Opbygning af et cyberrobust samfund

65 Forvaltning af cybersikkerhed er håndtering af trusler og risici, styrkelse af kapacitet og bevidsthed samt koordinering og informationsudveksling på grundlag af tillid.

Udfordring 6: Styrkelse af forvaltning og standarder

Forvaltning af informationssikkerhed

66 Forvaltning af informationssikkerhed har at gøre med etablering af strukturer og politikker, der sikrer datafortrolighed, -integritet og -tilgængelighed. Der er tale om mere end blot et teknisk spørgsmål, og det kræver effektivt lederskab, solide processer og strategier, der er tilpasset organisatoriske målsætninger[92]. Området omfatter forvaltning af cybersikkerhed, som har at gøre med alle typer cyberrelaterede trusler, herunder målrettede og sofistikerede angreb, brud på datasikkerheden eller hændelser, som er vanskelige at detektere eller håndtere.

67 Modellerne for forvaltning af cybersikkerhed varierer fra medlemsstat til medlemsstat, og ansvaret for cybersikkerhed er ofte fordelt på mange enheder i medlemsstaterne. Disse forskelle kan hindre det samarbejde, der er nødvendigt på nationalt plan - for ikke at tale om EU-plan - for at reagere på væsentlige, grænseoverskridende hændelser og udveksle efterretningsoplysninger om trusler. Vores spørgeundersøgelse henvendt til medlemsstaternes overordnede revisionsorganer viste, at svagheder i de offentlige myndigheders forvaltningsordninger og risikostyring blev anset for at være de største risici.

68 Og selv om konsekvenserne for organisationer i den private sektor kan være alvorlige, er der mange svagheder i denne sektors cyberforvaltning. Næsten ni ud af ti organisationer siger, at deres cybersikkerhedsfunktioner ikke fuldt ud opfylder deres behov[93], og cybersikkerhedspersonalet befinder sig ofte mindst to niveauer under bestyrelsen[94].

69 EU's selskabsdirektiver indeholder ingen specifikke krav om videregivelse af oplysninger om cyberrisici. I USA udsendte Securities and Exchange Commission for nylig ikkebindende retningslinjer, der skal hjælpe offentlige virksomheder til at udarbejde oplysninger om cybersikkerhedsrisici og -hændelser[95]. Det Fælles Udvalg af Europæiske Tilsynsmyndigheder[96] advarede om stigningen i cyberrisici, tilskyndede de

finansielle institutioner til at forbedre sårbare IT-systemer og undersøge de risici, som er forbundet med informationssikkerhed, konnektivitet og outsourcing[97].

70 Styrkelsen af SMV'ers forvaltning af informationssikkerhed er særligt vanskelig, da de i de fleste tilfælde ikke er i stand til at indføre de relevante systemer. SMV'erne mangler passende retningslinjer for overholdelse af krav om informationssikkerhed og beskyttelse af privatlivets fred samt imødegåelse af teknologiske risici[98]. De vigtigste udfordringer er derfor at forstå deres behov bedre og at give dem de nødvendige incitamenter og den rette støtte.

71 Manglen på en sammenhængende, international ramme for forvaltning af cybersikkerhed hæmmer det internationale samfunds evne til at reagere på og begrænse cyberangreb. Det er derfor vigtigt at skabe konsensus omkring en forvaltningsramme, der bedst muligt afspejler EU's interesser og værdier[99]. Forsøg på at fastsætte bindende internationale cyberspacenormer bliver stadig vanskeligere, hvilket kom til udtryk i 2017 i FN-gruppen af regeringseksperter, hvor der ikke blev opnået enighed om, hvordan international ret bør gælde for staters reaktion på hændelser.

72 For at styrke sin dagsorden for cyberspaceforvaltning har EU også formaliseret seks cyberpartnerskaber med henblik på at etablere regelmæssige politiske dialoger, som skal opbygge tillid og skabe fælles samarbejdsområder[100]. Resultaterne er blandede, men på internationalt plan kan EU generelt ikke anses for at være en "vigtig cybersikkerhedsaktør", selv om det har styrket sin profil[101].

Informationssikkerhed i EU-institutionerne

73 Hver EU-institution har sine egne regler vedrørende forvaltning af informationssikkerhed. En interinstitutionel aftale indeholder bestemmelser om informationssikkerhedsrelateret bistand fra Kommissionen til de andre institutioner og agenturer. EU's institutioner og organer har anerkendt behovet for at udvikle deres cyberkapacitet og risikostyringsmetoder på en sammenhængende måde. I 2020 vil Kommissionen, Rådet og EU-Udenrigstjenesten aflægge rapport for Den Horisontale Gruppe vedrørende Cyberspørgsmål om deres forvaltning og de fremskridt, der er gjort med hensyn til at præcisere og harmonisere forvaltningen af cybersikkerhed i EU's institutioner og agenturer[102].

74 I Kommissionen er Generaldirektoratet for Informationsteknologi (DIGIT) ansvarligt for sikkerheden i forbindelse med IT-infrastruktur og -tjenester (jf. ***tekstboks 3***). De væsentligste IT-sikkerhedsmål i Kommissionens digitale strategi er

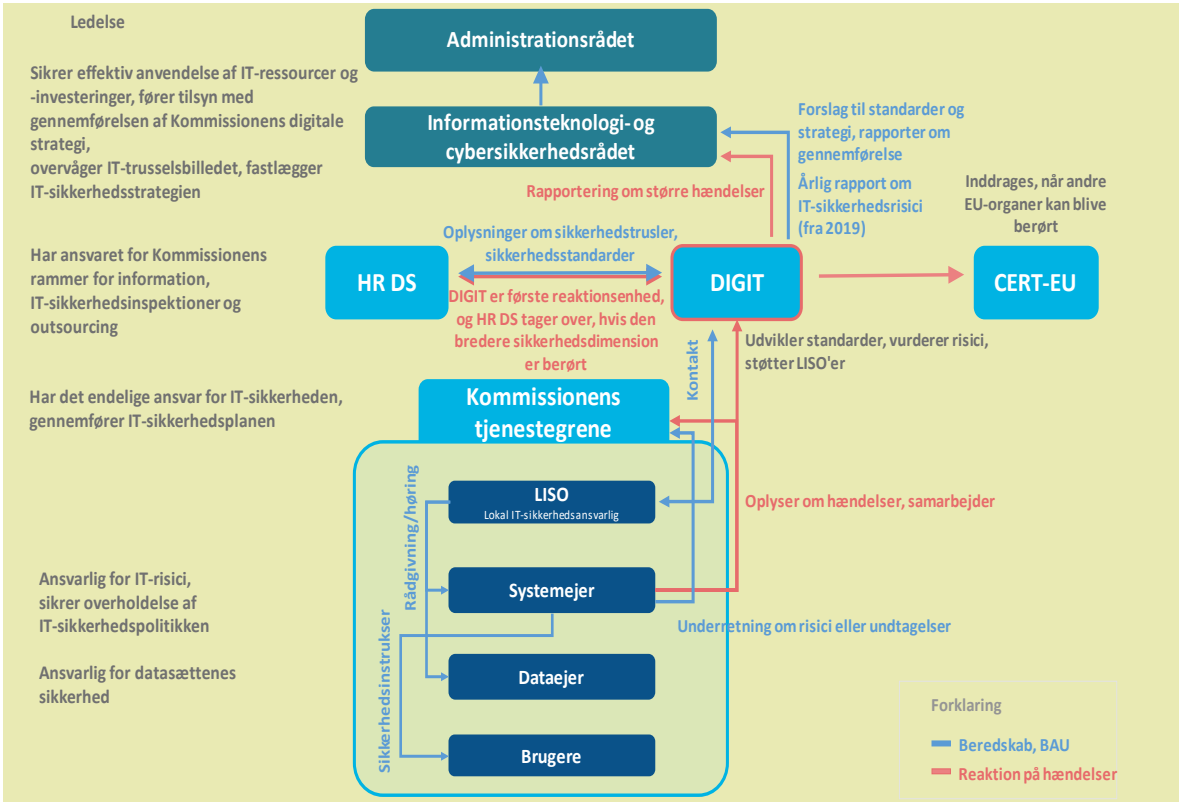
at inddrage IT-sikkerhed i forvaltningsprocedurer, skabe (omkostnings)effektiv infrastruktur og modstandsdygtighed, udvide detekteringen af og reaktionen på hændelser og integrere IT- og sikkerhedsforvaltningen[103]. Kommissionen sikrer i sin tjenesteudbyderkontrakt, at næsten al software vedligeholdes aktivt, og at kun leverandørunderstøttet software anvendes[104].

75 Vigtigheden af at beskytte institutionerne omfatter også EU's FSFP-missioner og -strukturer verden over. En af prioriteterne for EU's cyberforsvarspolitik (2018-ajourføring) er at styrke beskyttelsen af de FSFP-kommunikations- og -informationssystemer, som EU-enheder anvender. Et internt cyberstyringsråd i EU-Udenrigstjenesten er nu på plads og mødtes for første gang i juni 2017[105].

Tekstboks 3

Beskyttelse af Kommissionens informationssystemer

Kommissionens ca. 1 300 systemer og 50 000 enheder er konstante mål for cyberangreb. Ansvaret for IT er decentraliseret, jf. figuren nedenfor. Informations- og IT-sikkerheden er baseret på en fælles IT-sikkerhedsplan, der er fastlagt af DIGIT. Informationsteknologi- og cybersikkerhedsrådet er i praksis ansvarligt for Kommissionens informationssystemsikkerhed og er bindeleddet mellem den operationelle side af IT-sikkerheden og Kommissionens øverste ledelse, der er repræsenteret af administrationsrådet.



Kilde: Revisionsretten baseret på Kommissionens afgørelser[106].

Hovedopgaven i GD for Menneskelige Ressourcer og Sikkerhed (GD HR DS) er at beskytte Kommissionens personale, oplysninger og aktiver. Det foretager også sikkerhedsundersøgelser af hændelser, der har en bredere dimension end blot IT, og bidrager derfor til Kommissionens aktiviteter vedrørende kontraefterretning og terrorbekæmpelse.

DIGIT er ansvarligt for IT-sikkerheden og huser CERT-EU (EU's IT-Beredskabsenhed). CERT-EU, der blev oprettet i 2011, har et årligt budget på ca. 2,5 millioner euro og ca. 30 ansatte. Det udgør det første responsled i tilfælde af informationssikkerhedshændelser, der berører flere institutioner, men alligevel er det ikke i drift alle døgnets 24 timer. Det administrerer en informationsdelingsplatform. I 2018 undertegnede CERT-EU et ikkebindende aftalememorandum med ENISA, EC3 og Det Europæiske Forsvarsagentur om at styrke samarbejdet og koordineringen. Den har også en teknisk aftale med NATO's Computer Incident Response Capability (NCIRC).

Trussels- og risikovurderinger

76 Velbegrundede og løbende trussels- og risikovurderinger er vigtige redskaber for både offentlige og private organisationer. Der er imidlertid ingen fælles tilgang til klassificering og kortlægning af cybertrusler eller til risikovurderinger, og det betyder, at vurderingernes indhold varierer betydeligt, hvilket er en udfordring, når det gælder udviklingen af en sammenhængende EU-tilgang til cybersikkerhed[107]. Endvidere anvender organisationerne ofte de samme kilder, eller endda hinandens

trusselsvurderinger, hvilket resulterer i massevis af gentagne konstateringer[108], med den risiko til følge, at der ikke tages nok højde for andre trusler. Dette forværres af vedvarende uvilje til at udveksle oplysninger og underrapportering af hændelser.

77 Analyseenheden for hybride trusler[109], der hører under EU-Udenrigstjenesten, blev oprettet for at forbedre situationsforståelsen og støtte beslutningstagningen gennem deling af analyser, men den bør udvide sin ekspertise, bl.a. inden for cybersikkerhed. Parallelt hermed forsyner CERT-EU EU's institutioner, organer og agenturer med rapporter og briefinger om de cybertrusler, der er rettet mod dem.

78 ENISA har tidligere bemærket, at mange medlemsstater har en kvalitativ forståelse af trusler, og at der er behov for mere modellering i forbindelse med cybertrusler[110]. Overvågning af kapaciteten til strategisk analyse vil styrke den overordnede forståelse. Ud over at omfatte teknologiske trusler kunne trusselsvurderingerne imidlertid også behandle socialpolitiske og økonomiske trusselsforhold for at give et mere samlet billede, herunder årsagerne til trusler og aktørernes motiver.

Incitamenter

79 Der er stadig for få juridiske og økonomiske incitamenter for organisationer til at underrette og dele oplysninger om hændelser. Mange organisationer frygter omdømmemæssig skade og foretrækker stadig at håndtere cyberangreb diskret eller at betale løsepenge til dem, der står bag angrebene. Det er endnu uvist, i hvor høj grad NIS-direktivet vil medvirke til at øge underretningsniveauet. Kommissionen forventer, at der primært vil ske forbedringer på nationalt plan, men forordningen om cybersikkerhed vil tilføje en fælles EU-tilgang[111].

80 Ved at inddrage bestemte standarder i deres indkøbsprocedurer kan de offentlige myndigheder i deres egenskab af indkøbere af digitale varer og tjenester gennem offentlige indkøb styrke deres position over for leverandører samt i forbindelse med forsknings- og programfinansiering (f.eks. ved at kræve, at der vedtages bestemte tekniske standarder såsom internetprotokollen IPv6 for at bidrage til bekæmpelsen af cyberkriminalitet). På nuværende tidspunkt er der dog ingen fælles indkøbsramme for cybersikkerhedsinfrastruktur[112]. Kommissionen kan gøre meget mere i denne sammenhæng. Det foreslåede program for det digitale Europa i den næste flerårige finansielle ramme tager sigte på at adressere de hidtil begrænsede offentlige investeringer i indkøb af den nyeste cybersikkerhedsteknologi.

81 Kommissionen kan som reguleringsmyndighed sikre, at de rette standarder udarbejdes med sigte på vidtrækkende indførelse for at forbedre sikkerheden. Kommissionen og Europol samarbejder med internetforvaltningsorganer såsom ICANN (jf. punkt ***38***) og RIPE-NCC[113], hvilket er afgørende for at indføre den rette arkitektur for bekæmpelse af cyberkriminalitet med henblik på at støtte de retshåndhævende og retlige myndigheder.

Udfordring 7: Øget kompetence- og bevidsthedsniveau

82 ENISA har påpeget, at brugerne spiller en kritisk rolle i bekæmpelsen af cyberangreb, og at styrkelse af kompetencer, uddannelse og bevidsthed er nøglen til at opbygge et cyberrobust samfund[114]. Enkeltpersoner, der på arbejdspladsen eller i hjemmet er gode til at opdage advarselssignalerne og har de rette teknikker, kan bremse eller forhindre angreb.

83 Et problem af særlig bekymring er det stigende misforhold mellem den knowhow, som er nødvendig for at begå cyberkriminalitet eller iværksætte et cyberangreb, og de kompetencer, der er nødvendige for at forsvare sig mod det. Crime-as-a-service-modellen har gjort det lettere at komme ind på markedet for cyberkriminalitet: Enkeltpersoner uden de tekniske færdigheder til selv at udvikle dem kan nu leje botnet, exploit kits eller pakker med ransomware.

Uddannelse, kompetencer og kapacitetsopbygning

84 Verden står over for en stigende kompetencemangel inden for cybersikkerhed; manglen på arbejdskraft er steget med 20 % siden 2015[115] De traditionelle rekrutteringskanaler kan ikke dække behovet, herunder for ledende og tværfaglige medarbejdere[116]. Næsten 90 % af den globale arbejdsstyrke inden for cybersikkerhed består af mænd; den vedvarende mangel på kønsdiversitet begrænser talentmassen yderligere[117]. Endvidere er cyberrelaterede spørgsmål underrepræsenteret inden for ikketekniske programmer på universiteter.

85 Der er behov for uddannelse over hele linjen, blandt embedsmænd, retshåndhævelsespersonale, retlige myndigheder, de væbnede styrker og undervisere. Det er f.eks. nødvendigt, at domstolene kan håndtere de hurtigt skiftende tekniske spørgsmål vedrørende cyberkriminaliteten og beskytte dens ofre[118]; der er på nuværende tidspunkt ingen EU-standarder for uddannelse og certificering[119]. I EU-institutionerne er det vigtigt at have det rette kompetencemiks. Uden det rette kompetencemiks kan institutionerne være ude af stand til at definere rammer korrekt

og identificere de rette partnere og sikkerhedsbehov, eller de kan mangle kapacitet til at forvalte deres programmer. Det kan igen undergrave effektiviteten af EU's programmer eller politikudviklingen.

86 Medlemsstaterne er ansvarlige for uddannelsespolitikker på EU-plan, og adskillige uddannelsesaktiviteter (jf. ***tabel 2***) og øvelser (jf. ***tekstboks 4***) finder allerede sted. EU kan hjælpe med til at få indarbejdet EU-standarder i læseplaner på alle relevante fagområder[120]. Inden for f.eks. digital kriminalteknik er fælles uddannelsesstandarder nødvendige for at lette vejen hen imod antagelse af bevismateriale i medlemsstaterne. På grund af cyberkriminalitetens grænseoverskridende karakter kan flere jurisdiktioner være involveret, hvilket kræver uddannelse på EU-plan. Og alligevel har Cepol, EU's agentur for uddannelse inden for retshåndhævelse, bemærket, at mere end to tredjedele af medlemsstaterne ikke tilbyder regelmæssig cyberuddannelse til det retshåndhævende personale[121]. EU kan også potentielt identificere metoder til at skabe synergi mellem uddannelse på det civile og det militære område[122]. Når det er sagt, har NISA konstateret, at selv om de nuværende uddannelsesmuligheder i kritiske sektorer er omfattende, har de ikke tilstrækkeligt fokus på modstandsdygtighed i kritisk infrastruktur[123].

Tabel 2 - Nogle af EU's cyberrelaterede uddannelsesinitiativer

Det Europæiske Forsvarsagenturs projekter, f.eks. om øvelsesstøtte fra den private sektor og om cybertestmiljøer (Cyber Ranges)	Det Europæiske Sikkerheds- og Forsvarsakademis netværk (tilbyder civil-militær uddannelse), herunder platformen for cyberuddannelse, træning, øvelser og evaluering	ENISA-arrangerede uddannelsesprogrammer, som kan tilbydes, når de ikke er tilgængelige på det kommercielle marked
Uddannelsesprogrammer under Europol, Cepol og ECTEG[124], bl.a. Training Governance Model og Training Competency Framework (herunder certificering)	Netværket af nationale kompetencecentre og et forskningskompetencecenter (foreslået)	Krypteringsforanstaltninger foreslået i den 11. statusrapport for sikkerhedsunionen
Samarbejdet mellem EU og NATO om cyberforsvarstræning- og uddannelse	Det militære Erasmusprogram	Det Europæiske Netværk for Uddannelse af Dommere og Anklagere

Kilde: Revisionsretten.

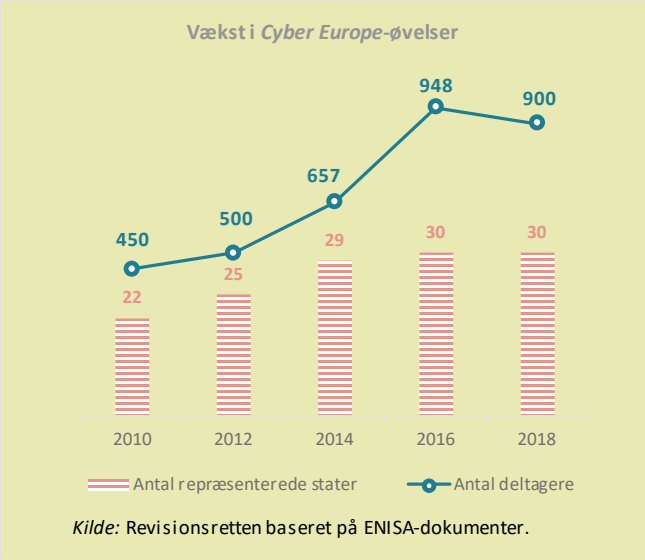
87 EU har udsendt eksperter i terrorbekæmpelse og sikkerhed til 17 delegationer for at styrke forbindelsen mellem EU's interne og eksterne sikkerhed[125] Uanset ressourcebegrænsningerne kan større knowhow på cyberområdet bidrage til at gennemføre de rette projekter samt identificere synergier med andre programmer og finansieringskilder[126]. Det kan også styrke cybersikkerhedens profil i den politiske dialog, selv om den kommer til at konkurrere med mange andre prioriteter, f.eks. migration, organiseret kriminalitet og hjemvendte fremmedkrigere.

Tekstboks 4

Øvelser

Øvelser er vigtige elementer i cyberuddannelse; de giver rig mulighed for at styrke beredskabet ved at teste dets kapacitet, tilbyde løsninger på virkelige scenarier og opbygge netværk af arbejdsforbindelser. Siden 2010 er deres hyppighed steget markant.

Deltagerne deltager på stedet eller via en fjernforbindelse. Der foretages vurderinger efter øvelserne for at afdække de gjorte erfaringer, men disse udveksles endnu ikke i fuldt omfang mellem det strategiske/politiske lag, det operationelle lag og det tekniske lag[127].



Kilde: Revisionsretten baseret på ENISA-dokumenter.

EU's og NATO's flagskibsøvelser - den toårige Cyber Europe (operationel) og den årlige Locked Shields (teknisk) - samler over 1 000 deltagere fra ca. 30 deltagende stater. Begge øvelser har fokus på at beskytte og opretholde kritisk infrastruktur i simulerede angrebsscenarier. Øvelserne er blevet betydeligt mere udførlige, og begge omfatter nu medierne samt elementer af rets- og finanspolitik for at forbedre aktørernes situationsforståelse. Parallelle og koordinerede PACE-øvelser (strategi) tester samspillet mellem EU og NATO i et hybridt krisescenarie.

Det er ikke de eneste internationale øvelser. ENISA tilrettelægger en årlig cyberudfordring, hvor team konkurrerer om at løse sikkerhedsrelaterede opgaver i kategorier såsom web- og mobilsikkerhed, crypto puzzles, dekompilering, etik og kriminalteknik. Den første øvelse på ministerielt niveau, EU CYBRID, fandt sted i september 2017 og havde fokus på strategisk beslutningstagning. I 2018 blev NATO-øvelsen Crossed Swords iværksat for at forbedre de offensive elementer i Locked Shields-øvelsen. NATO tilrettelægger også Cyber Coalition-øvelser.

En vigtig udfordring er at sikre den aktive deltagelse af alle vigtige interessenter og koordineringen af alle øvelserne samt at undgå overlapning og at udveksle erfaringer effektivt.

Bevidsthed

88 Borgerne er ofte vektorer for angreb og spredning af desinformation, da de ufrivilligt kan udsættes for sårbarheder i billigt og vidt udbredt udstyr og software eller bliver ofre for social engineering. Det er derfor afgørende at øge bevidsthedsniveauet for at opbygge en effektiv cyberrobusthed, men dette er på ingen måde en nem opgave, da det er vanskeligt for personer, der ikke er eksperter, at forstå cybersikkerhedens kompleksitet og de tilhørende risici.

89 Den årlige europæiske måned for øget bevidsthed om cybersikkerhed og sikkert internet-dagen er eksempler på bevidstgørelse. Syv ikke-EU-medlemsstater har nu tilsluttet sig den europæiske måned for øget bevidsthed om cybersikkerhed[128]. Europols *Say No!*- kampagne tager sigte på at mindske risikoen for, at børn bliver ofre for seksuel tvang og afpresning online. Det er vigtigt at mindske risikoen, fordi få ofre for angreb på nuværende tidspunkt anmelder disse forbrydelser til politiet[129]. Kommissionen erkender, at strategien for cybersikkerhed kun til dels har været effektiv med hensyn til at øge borgernes og erhvervslivets bevidsthed[130]. Dette skyldes opgavens omfang, de begrænsede ressourcer, medlemsstaternes uensartede engagement og den manglende videnskabelige dokumentation om, hvordan bevidstheden bedst øges og måles.

90 Den udfordring, som Kommissionen og de relevante agenturer står over for, er at sikre, at bevidstgørelsesforanstaltningerne er målrettede og kendte, inklusive og i overensstemmelse med trusselsbilledet og undgår utilsigtede virkninger såsom "security fatigue"[131], og at udvikle evalueringsmetoder og parametre til at vurdere deres effektivitet. Dette gælder i lige så høj grad inden for de europæiske institutioner, hvor bevidsthedskulturen bør forbedres[132].

Udfordring 8: Bedre informationsudveksling og koordinering

91 Cybersikkerhed kræver samarbejde mellem den offentlige og den private sektor, især med henblik på informationsudveksling og udveksling af bedste praksis. Tillid er afgørende på alle niveauer for at skabe det rette miljø for udveksling af følsomme oplysninger på tværs af grænserne. Dårlig koordinering fører til fragmentering, dobbeltarbejde og manglende formidling af ekspertise. Effektiv koordinering kan give mærkbare resultater, f.eks. lukning af markedspladser på det mørke net[133]. På trods af de fremskridt, der er gjort i de seneste år, er niveauet af tillid stadig utilstrækkeligt[134] på EU-plan og i en række medlemsstater[135].

Koordinering mellem EU-institutionerne og med medlemsstaterne

92 Et af formålene med strategien for cybersikkerhed og de samarbejdsstrukturer, der er indført med NIS-direktivet, har været at styrke tilliden mellem interessenterne. I vurderingen af strategien anerkendtes det, at der var dannet et grundlag for strategisk og operationelt samarbejde på EU-plan[136]. Til trods for dette er koordineringen generelt "utilstrækkelig"[137]. Udfordringen består i at sikre, at informationsudvekslingen ikke blot er hensigtsmæssig, men også giver mulighed for et fuldstændigt overblik over det store billede. I denne sammenhæng er det vigtigt at nå til en fælles forståelse, der er baseret på accepteret terminologi (jf. ***tekstboks 5***).

93 Ifølge ENISA-evalueringen var EU's tilgang til cybersikkerhed dog ikke tilstrækkeligt koordineret, hvilket resulterede i manglende synergi mellem ENISA's aktiviteter og andre interessenters aktiviteter. Samarbejdsmekanismerne er stadig relativt umodne[138]; forordningen om cybersikkerhed har til formål at tage fat på dette ved at styrke ENISA's koordinerende rolle. Ønsket om at styrke samarbejdet var begrundelsen for det aftalememorandum, der blev undertegnet i 2018 mellem ENISA, EDA, Europols EC3 og CERT-EU[139]. Det har prioritet for Kommissionen i de kommende år at sikre overensstemmelse mellem de politiske initiativer, behovene og investeringsprogrammerne for at afhjælpe fragmenteringen og skabe synergier[140].

94 Koordinationsfunktionerne hører under forskellige institutionelle organer. Taskforcen vedrørende sikkerhedsunionen blev oprettet for, at den kunne spille en central rolle i koordineringen af Kommissionens forskellige generaldirektorater med henblik på at støtte sikkerhedsunionens dagsorden[141]. GD CNECT leder taskforcens underarbejdsgruppe vedrørende cybersikkerhed.

95 I Rådet varetages cybersikkerheden af Den Horisontale Gruppe vedrørende Cyberspørgsmål, som koordinerer strategiske og horisontale cyberspørgsmål og hjælper med at forberede øvelser og evaluere resultaterne. Den arbejder tæt sammen med Den Udenrigs- og Sikkerhedspolitiske Komité, der har en central beslutningstagende rolle for så vidt angår cyberrelaterede diplomatiske foranstaltninger (jf. ***tekstboks 6*** i næste kapitel). Da cybersikkerhed er et tværgående emne, er det ikke ligetil at koordinere alle de relevante interesser: Ikke mindre end 24 arbejdsgrupper og forberedende organer har på det seneste behandlet cyberrelaterede spørgsmål[142].

96 De to seneste lovgivningsforslag om styrkelse af ENISA (2017) og om oprettelse af et netværk af kompetencecentre for cybersikkerhed og et forskningskompetencecenter (2018) er specifikt udformet til at afhjælpe

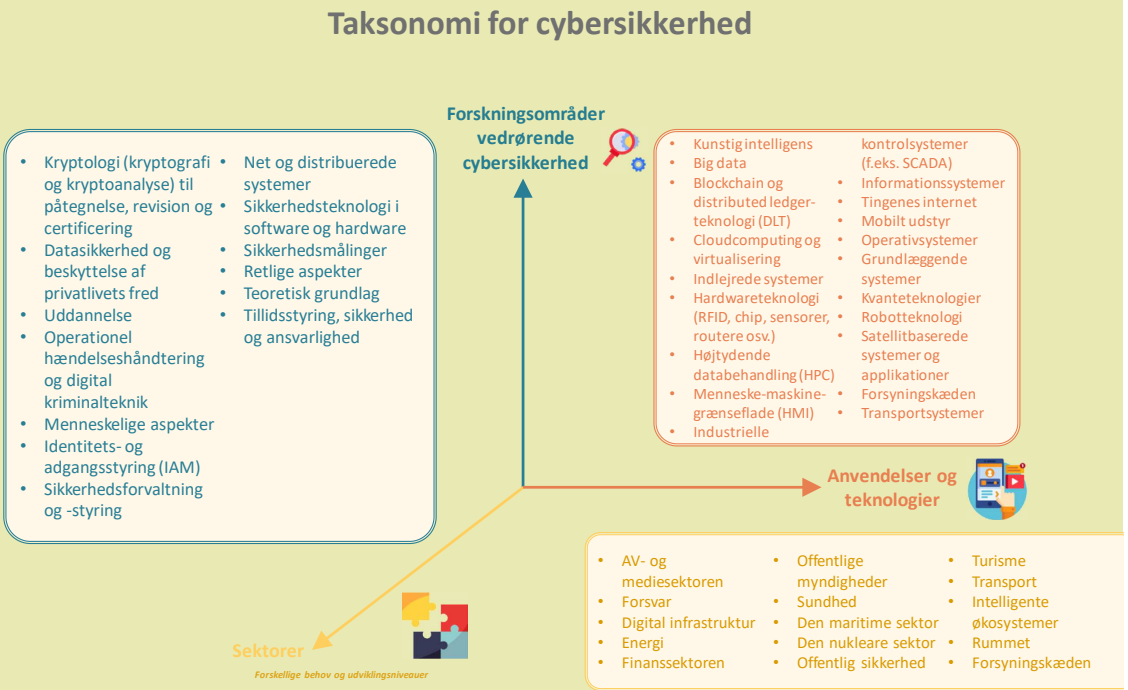
fragmentering og dobbeltarbejde. En vigtig drivkraft bag netværket af kompetencecentre for cybersikkerhed og et forskningskompetencecenter har været behovet for at lukke det hul, som NIS-direktivets samarbejdsstrukturer ikke udfylder, da de ikke blev ikke udformet med henblik på at støtte udviklingen af avancerede løsninger.

Tekstboks 5

Forsøg på at tale det samme cybersprog: *teknologisk sammenhæng*

Terminologisk klarhed forbedrer situationsforståelsen og koordineringen[143] og medvirker til at præcisere, hvad der udgør en trussel og en risiko.

Kommissionens Fælles Forskningscenter (JRC) har for nylig udarbejdet en revideret forskningtaksonomi på grundlag af forskellige internationale standarder[144]. Hensigten er, at den skal blive en reference, der kan anvendes som et indeks af forskningscentre i hele Europa.



Kilde: Revisionsretten, tilpassede data fra Europa-Kommissionen.

Indtil for nylig havde EU-institutionerne og -agenturerne ingen fælles definitioner. Det er ved at ændre sig. Samarbejdsgruppen har som led i sin arbejdsplan udarbejdet en taksonomi over hændelser med det formål at lette et effektivt samarbejde på tværs af grænserne.

Samarbejde og informationsudveksling med den private sektor

97 Samarbejde mellem offentlige myndigheder og den private sektor er afgørende for at styrke det overordnede niveau af cybersikkerhed. På trods af dette konstaterede Kommissionen i sin 2017-vurdering af strategien for cybersikkerhed, at informationsudvekslingen mellem private interessenter og mellem den offentlige og den private sektor endnu ikke var optimal, da der ikke er pålidelige rapporteringsmekanismer og incitamenter til at udveksle oplysninger[145], hvilket hæmmer opfyldelsen af strategiske mål. Kommissionen har også bemærket, at der mangler en effektiv samarbejdsmekanisme, inden for hvilken medlemsstaterne kan samarbejde om strategisk at fremme varig industriel kapacitet i stor skala[146].

98 Centre for informationsudveksling og analyse (ISAC'er) er organisationer, der er oprettet for at tilbyde platforme og ressourcer til at lette informationsudvekslingen mellem den offentlige og den private sektor samt for at indsamle oplysninger om cybertrusler. De tager sigte på at opbygge tillid gennem udveksling af erfaringer, viden og analyser, navnlig om grundlæggende årsager, hændelser og trusler. Der findes allerede nationale og sektorspecifikke ISAC'er i mange medlemsstater, men på europæisk plan er de stadig relativt begrænsede[147]. De er imidlertid forbundet med en række udfordringer (ressourcemæssige begrænsninger, vanskeligheder med at evaluere deres succes, sikring af de rette strukturer for inddragelse af både den offentlige og den private sektor, inddragelse af de retshåndhævende myndigheder), der skal tackles, hvis ISAC'erne skal bidrage til at gennemføre NIS-direktivet og opbygge sikkerhedskapaciteten på europæisk plan[148].

99 Et tæt samarbejde med den private sektor er især afgørende for at bekæmpe kompleks cyberkriminalitet, men effektiviteten af samarbejdet er ujævnt i medlemsstaterne og afhænger af tillidsniveauet[149] Europols EC3 har imidlertid nedsat en række rådgivende grupper med aktører fra den private sektor, EU-institutionerne og -agenturerne og andre internationale organisationer for at forbedre samarbejdet gennem netværksarbejde og udveksling af strategiske efterretningsoplysninger. De arbejder i henhold til planer, der er i overensstemmelse med målene for EU's politikcyklus[150]. De kriminelle aktiviteter i forbindelse med kryptering er et andet område med udfordringer, der kræver øget samarbejde med den private sektor. Europols EC3 er på nuværende tidspunkt ved at undersøge mulighederne for fra sag til sag at tilknytte eksperter fra den private sektor og akademiske kredse til J-CAT i korte perioder (jf. punkt ***62***).

100 Der mangler effektive samarbejdsmekanismer mellem den civile sektor og forsvarssektoren - såvel offentlige som private. Områder, der udgør en fælles udfordring, omfatter kryptografi, indlejrede systemer, detektion af malware, simuleringsteknikker, beskyttelse af net- og kommunikationssystemer og autentifikationsteknologi. Fremme af civil-militært samarbejde og støtte til forskning og teknologi (navnlig støtte til SMV'er) er to af prioriteterne i den ajourførte ramme for EU's cyberforsvarspolitik (2018-ajourføring).

Refleksionspunkter - Opbygning af modstandsdygtighed

- Hvordan kan der på EU-plan opnås den rette balance mellem behovet for at integrere cybersikkerhedspolitikken i andre politikker og behovet for at sikre en effektiv koordinering mellem de forskellige aktører og en hensigtsmæssig ansvarsfordeling?
- Hvor velforberedte er EU-institutionerne og -agenturerne på det næste store angreb, der rettes direkte mod dem?
- Hvordan kan EU-agenturerne for cyberspørgsmål gøres mere attraktive for talenter?
- Hvilke yderligere skridt er nødvendige for at sikre tilstrækkelig kapacitet i EU-institutionerne og -agenturerne til at muliggøre en sammenhængende ramme for risiko- og trusselsvurdering?
- På hvilke måder tackler de europæiske tilsynsmyndigheder (Den Europæiske Banktilsynsmyndighed, Den Europæiske Værdipapir- og Markedstilsynsmyndighed og Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger) cybersårbarheder i finanssektoren, og hvad kan der læres herfra med henblik på andre sektorer?
- I lyset af den generelle mangel på ekspertise, hvordan kan EU's tekniske bistand til de offentlige myndigheder bedst anvendes til at opnå den størst mulige samlede virkning med hensyn til forbedring af cyberrobustheden?
- Hvordan kan EU og medlemsstaterne sikre en meningsfyldt deltagelse i internationale drøftelser med henblik på at forme cyberspaceforvaltningen og -standarderne og fremme EU's værdier?
- Hvilke bevidstgørelsestiltag (herunder forebyggelsesindsatser) i EU og medlemsstaterne gør rent faktisk en forskel, og hvordan kan EU bidrage til at styrke dem?
- Hvilken rolle kan EU spille for at bidrage til at fremme kønsdiversitet på cybersikkerhedsområdet?
- Hvordan kan EU og medlemsstaterne styrke synergierne mellem den civile sektor og forsvarssektoren i overensstemmelse med rammen for EU's cyberforsvarspolitik (2018-ajourføring)?

Effektiv reaktion på cyberhændelser

101 En effektiv reaktion på cyberangreb er afgørende for at standse dem så tidligt som muligt. Det er især vigtigt, at de kritiske sektorer, medlemsstaterne og EU-institutionerne er i stand til at reagere hurtigt og koordineret. En væsentlig forudsætning for dette er tidlig detektering.

Udfordring 9: Effektiv detektering og reaktion

Detektering og underretning

102 Almindelige detektionsværktøjer gør det hver dag muligt at afvise langt de fleste angreb[151]. De digitale systemer er imidlertid blevet så komplekse, at det er umuligt at forhindre alle angreb. Nogle af dem er så sofistikerede, at de forbliver uopdagede i lang tid. Ifølge eksperterne bør man derfor fokusere på hurtigt at detektere angreb og forsvare sig mod dem[152]. Nogle detektionsværktøjer - såsom automatisering, maskinindlæring og adfærdsanalyse, der sigter mod at reducere risici og at analysere og lære af systemadfærd - har imidlertid kun vundet ringe udbredelse blandt virksomheder[153]. Det skyldes delvis de falsk positive resultater, hvor ufarlige aktiviteter fejlagtigt identificeres som skadelige.

103 Når et brud på datasikkerheden er blevet afsløret og analyseret, er der brug for hurtig underretning og rapportering, så andre offentlige og private enheder kan træffe forebyggende foranstaltninger, og de relevante myndigheder kan støtte de berørte. Mange organisationer er tilbageholdende med at anerkende og rapportere om cyberhændelser[154]. Det er også afgørende at inddrage retshåndhævende myndigheder i forbindelse med den første reaktion på formodet cyberkriminalitet og at sikre en proaktiv informationsudveksling med CSIRT'er.

104 Den tidligere mangel på fælles EU-krav vedrørende underretning om hændelser kunne forsinke meddelelser om brud på datasikkerheden og svække reaktionen. Formålet med NIS-direktivet var at afhjælpe dette problem (jf. punkt ***20***). Efter angrebene med Wannacry i 2017 konkluderede Kommissionen, at CSIRT-netværket "endnu ikke var fuldt operationelt"[155]. Gennemførelsen af direktivet fortsætter, og det vil vise sig, om de retningslinjer, der er udarbejdet af samarbejdsgruppen, vil være effektive med hensyn til at overvinde modviljen mod at rapportere om hændelser[156].

105 I visse sektorer pålægger de eksisterende EU-forordninger operatører af væsentlige tjenester mange underretningsforpligtelser (bl.a. over for forbrugerne), hvilket kan svække processens effektivitet. F.eks. er operatører i den finansielle sektor og banksektoren underlagt forskellige kriterier, standarder, grænseværdier og frister for underretning, som er fastsat i GDPR, NIS-direktivet, betalingstjenestedirektivet, ECB/FTM, Target2 og eIDAS-forordningen[157]. Det er derfor vigtigt at strømline disse forpligtelser, eftersom uensartetheden - ud over at skabe en unødig administrativ byrde - kan føre til usammenhængende rapportering.

Koordineret reaktion

106 Den europæiske krisekoordineringsramme for cybersikkerhed er stadig under udvikling. Den dertil knyttede plan[158] (jf. punkt ***18***), blev derfor udarbejdet for at tilføre de integrerede ordninger for politisk kriserespons (IPCR) et cyberperspektiv, forbedre situationsforståelsen og sikre bedre integration med andre EU-krisestyringsmekanismer[159]. Planen omfatter EU's institutioner og agenturer samt medlemsstaterne. Det er en udfordring at integrere alle disse kriseberedskabsmekanismer problemfrit[160]. Den aktuelle mangel på et fælles sikkert kommunikationsnet i EU-institutionerne er også en stor svaghed[161].

107 EU's kapacitet til at reagere på cyberangreb på operationelt og politisk plan i tilfælde af en væsentlig, grænseoverskridende hændelse er blevet betegnet som "begrænset", delvis fordi cybersikkerhed endnu ikke er integreret i de nuværende samordningsmekanismer for kriseberedskab på EU-plan[162]. NIS-direktivet adresserede ikke dette forhold.

108 Den nyligt foreslåede reform af ENISA, som skulle give agenturet en større operationel rolle i håndteringen af væsentlige cybersikkerhedshændelser, blev ikke støttet af medlemsstaterne, som foretrækker, at det støtter og supplerer deres egne operationelle tiltag[163]. Der findes allerede mange CERT'er/CSIRT'er på medlemsstatsniveau, men deres kapacitet varierer betydeligt. Dette udgør en hindring for det effektive grænseoverskridende samarbejde, der er nødvendigt i forbindelse med reaktion på væsentlige hændelser[164].

109 Vi forsøgte at kortlægge de roller, der var tildelt de forskellige aktører i planen, men vi konstaterede mangler, der bør udbedres, efterhånden som gennemførelsen skrider frem. Retshåndhævelse var et af de områder, der var utilstrækkeligt behandlet, selv om EU's beredskabsprotokol i forbindelse med retshåndhævelse trådte i kraft i december 2018[165]. Det er afgørende for planens succes at sikre, at den er praktisk

gennemførlig, og at alle parter ved, hvad de skal gøre. Dette vil kræve omfattende testning i de kommende år.

110 Effektiv reaktion handler ikke kun om at begrænse skaderne - det er også afgørende at få placeret ansvaret for angrebene. Især i forbindelse med hybride angreb kan det være meget vanskeligt at spore og identificere gerningsmænd på grund af det stigende misbrug af anonymiseringsværktøjer, kryptovalutaer og kryptering. Dette kaldes placeringsproblemet. At afhjælpe dette problem er ikke blot et teknisk spørgsmål, men også en strafferetlig udfordring. Retlige og proceduremæssige forskelle mellem lande kan vanskeliggøre den strafferetlige efterforskning og retsforfølgelsen af mistænkte. Placeringsproblemet kan kun afhjælpes ved, at der indføres klarere procedurer for en mere formaliseret operationel udveksling af oplysninger med f.eks. Europol eller Eurojusts Retlige Netværk for Cyberkriminalitet.

111 På det politiske plan er den cyberdiplomatiske værktøjskasse (jf. ***tekstboks 6***) blevet udarbejdet med henblik på at støtte bilæggelse af internationale tvister i cyberspace med fredelige midler. To af de projekter til fremme af øget informationsudveksling, som udvikles inden for rammerne af PESCO, er oprettelsen af cyberberedskabshold og initiativet om gensidig bistand inden for cybersikkerhed[166].

Tekstboks 6

Den cyberdiplomatiske værktøjskasse

EU's fælles diplomatiske reaktion på ondsindede cyberaktiviteter[167] eller "cyberdiplomatiske værktøjskasse" udsprang af Rådets 2015-konklusioner om cyberdiplomati[168]. Cyberdiplomati sigter mod at udvikle og gennemføre en fælles og samlet tilgang til cyberspace baseret på EU's værdier, retsstatsprincippet, kapacitetsopbygning og partnerskaber, fremme af flerpartsmodellen for internetforvaltning, afbødning af trusler mod cybersikkerheden og opnåelse af større stabilitet i internationale forbindelser.

Værktøjskassen giver EU og medlemsstaterne mulighed for at iværksætte en fælles diplomatisk reaktion på ondsindede cyberaktiviteter med fuld anvendelse af foranstaltninger under den fælles udenrigs- og sikkerhedspolitik. Det kan være foranstaltninger med fokus på forebyggelse (f.eks. bevidstgørelse eller kapacitetsopbygning), på samarbejde, stabilitet og restriktioner (f.eks. rejseforbud, våbenembargo, indefrysning af midler), eller på støtte til medlemsstaternes reaktion[169]. Tanken er, at et stærkere samarbejde om imødegåelse trusler og et klart signal om de sandsynlige konsekvenser af en fælles indsats kan modvirke (potentielt) aggressiv adfærd.

En fælles EU-reaktion på ondsindede cyberaktiviteter skal stå i rimeligt forhold til cyberaktivitetens omfang, størrelse, varighed, intensitet, kompleksitet, sofistikerede karakter og virkninger.

Det er afgørende for værktøjskassens succes, hvor godt den integreres i planen og IPCR (jf. punkt ***106***), hvor godt der etableres en situationsforståelse gennem hurtig og kontinuerlig udveksling af oplysninger (bl.a. om ansvarsplaceringen)[170], og hvor effektivt der samarbejdes. Effektiv og koordineret kommunikation er også central for en vellykket anvendelse af værktøjskassen. Værktøjskassen er hidtil blevet brugt to gange: Til at indlede en dialog med USA efter angrebet med Wannacry[171] og til at udarbejde rådskonklusioner om fordømmelse af ondsindet brug af IKT[172]. Operationaliseringen af værktøjskassen er i gang. Det vil vise sig, hvor effektiv den bliver med hensyn til at opfylde sine mål.

Udfordring 10: Beskyttelse af kritisk infrastruktur og kritiske samfundsmæssige funktioner

Beskyttelse af infrastruktur

112 En stor del af EU's kritiske infrastruktur styres af industrielle styringssystemer (ICS'er)[173]. Mange af disse blev oprindelig udformet som selvstændige systemer med begrænset forbindelse til omverdenen. Efterhånden som ICS-komponenter er blevet tilsluttet internettet, er de blevet mere sårbare over for påvirkning udefra. På et tidspunkt er det ikke længere muligt at vedligeholde og patche de eksisterende systemer, men det er hverken hurtigt eller billigt at opgradere dem. Indsatsen for at forbedre sikkerheden i de kritiske infrastrukturer skal derfor også omfatte opgradering af ICS'er.

113 Eftersom industrien fortsætter med at digitalisere (ofte kaldet "Industri 4.0"), kan en væsentlig hændelse i én industrisektor have afsmittende virkninger andre steder. ENISA har bemærket vigtigheden af at kortlægge effekten af de kritiske sektorers indbyrdes afhængighed[174]. Dette er vigtigt for at forstå en hændelses potentielle spredning og er en forudsætning for velkoordinerede reaktioner.

114 NIS-direktivet sigter mod at styrke beredskabet i vigtige sektorer med ansvar for kritisk infrastruktur. Det er imidlertid ikke alle sektorer, der er dækket (jf. ***tabel 1***)[175], hvilket ifølge Kommissionen reducerer strategiens effektivitet[176]: I denne henseende er det særlig vigtigt at sikre valghandlingers demokratiske integritet ved at beskytte mod påvirkning af valgrelateret infrastruktur og mod desinformation

(jf. ***tekstboks 7***). Ud over ændringer af den eksisterende lovgivning vil det derfor være en central udfordring at se på, hvordan disse sektorer kan inddrages i effektive reaktioner på væsentlige hændelser.

115 Sårbarhederne i den kritiske infrastruktur standser ikke ved Europas grænser. Det er en særlig udfordring for Kommissionen at tilskynde kandidatlandene til at vedtage de samme standarder som medlemsstaterne, f.eks. på områder såsom cyberrelateret lovgivning og beskyttelse af kritisk infrastruktur.

Tekstboks 7

Beskyttelse af kritiske samfundsmæssige funktioner: *bekæmpelse af valgindblanding*

I maj 2019 går ca. 400 millioner vælgere til valgurnerne for at stemme i det første valg til Europa-Parlamentet, der finder sted efter GDPR's ikrafttrædelse. Valget kommer kort tid efter skandalerne om misbrug af personoplysninger til politisk micro-targeting og koordinerede desinformationskampagner ("fake news") i et hidtil uset omfang. Kommissionen har advaret om, at der sandsynligvis vil være forsøg på cyberbaseret indblanding i dette valg[177]. Det vil kræve en samlet indsats fra hele den offentlige sektor og hele samfundet at bekæmpe denne indblanding.

Valginfrastruktur

Det er en kompleks opgave at afholde valg, og det er medlemsstaternes ansvar at beskytte valghandlingens integritet. Indblanding i valg og påvirkning af valgrelateret infrastruktur kan have til formål at øve indflydelse på vælgernes præferencer, valgdeltagelsen eller selve valgprocessen, herunder stemmeafgivningen, foruden stemmeoptællingen og kommunikationen om valget. I valget til Europa-Parlamentet er det en særlig kritisk udfordring at beskytte den såkaldte "sidste kilometer" (meddelelsen af resultater fra de nationale hovedstæder til Bruxelles), da der hverken er etableret eller testet en fælles sikkerhedstilgang til dette formål[178].

Kommissionens nyligt udarbejdede valgpakke omfatter foranstaltninger til at styrke cybersikkerheden i forbindelse med valget, f.eks. udpegelse af nationale kontaktpunkter til at koordinere og udveksle oplysninger i tiden op til valget. Udveksling af bedste praksis og indhøstede erfaringer har særlig stor betydning[179].

Valgsystemer betragtes ikke som en del af den kritiske infrastruktur[180], og de er heller ikke omfattet af NIS-direktivet. Trods dette har samarbejdsgruppen udviklet en praktisk vejledning om sikkerhed i forbindelse med valgteknologi for at støtte de offentlige myndigheder. De nationale kontaktpunkter forventes at mødes i begyndelsen af 2019[181]. Medlemsstaterne opfordres også til at foretage risikovurderinger vedrørende cybertrusler mod deres valgprocesser.

Desinformation

Desinformation er et stadig vigtigere element i hybride angreb, der også omfatter cyberangreb og hacking af net. Desinformation kan bruges til at splitte samfund, skabe mistro og undergrave tilliden til demokratiske processer eller andre tiltag (f.eks. i den offentlige debat om vaccination eller klimaændringer). Den er vokset i omfang, hastighed og rækkevidde og udgør en reel sikkerhedstrussel for EU.

EU har truffet en række foranstaltninger til at adressere desinformation. I 2015 blev EU-Udenrigstjenestens East StratCom Task Force oprettet som reaktion på Ruslands desinformationskampagner[182]. Eksperter har rost dens arbejde med fremme af EU's politikker, støtte til uafhængige medier i naboskabsområdet samt forudsigelse, sporing og bekæmpelse af desinformation[183]. Taskforcens ressourcer er imidlertid begrænsede sammenlignet med omfanget og kompleksiteten af desinformationskampagnerne[184]. Der er brug for et mere systematisk samspil med de eksisterende EU-strukturer og et bedre strategisk kommunikationssamarbejde[185]. En ny handlingsplan[186] blev godkendt af Det Europæiske Råd i december 2018.

Senest har Kommissionen på baggrund af sin meddelelse fra april 2018 om bekæmpelse af desinformation på nettet[187] udviklet en frivillig, selvregulerende adfærdskodeks[188] baseret på eksisterende politikinstrumenter, som onlineplatforme og reklamebranchen har tilsluttet sig[189]. Tiltagene omfatter hjælp til at øge troværdigheden af indhold og støtte til bestræbelser på at fremme medie- og nyhedskendskab. Et uafhængigt europæisk netværk af faktatjekkere er også blevet lanceret.

Kommissionen har udtalt, at der kan komme yderligere lovgivningsmæssige foranstaltninger, hvis adfærdskodeksen ikke bliver overholdt. Vurderingen af tiltagenes effektivitet vil få stor betydning, herunder især fastlæggelsen af, hvordan forbedringer med hensyn til tillid, gennemsigtighed og ansvarlighed skal måles.

En anden udfordring vil være at finde metoder til at forbedre opdagelsen, analysen og blotlæggelsen af desinformation[190]. Der er også brug for aktiv og strategisk overvågning og analyse af åbne datakilder[191]. Forsøg på at få en bedre forståelse af trusselsmiljøet bør også omfatte nye tendenser såsom "deepfakes" (falske videoer lavet ved hjælp af kunstig intelligens og dyb maskinindlæring) såvel som de nødvendige redskaber til at detektere dem.

Større autonomi

116 EU er nettoimportør af cybersikkerhedsprodukter og -tjenester, hvilket øger risikoen for teknologisk afhængighed af og sårbarhed over for operatører fra ikke-EU-lande[192]. Dette forhold underminerer navnlig sikkerheden i EU's kritiske infrastruktur, som også understøttes af komplekse globale forsyningskæder. Risikoen forværres

yderligere, når operatører fra ikke-EU-lande erhverver europæiske cybersikkerhedsvirksomheder. Medlemsstaterne er ansvarlige for at screene udenlandske direkte investeringer, og der findes på nuværende tidspunkt ingen EU-dækkende screeningsmekanisme[193].

117 Større strategisk autonomi er angivet som mål i EU's globale strategi og 2017-meddelelsen *Modstandsdygtighed, afskrækkelse og forsvar*[194]. Adressering af de utallige udfordringer, der er beskrevet i dette dokument, vil bidrage til at opnå den ønskede autonomi. Men ingen enkeltstående foranstaltning kan gøre det.

Refleksionspunkter - Effektiv reaktion

- Hvordan har NIS-direktivet forbedret underretningen om cyberhændelser i kritiske sektorer og andre steder?
- Hvor gode er EU-institutionerne til at internalisere deres kriseberedskabssamordning med henblik på en væsentlig cyberhændelse?
- Hvordan kan cyberdiplomati spille en mere fremtrædende rolle i EU's foranstaltninger udadtil?
- Står de nuværende EU-strukturer og -aktioner til håndtering af desinformation i et rimeligt forhold til problemets omfang og kompleksitet?

Afsluttende bemærkninger

118 I de seneste år har EU og medlemsstaterne sat cybersikkerhed højere på dagsordenen for at forbedre den overordnede cyberrobusthed. Ikke desto mindre er det fortsat en monumental opgave at nå et højere cybersikkerhedsniveau i Unionen. I dette briefingpapir har vi forsøgt at fremhæve nogle af de største udfordringer for EU's ambitionsniveau om at blive verdens sikreste digitale miljø.

119 Vores analyse viser, at et skift i retning af en resultatorienteret kultur med etablerede evalueringspraksis er nødvendigt for at sikre fornuftig **ansvarliggørelse og evaluering**. Der er fortsat nogle **huller i EU-retten, og den nuværende lovgivning gennemføres ikke ensartet af medlemsstaterne**. Dette kan gøre det vanskeligt for lovgivningen at nå sit fulde potentiale. En anden udfordring vedrører **tilpasning af investeringsniveauerne til de strategiske mål**, hvilket kræver opskalering af investeringerne og deres virkninger. Dette er endnu mere krævende, fordi EU og dets medlemsstater ikke har et **klart overblik over EU's udgifter** til cybersikkerhed. Der er også rapporteret om **ressourcemæssige begrænsninger i EU's agenturer for cyberspørgsmål**, bl.a. vanskeligheder med at tiltrække nye talenter og holde på dem.

120 Det konkluderes i forskellige undersøgelser, at **forvaltningen af cybersikkerhed kan styrkes** for at øge det globale samfunds evne til at reagere på cyberangreb og -hændelser. Det er dog ikke muligt at forhindre alle angreb. Derfor er **hurtig detektering og reaktion** og **beskyttelse af kritisk infrastruktur og kritiske samfundsmæssige funktioner** samt bedre **informationsudveksling og koordinering** mellem den offentlige og den private sektor nogle af de centrale udfordringer, der skal tackles. Endelig betyder den stigende globale mangel på cybersikkerhedskompetencer, at det også er en vital udfordring at **øge kompetence- og bevidsthedsniveauet**.

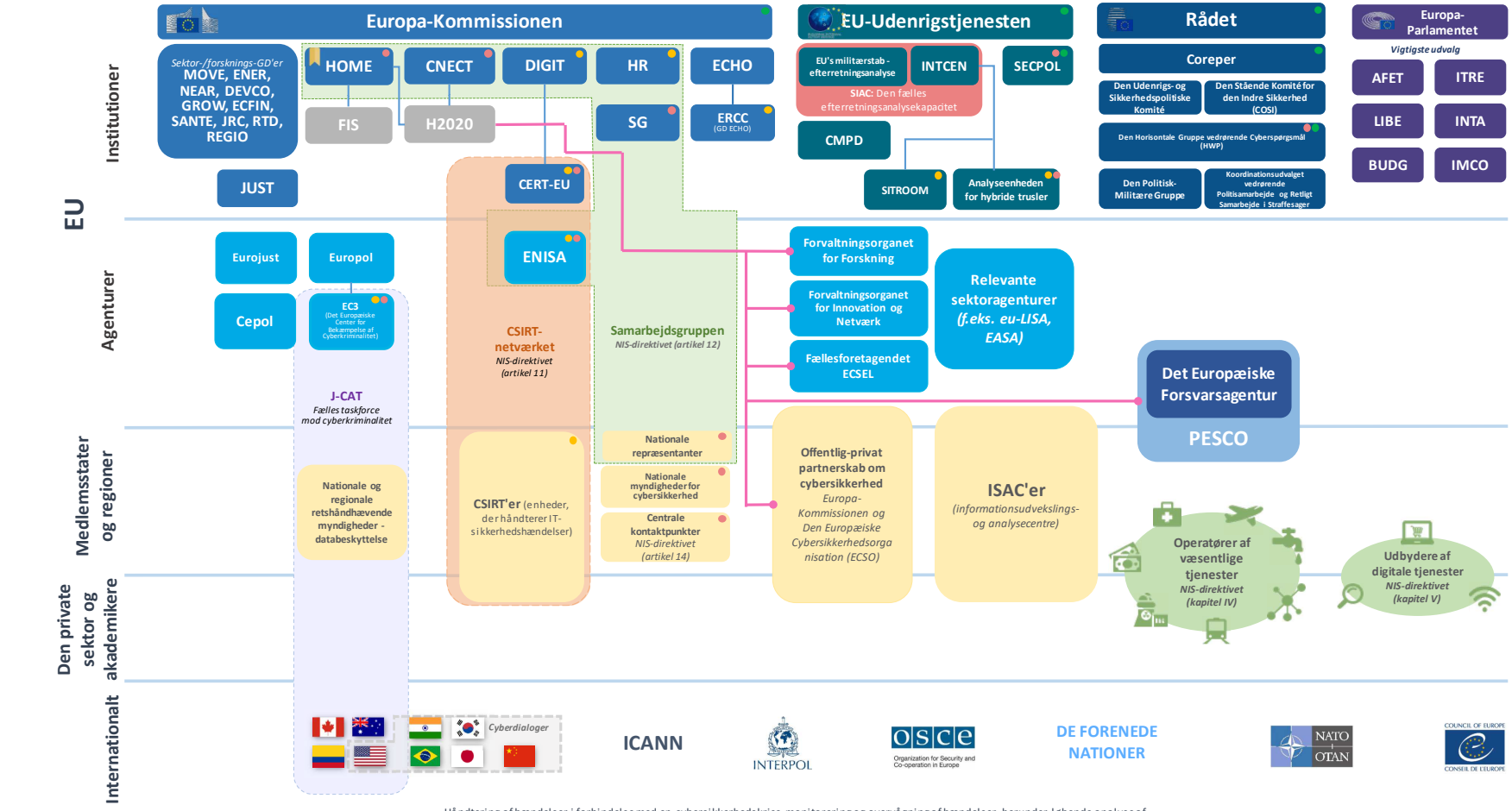
121 Disse cybertrusselsrelaterede udfordringer, som EU og det internationale samfund står over for, kræver et fortsat engagement i og en vedvarende loyalitet over for EU's værdier.

Vedtaget af Afdeling III på mødet den 14. februar 2019.

På Revisionsrettens vegne

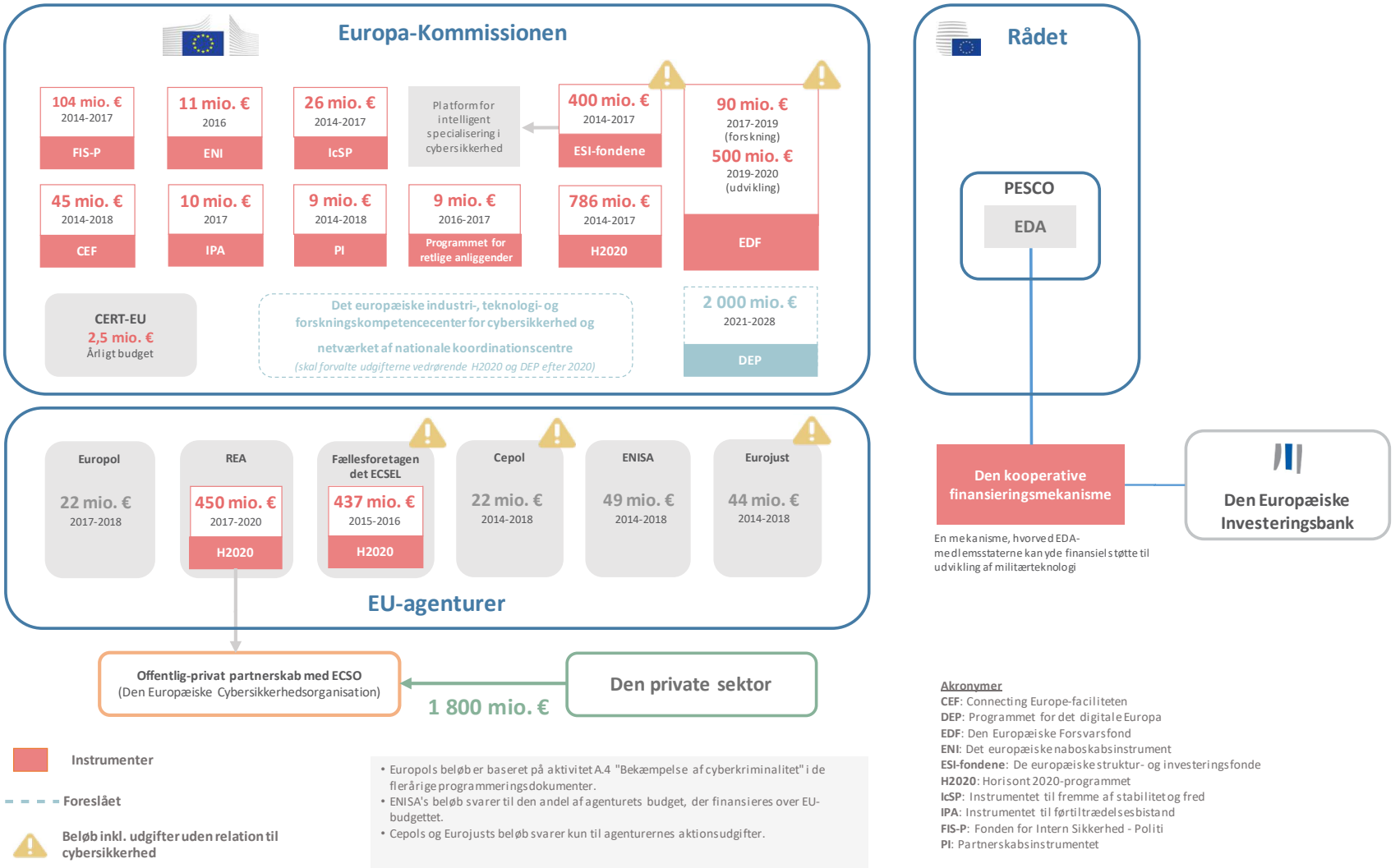
Klaus-Heiner Lehne
Formand

Bilag I — Et komplekst landskab med mange lag og aktører



Kilde: Revisionsretten.

Bilag II — EU's udgifter til cybersikkerhed siden 2014



Kilde: Revisionsretten på grundlag af dokumenter fra Europa-Kommissionen og EU-agenturerne.

Bilag III — Beretninger fra EU-medlemsstaternes revisionsorganer

Type	Titel (med hyperlink)	År	Medlemsstat
Juridisk-kritiske revisioner	Note vedrørende vurdering af den interne kontrol	2014	FR
	Attesteringsrapport vedrørende den almindelige sociale sikringsordnings regnskaber (forsvar, udenrigsanliggender)	2016	FR
	Attestering af statsregnskabet	2016	FR
	Sikring af sikkerheden og opretholdelsen af estiske nationale databaser af kritisk betydning	Afsluttet 2018/endnu ikke offentliggjort	EE
	Effektiviteten af intern kontrol vedrørende beskyttelsen af personoplysninger i nationale databaser	2008	EE
Forvaltningsrevisioner/"value-for-money"-revisioner	Beretning om forebyggelse af hackerangreb	2013	DK
	RiR 2014:23 Informationssikkerheden i den civile statsforvaltning	2014	SE
	Beretning om statens behandling af fortrolige oplysninger om personer og virksomheder	2014	DK
	Det nationale cybersikkerhedsprogram	2014	UK
	Beretning til budgetudvalget i den tyske Forbundsdag i henhold til artikel 88, stk. 2, i forbundsbudgetreglerne (BHO) - IT-konsolidering, forbundsregeringen	2015	DE
	Beretning om adgangen til it-systemer, der understøtter samfundsvigtige opgaver	2015	DK
	Myndigheden for offentlig planlægning, Plaine de France	2015	FR
	Cybersikkerhedssituationen i Litauen litauisk udgave sammendrag oversat til engelsk	2015	LT
	Offentlige myndigheders udførelse af cybersikkerhedsrelaterede opgaver i Polen (polsk udgave)	2015	PL
	RiR 2015:21 Cyberkriminalitet - politi og anklagere kan være mere effektive	2015	SE
	Kløften for så vidt angår digitale færdigheder i staten (undersøgelse)	2015	UK
	Beretning til det belgiske parlament: Føderale finanser: opkrævning af arveafgift	2016	BE
	Beretning om styring af it-sikkerhed hos it-leverandører	2016	DK
	Revisionsberetning om låneaktiviteten i det officielle kreditinstitut 2016	2016	ES

Type	Titel (med hyperlink)	År	Medlemsstat
	Styring af det statslige sikkerhedsnet	2016	FI
	Sikring af sikkerheden i IT-systemer, der anvendes til offentlige opgaver	2016	PL
	Forebyggelse og bekæmpelse af cybermobning blandt børn og unge	2016	PL
	Informationssikkerhedsarbejdet i ni agenturer - En anden revision om informationssikkerhed på statsniveau. RiR 2016:8	2016	SE
	Beskyttelse af oplysninger i de statslige myndigheder	2016	UK
	Beretning om 3 regioners beskyttelse af adgangen til it-systemer og sundhedsdata	2017	DK
	Note vedrørende resultaterne af den internationale parallelrevision om effektiviteten af intern kontrol vedrørende beskyttelsen af personoplysninger i nationale databaser.	2017	EE
	Cyberbeskyttelsesordninger	2017	FI
	Styring af den operationelle pålidelighed af elektroniske tjenester	2017	FI
	Landbrugssammenslutningens net (sammenfattende rapport)	2017	FR
	Vaucluse, Industri- og handelskammeret (fra det regionale revisionsorgan for PACA)	2017	FR
	Sikring af sikkerheden og opretholdelsen af estiske nationale databaser af kritisk betydning	Afsluttet 2018/endnu ikke offentliggjort	EE
	Udvikling af statens elektroniske kommunikationsinfrastruktur litauisk udgave sammendrag oversat til engelsk	2017	LT
	Informationsteknologirevision: Cybersikkerhed i offentlige enheder	2017	MT
	Det nationale registersystems sikkerhed, ydeevne og anvendelighed	2017	PL
	WannaCry-angrebet	2017	UK
	Onlinesvig	2017	UK
	Beretning om beskyttelse mod ransomwareangreb	2018	DK
	Arpajon Hospital (fra det regionale revisionsorgan for Île-de-France)	2018	FR
	Forvaltning af statens kritiske informationsressourcer	2018	LT
	Elektroniske forbrydelser	2019	LT
	Informationssikkerhed i Polen	2019	PL

Type	Titel (med hyperlink)	År	Medlemsstat
Andet	Database over offentlige organer	Ikke relevant	BE
	Spørgeskema om politikken vedrørende sikkerheds- og risikoanalyser (igangværende)	Ikke relevant	BE

Akronymer og forkortelser

CERT-EU: IT-Beredskabsenheden

cPPP: Det kontraktlige offentlig-private partnerskab

CSIRT: Enhed, der håndterer IT-sikkerhedshændelser

DDoS: Distribueret Denial of Service

DEP: Programmet for det digitale Europa

EC3: Europols Europæiske Center for Bekæmpelse af Cyberkriminalitet

ECSEL: Fællesforetagendet vedrørende elektronikkomponenter og -systemer for europæisk førerskab

ECSO: Den Europæiske Cybersikkerhedsorganisation

EDA: Det Europæiske Forsvarsagentur

ENISA: Det Europæiske Agentur for Net- og Informationssikkerhed

ESI-fondene: De europæiske struktur- og investeringsfonde

EU: Den Europæiske Union

EU-Udenrigstjenesten: Tjenesten for EU's Optræden Udadtil

FIS-P: Fonden for Intern Sikkerhed - Politi

FSFP: Den fælles sikkerheds- og forsvarspolitik

GD CNECT: Generaldirektoratet for Kommunikationsnet, Indhold og Teknologi

GD DIGIT: Generaldirektoratet for Informationsteknologi

GD HOME: Generaldirektoratet for Migration og Indre Anliggender

GD JUST: Generaldirektoratet for Retlige Anliggender og Forbrugere

GDPR: Den generelle forordning om databeskyttelse

ICS: Industrielt styringssystem

JRC: Det Fælles Forskningscenter

LISO: Lokal IT-sikkerhedsansvarlig

NIS-direktivet: Direktivet om net- og informationssikkerhed

PESCO: Det permanente strukturerede samarbejde

SMV'er: Små og mellemstore virksomheder

Glossar

Adgangsdata: Oplysninger om en brugers log in- og log out-aktivitet vedrørende en bestemt tjeneste, f.eks. tidspunkt, dato og IP-adresse.

Adware: Skadelig software, der viser reklamebannere eller pop op-vinduer, som indeholder kode til at registrere ofres adfærd på internettet.

Botnet: Et netværk af computere, der er blevet inficeret med malware og fjernstyres til at sende spammail, stjæle oplysninger eller iværksætte koordinerede cyberangreb, uden at brugerne ved det.

Cloudcomputing: On-demand levering over internettet af IT-ressourcer fra fjernservere - f.eks. lagring, datakraft eller datadelingskapacitet.

Crime-as-a-service-modellen: En fremherskende kriminel forretningsmodel i den digitale undergrundsøkonomi, som tilbyder en bred vifte af kommercielle tjenester og værktøjer, der giver cyberkriminelle på begynderniveau mulighed for at begå cyberkriminalitet.

Cyberangreb: Et forsøg på at underminere eller ødelægge fortroligheden, integriteten og tilgængeligheden af data eller et computersystem via cyberspace.

Cyberbaseret kriminalitet: En traditionel forbrydelse begået i større målestok ved hjælp af IT-systemer.

Cyberforsvar: Den del af cybersikkerheden, der sigter mod at forsvare cyberspace med militære og andre egnede midler for at nå militære og strategiske mål.

Cyberhændelse: En begivenhed, der direkte eller indirekte skader eller truer modstandsdygtigheden og sikkerheden af et IT-system og de data, som det behandler, opbevarer eller formidler.

Cyberkriminalitet: Forskellige kriminelle aktiviteter, hvor computere og IT-systemer enten er de primære værktøjer eller de primære mål. Der kan være tale om traditionelle forbrydelser (f.eks. svig, forfalskning og identitetstyveri), indholdsrelaterede forbrydelser (f.eks. onlinedistribution af børnepornografi eller tilskyndelse til racehad) og forbrydelser, der udelukkende vedrører computere og informationssystemer (f.eks. systemangreb, denial of service-angreb og malware).

Cyberrelateret kriminalitet: En forbrydelse, der kun kan begås ved hjælp af IT-udstyr.

Cyberrobusthed: Evnen til at forhindre, forberede sig på, modstå og komme sig over cyberangreb og -hændelser.

Cybersikkerhed: Alle de sikkerhedsforanstaltninger, der er truffet for at beskytte IT-systemer og deres data mod uautoriseret adgang, angreb og skader for at sikre deres tilgængelighed, fortrolighed og integritet.

Cyberspace: Det uhåndgribelige globale miljø, hvor onlinekommunikation foregår mellem mennesker, software og tjenesteydelser via computernet og teknologisk udstyr.

Cyberøkosystem: Et komplekst system af interagerende udstyr, data, net, mennesker, processer og organisationer samt det miljø af processer og teknologier, der påvirker og understøtter systemets interaktioner.

Desinformation: Oplysninger, der er verificeret som falske eller vildledende, som er fabrikeret, fremlagt og udbredt med henblik på økonomisk gevinst eller for bevidst at manipulere offentligheden, og som kan være til skade for offentligheden.

Digitalt indhold: Alle former for data - såsom tekst, lyd, billeder eller video - der opbevares i et digitalt format.

Distribueret Denial of Service (DDoS): Et cyberangreb, der forhindrer legitime brugere i at få adgang til en onlinetjeneste eller -ressource ved at oversvømme den med flere anmodninger, end den kan klare.

Exploit kit: En type værktøjssæt, som cyberkriminelle bruger til at angribe svagheder i net og informationssystemer, så de kan distribuere malware eller udføre andre skadelige aktiviteter.

Fortrolighed: Beskyttelse af oplysninger, data eller aktiver mod uautoriseret adgang eller videregivelse.

Hacktivist: Enkeltpersoner eller grupper, der skaffer sig uautoriseret adgang til informationssystemer eller net med henblik på at fremme sociale eller politiske formål.

Hybrid trussel: En fjendtlig tilkendegivelse, som modstandere fremsætter med en kombination af konventionelle og ikkekonventionelle krigsførelsesteknikker (f.eks. militære, politiske, økonomiske og teknologiske) for at efterstræbe deres mål med magt.

Informationssikkerhed: Det sæt af processer og værktøjer, der beskytter fysiske og digitale data mod uautoriseret adgang, anvendelse, videregivelse, afbrydelse, ændring, registrering eller ødelæggelse.

Integritet: Beskyttelse mod uretmæssig ændring eller ødelæggelse af oplysninger og sikring af deres ægthed.

Kritisk infrastruktur: Fysiske ressourcer, tjenester og anlæg, hvis afbrydelse eller ødelæggelse vil have alvorlige virkninger for økonomien og samfundet.

Kryptering: Omdannelse af læselige oplysninger til ikkelæsbar kode for at beskytte dem. For at kunne læse oplysningerne skal brugeren have adgang til en hemmelig nøgle eller et hemmeligt password.

Kryptovaluta: En digital valuta, som udstedes og udveksles ved hjælp af krypteringsteknikker, uafhængigt af en centralbank. Den accepteres som betalingsmiddel blandt medlemmerne af et virtuelt fællesskab.

Malware: Skadelig software. Et computerprogram, der har til formål at skade en computer, en server eller et net.

Nedarvet system: Et forældet computersystem, program eller programmeringssprog, som stadig er i brug, men hvortil der måske ikke kan fås opgraderinger og sælgersupport, herunder sikkerhedssupport.

Netsikkerhed: Den del af cybersikkerheden, der sigter mod at beskytte data, som sendes via udstyr på det samme net, for at sikre, at oplysningerne ikke opsnappes eller ændres.

Patching: Foretagelse af ændringer i software med henblik på opdatering, problemløsning eller forbedring, herunder udbedring af sikkerhedsmangler.

Personoplysninger: Oplysninger om en identificerbar person.

Phishing: Udsendelse af e-mail, der foregiver at stamme fra en pålidelig kilde, med henblik på at vildlede modtagerne til at klikke på skadelige link eller udlevere personlige oplysninger.

Ransomware: Skadelig software, der nægter offeret adgang til et computersystem eller gør datafilerne ulæselige, som regel ved hjælp af kryptering. Normalt afpresser angriberen derefter offeret ved at nægte at genåbne adgangen, før der betales en løsesum.

Skimming: Tyveri af kredit- eller debetkortdata, når de indtastes online.

Social engineering: Dette udtryk bruges i forbindelse med informationssikkerhed om psykologisk manipulation, der har til formål at narre mennesker til at udføre en bestemt handling eller afsløre fortrolige oplysninger.

Sårbarhedsstyring: En integrerende del af computer- og netsikkerheden, der proaktivt modvirker eller forhindrer udnyttelse af system- og softwaresårbarheder ved at identificere, klassificere og afhjælpe dem.

Tekstvektorisering: Konvertering af ord, sætninger eller hele dokumenter til numeriske vektorer, så de kan bruges af maskinlæringsalgoritmer.

Tilgængelighed: Rettidig og pålidelig adgang til og anvendelse af oplysninger.

Tillidstjenester: Tjenester, der styrker den retlige gyldighed af en elektronisk transaktion, f.eks. elektroniske signaturer, segl og tidsstempler, registreret levering og webstedsautentifikation.

Tingenes internet: Det net af hverdagsgenstande, som er udstyret med elektronik, software og sensorer, så de kan kommunikere og udveksle data over internettet.

Valginfrastruktur: Eksempelvis IT-systemer og databaser, der bruges til kampagner, følsomme oplysninger om kandidater og vælgerregistreringssystemer.

Wipermalware: En type malware, hvis mål er at slette harddisken i den computer, den inficerer.

[1] I udkastet til EU's forordning om cybersikkerhed er det blevet defineret som "alle aktiviteter, der er nødvendige for at beskytte net- og informationssystemer, deres brugere og berørte personer mod cybertrusler". Forordningen forventes at blive vedtaget af Europa-Parlamentet og Rådet i begyndelsen af 2019.

[2] Europol, *Internet Organised Crime Threat Assessment 2017*.

[3] Den Europæiske Cybersikkerhedsorganisation (ECSO), *European Cybersecurity Industry Proposal for a contractual Public-Private Partnership*, juni 2016.

[4] Europa-Parlamentet, *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses*, undersøgelse udarbejdet for LIBE-udvalget, september 2015.

[5] ENISA, *ENISA Threat Landscape Report 2017*, 18. januar 2018.

[6] Europol, *Internet Organised Crime Threat Assessment 2018*.

[7] Europol, *ibid.*, 2018.

[8] European Centre for Political Economy, *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?*, Occasional Paper No 2/18. februar 2018.

[9] Europa-Kommissionen, formandens tale om Unionens tilstand 2017.

[10] Europol, *World's Biggest Marketplace selling internet paralysing DDoS attacks taken down*, pressemeddelelse, 25. april 2018.

[11] Europol, *Internet Organised Crime Threat Assessment 2017*.

[12] Europa-Kommissionen, *Factsheet on cybersecurity*, september 2017.

[13] Omkostningerne kan omfatte: mistede indtægter, omkostninger til genopretning af ødelagte systemer, potentielt ansvar i forbindelse med stjålne aktiver eller oplysninger, incitamenter til kundefastholdelse, højere forsikringspræmier, øgede produktionsomkostninger (nye systemer, ansatte, undervisning) og potentielle overholdelsesomkostninger eller retsomkostninger.

[14] NTT Security, *Risk:Value 2018 Report*.

[15] Ransomwaren *Wannacry* udnyttede sårbarheder i en protokol i Microsoft Windows, som gjorde det muligt at fjernovertage hvilken som helst computer. Microsoft udsendte et patch efter at have opdaget sårbarheden. Men hundredtusindvis af computere var endnu ikke blevet opdateret, og mange af dem blev efterfølgende inficeret. Kilde: A. Greenberg, *Hold North Korea Accountable For Wannacry—and the NSA, too*, WIRED, 19. december 2017.

[16] Europa-Kommissionen, *Europæernes holdninger til cybersikkerhed*, Eurobarometersærnummer 464a, september 2017. En opfølgende undersøgelse forventes at blive offentliggjort i begyndelsen af 2019.

[17] Budapestkonventionen er bindende internationale retningslinjer for lande, der udvikler lovgivning mod cyberkriminalitet. Den danner en ramme for internationalt samarbejde mellem deltagerstaterne. Kommissionen, Rådet for Den Europæiske Union, Europol, ENISA og Eurojust repræsenterer på nuværende tidspunkt EU.

[18] Europa-Kommissionen, *EU-strategi for cybersikkerhed: Et åbent, sikkert og beskyttet cyberspace*, COM JOIN (2013) 1 final af 7. februar 2013.

[19] Europa-Kommissionen, *Den europæiske dagsorden om sikkerhed*, COM (2015) 185 final af 28. april 2015.

[20] Europa-Kommissionen, *En strategi for et digitalt indre marked i EU*, COM (2015) 192 final af 6. maj 2015.

[21] EU-Udenrigstjenesten, *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, juni 2016.

[22] Centre for European Policy Studies, *Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force*, november 2018.

[23] Den malware, der blev brugt i angrebet med ransomwaren Wannacry, som Nordkorea stod bag ifølge USA, Det Forenede Kongerige og Australien, blev oprindeligt udviklet og opbevaret af det amerikanske sikkerhedsagentur (NSA) for at udnytte sårbarheder i Windows. Kilde: A. Greenberg, ibid., WIRED, 19. december 2017. I kølvandet på angrebene fordømte Microsoft, at statslige myndigheder opbevarer skadelig software, og gentog sin opfordring til at skabe en digital Genèvekonvention.

[24] Foruden landjorden, havet, luften og rummet.

[25] Ramme for EU's cyberforsvarspolitik (2018-ajourføring), 14413/18, 19. november 2018.

[26] Europa-Kommissionen/EU-Udenrigstjenesten, *Fælles ramme for imødegåelse af hybride trusler*, JOIN (2016) 18 final af 6. april 2016.

[27] Fælles erklæring fra formanden for Det Europæiske Råd, formanden for Europa-Kommissionen og generalsekretæren for Den Nordatlantiske Traktats Organisation, 8. juli 2016 og 10. juli 2018.

[28] Europa-Kommissionen/EU-Udenrigstjenesten, *Modstandsdygtighed, afskrækkelse og forsvar: opbygning af en stærk cybersikkerhed for EU*, JOIN (2017) 450 final af 13. september 2017.

[29] 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 (EUT L 194 af 19.7.2016, s. 1).

[30] 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.

[31] Disse er integreret i samarbejdsstrukturer, der er oprettet ved direktivet, nemlig CSIRT-netværket (et netværk bestående af CERT-EU og de CSIRT'er, der er udpeget af EU-medlemsstaterne; ENISA varetager sekretariatet) og samarbejdsgruppen (som støtter og fremmer det strategiske samarbejde og informationsudvekslingen mellem medlemsstaterne; Kommissionen varetager sekretariatet).

[32] 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 og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

[33] Europa-Kommissionen, *Forslag til Europa-Parlamentets og Rådets forordning om ENISA, "EU's Agentur for Cybersikkerhed", om ophævelse af forordning (EU) nr. 526/2013 og om cybersikkerhedscertificering af informations- og kommunikationsteknologi ("forordningen om cybersikkerhed")*, COM(2017) 477 final af 13. september 2017.

[34] Europa-Kommissionen, *Forslag til Europa-Parlamentets og Rådets forordning om europæiske editions- og sikringskendelser om elektronisk bevismateriale i straffesager*, COM (2018) 225 final af 17. april 2018.

[35] Europa-Kommissionen, *Forslag til Europa-Parlamentets og Rådets direktiv om harmoniserede regler for udpegning af retlige repræsentanter med henblik på indsamling af bevismateriale i straffesager*. COM (2018) 226 final, 17. april 2018.

[36] Europa-Kommissionen, *Forslag til Europa-Parlamentets og Rådets forordning om oprettelse af det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed og netværket af nationale koordinationscentre,* COM (2018) 630 final af 12. september 2018.

[37] H. Carrapico and A. Barrinha, *The EU as a Coherent (Cyber)Security Actor?*, Journal of Common Market Studies, bind 55, nr. 6, 2017.

[38] Europa-Kommissionen, ibid., SWD (2017) 295 final af 13. september 2017.

[39] Europa-Parlamentets forskningstjeneste, *Transatlantic cyber-insecurity and cybercrime. Economic impact and future prospects*, PE 603.948, december 2017.

[40] ENISA, *An evaluation framework for Cyber Security Strategies*, 27. november 2014.

[41] En undtagelse er artikel 14 ("Overvågning og statistik") i Europa-Parlamentets og Rådets direktiv 2013/40/EU af 12. august 2013 om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/RIA.

[42] Det Europæiske Økonomiske og Sociale Udvalg, *Cybersecurity: ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks*, marts 2018. CEPS-ECRI Task Force, Cybersecurity in Finance: Getting the policy mix right!, juni 2018.

[43] 24 af de 28 overordnede revisionsorganer besvarede vores spørgeskema.

[44] Dette betyder, at den er principbaseret og så teknologineutral som muligt.

[45] Europa-Kommissionens mekanisme for videnskabelig rådgivning, Scientific Opinion 2/2017, 24. marts 2017.

[46] L. Rebuffi, *EU Digital Autonom* Informationssicherheit, september 2018. European Centre for Political Economy, ibid., Occasional Paper No 2/18, februar 2018.*y: A possible approach*, Digma Zeitschrift für Datenrecht und

[47] Europa-Kommissionen, *Forslag til Europa-Parlamentets og Rådets direktiv om visse aspekter af aftaler om levering af digitalt indhold*, COM(2015) 634 final af 9. december 2015.

[48] Europa-Kommissionen, *Forslag til Europa-Parlamentets og Rådets direktiv om visse aspekter af aftaler om onlinesalg og andre former for fjernsalg af varer*, COM(2017) 635 final af 9. december 2015.

[49] Dutch Cyber Security Council, *European Foresight Cyber Security Meeting 2016: Public private academic recommendations to the European Commission about Internet of Things and Harmonization of duties of care*, 2016.

[50] Centre for European Policy Studies, *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges – Report of a CEPS Task Force*, juni 2018.

[51] Europa-Kommissionen, *Fuld udnyttelse af NIS - mod en effektiv gennemførelse af direktiv (EU) 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen*, COM(2017) 476 final/2 af 4 oktober 2017.

[52] Europol, ibid., 2017.

[53] Rådet for den Europæiske Union, *Endelig rapport om syvende runde af gensidige evalueringer af den praktiske gennemførelse af de europæiske politikker for forebyggelse og bekæmpelse af cyberkriminalitet og deres anvendelse*, 12711/1/17 REV 1, 9. oktober 2017.

[54] Europa-Kommissionen, *Impact assessment accompanying the document Proposal for a Directive on combating fraud and counterfeiting of non-cash means of payment*, SWD/2017/0298 final af 13 september 2017. Der blev opnået politisk enighed om den nye lovgivning i december 2018, og direktivet forventes at blive vedtaget i begyndelsen af 2019.

[55] Europol, ibid., 2017.

[56] C-362/14: Maximillian Schrems mod Data Protection Commissioner (Irland), 6. oktober 2015.

[57] Europol/Eurojust, *Common challenges in combating cybercrime*, 7021/17, 13. marts 2017.

[58] Europa-Kommissionen, *Assessment of the EU 2013 Cybersecurity Strategy*, SWD (2017) 295 final af 13. september 2017.

[59] Europa-Parlamentets Forskningstjeneste, *Briefing: EU Legislation in Progress – Review of dual-use export controls*, *PE589.832*.

[60] Europa-Parlamentets beslutning, *Menneskerettigheder og teknologi: Indvirkningen af udspionerings- og overvågningssystemer på menneskerettighederne i tredjelande* (2014/2232(INI)), 8. september 2015. Produkter og tjenester med dobbelt anvendelse, der omfatter software og teknologi, kan anvendes til både civile og militære formål.

[61] De offentligt tilgængelige oplysninger opbevares i WHOIS-databasen, der forvaltes af ICANN (Internet Corporation for Assigned Names and Numbers). ICANN varetager domænenavnesystemet. Misbrug af domænenavne gør cyberkriminalitet lettere.

[62] Artikel 3, NIS-direktivet, ibid.

[63] Atlantic Council, *Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures*, 10 september 2015.

[64] The White House, *Cybersecurity spending fiscal year 2019*.

[65] Europa-Kommissionen, *Commission Staff Working Document: Impact Assessment Accompanying the document 'Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027'*, SWD(2018) 305 final af 6. juni 2018.

[66] The Hague Centre for Strategic Studies, *Dutch investments in ICT and cybersecurity: putting it in perspective*, december 2016.

[67] Europa-Kommissionen, ibid., SWD (2018) 630 final af 13. september 2017.

[68] Europa-Parlamentets Forskningstjeneste/Enheden for Videnskabeligt Fremsyn, *Achieving a sovereign and trustworthy ICT industry in the EU*, december 2017.

[69] European Digital SME Alliance, *Position Paper on European Cybersecurity Strategy: Fostering the SME ecosystem*, 31. juli 2017.

[70] Europa-Parlamentets Forskningstjeneste/Enheden for Videnskabeligt Fremsyn, ibid., december 2017.

[71] Ibid.

[72] Europa-Kommissionen, *Impact assessment on the proposed research competence centre and network of national coordination centres*, SWD(2018) 403 final (Part 1/4), 12. september 2018.

[73] Europa-Kommissionen, ibid., SWD (2018) 630 final af 12. september 2018.

[74] Revisionsrettens særberetning nr. 13/2018: "Bekæmpelse af radikalisering, der fører til terrorisme".

[75] Tallene i dette afsnit stammer fra Kommissionens offentligt tilgængelige dokumenter, bortset fra de 42 millioner euro i punkt ***51***, som Kommissionen gav os direkte.

[76] Horisont 2020 er EU's forsknings- og innovationsprogram på 80 milliarder euro til støtte for "Innovation i EU", der tager sigte på at sikre EU's konkurrenceevne på verdensplan.

[77] Horisont 2020's samfundsmæssige udfordring nr. 7 "Sikre og innovative samfund: Beskyttelse af Europas og dets borgeres frihed og sikkerhed".

[78] Vi analyserede Horisont 2020-projekter fra CORDIS-datasættet. Vi udførte tekstvektorisering af hvert projekts beskrivelse ved anvendelse af JRC's taksonomi for cybersikkerhed (jf. ***tekstboks 5*** i næste kapitel) for at identificere projekter, der kunne omhandle cybersikkerhed. Herefter tjekkede og analyserede vi resultaterne manuelt.

[79] Den Europæiske Cybersikkerhedsorganisation, *ECS cPPP Progress Monitoring Report 2016-2017*, 29. oktober 2018.

[80] Artikel 9, stk. 2, NIS-direktivet, ibid.

[81] GLACY+ (den globale indsats mod IT-kriminalitet) er et fælles projekt med Europarådet. Det støtter tolv lande i Afrika, Asien/Stillehavsområdet, Latinamerika og Vestindien, der efterfølgende kan fungere som knudepunkter for udveksling af erfaringer i deres respektive regioner.

[82] Det Europæiske Center for Politisk Strategi (EPSC), Kommissionens tænketank, har udtalt sig om risikoen for et "digitalt hul", der kan opstå, hvis kløften mellem EU og dets naboer på det vestlige Balkan fortsætter med at vokse. Lande som Kina og Rusland investerer betydelige beløb i regionen, hvilket kan marginalisere EU som cyberaktør i regionen. Kilde: EPSC, *Engaging with the Western Balkans: an investment in Europe's security*, 17. maj 2018.

[83] Den Europæiske Investeringsbank, *The EIB Group Operating Framework and Operational Plan 2018*, 12. december 2017. Ingen yderligere oplysninger var tilgængelige i skrivende stund.

[84] Europa-Kommissionen, *Forslag til Europa-Parlamentets og Rådets forordning om programmet for et digitalt Europa for perioden 2021-2027*, COM(2018) 434 final af 6. juni 2018.

[85] Europa-Kommissionen, *Europa-Parlamentets og Rådets forordning (EU) 2018/1092 af 18. juli 2018 om oprettelse af programmet for udvikling af den europæiske forsvarsindustri med henblik på at støtte konkurrenceevnen og innovationskapaciteten i Unionens forsvarsindustri* (EUT L 200 af 7.8.2018, s. 30). Desuden blev der i 2017 etableret en forberedende foranstaltning vedrørende forsvarsforskning, som beløber sig til i alt 90 millioner euro i perioden 2017-2019 og finansieres under Horisont 2020. Det er uklart, om beløbet omfatter udgifter til cybersikkerhed.

[86] Revisionsretten planlægger at offentliggøre et særskilt briefingpapir om EU-forsvar i 2019.

[87] Europols EC3, ENISA, EU-Udenrigstjenesten, Det Europæiske Forsvarsagentur og CERT-EU har en samlet arbejdsstyrke på 159 personer. Dette samlede tal omfatter ikke cyberrelateret personale i Europa-Kommissionen og i medlemsstaterne. Kilde: Centre for European Policy Studies, ibid., november 2018.

[88] *ENISA evaluation*, 2017.

[89] Europol anmodede om en årlig personaleforøgelse på 70 midlertidigt ansatte i sin flerårige plan for 2018-2020, men der blev kun godkendt en forøgelse på 26 i 2018. I udkastet til den næste flerårige plan for 2019-2021 anmodede Europol kun om en beskeden forøgelse ud fra den antagelse, at en større ressourceanmodning ikke ville blive imødekommet. Kilde: Høring om udkast til den flerårige programmering for 2019-2021, som blev forelagt for Gruppen for Fælles Parlamentarisk Kontrol, A 000834, den 1. februar 2018.

[90] *ENISA evaluation*, 2017. Mellem 2014 og 2016 blev ca. 80 % af ENISA's operationelle budget brugt på indkøb af undersøgelser.

[91] ENISA, *Exploring the opportunities and limitations of current Threat Intelligence Platforms*, december 2017.

[92] ISACA (tidligere Information Systems Audit and Control Association), *Information Security Governance: Guidance for Boards of Directors and Executive Management*, 2. udg., 2006.

[93] EY, *Cybersecurity regained: preparing to face cyber attacks. 20th Global Information Security Survey 2017*, s. 16.

[94] McKinsey (J. Choi, J. Kaplan, C. Krishnamurthy and H. Lung), *Hit or myth? Understanding the true costs and impact of cybersecurity programs*, juli 2017.

[95] Securities and Exchange Commission, *Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures*, 21. februar 2018.

[96] Et forum for samarbejde mellem Den Europæiske Banktilsynsmyndighed, Den Europæiske Værdipapir- og Markedstilsynsmyndighed og Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger.

[97] Den Europæiske Værdipapirtilsynsmyndighed, *Joint Committee report on risks and vulnerabilities in the EU financial system*, april 2018.

[98] ENISA, *Information security and privacy standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in SMEs*, december 2015.

[99] For så vidt angår EU-medlemsstaterne er der ifølge Kommissionens mekanisme for videnskabelig rådgivning en væsentlig og enestående grad af enighed om de grundlæggende principper og værdier samt en fælles strategisk interesse, der kan blive kernen i en effektiv forvaltning af cybersikkerhed i EU. Kilde: Scientific Opinion 2/2017, 24. marts 2017.

[100] USA, Kina, Japan, Sydkorea, Indien og Brasilien.

[101] Det Europæiske Sikkerheds- og Forsvarsakademi (T. Renard and A. Barrinha), *Handbook on cyber security, chapter 3.4 The EU as a partner in cyber diplomacy and defence*, 23. november 2018.

[102] Rådet for Den Europæiske Union, *Handlingsplan for gennemførelse af Rådets konklusioner om den fælles meddelelse til Europa-Parlamentet og Rådet: Modstandsdygtighed, afskrækkelse og forsvar: opbygning af en stærk cybersikkerhed for EU*, 15748/17, 12. december 2017.

[103] Europa-Kommissionen, *European Commission Digital Strategy: A digitally transformed, user-focused and data-driven Commission*, C(2018) 7118 final af 21. november 2018.

[104] Kommissær Mariya Gabriels svar på en skriftlig parlamentarisk forespørgsel (E-004294-17), 28. juni 2017.

[105] Rådet for Den Europæiske Union, *Annual Report on the Implementation of the Cyber Defence Policy Framework*, 15870/17, 19. december 2017.

[106] Afgørelse 2015/443, 2015/444 og 2017/46 regulerer sikkerheden i Kommissionens kommunikations- og informationssystemer. Kommissionens afgørelse C (2018) 7706 af 21. november 2018 opretter et informationsteknologi- og cybersikkerhedsråd, som samler det tidligere IT-råd og Styrelsesrådet for Informationssikkerhed.

[107] Det Europæiske Økonomiske og Sociale Udvalg, ibid., marts 2018.

[108] Europa-Parlamentet, ibid., september 2015.

[109] Analyseenheden for hybride trusler blev oprettet i 2016 under EU's Efterretnings- og Situationscenter i EU-Udenrigstjenesten. Den modtager og analyserer klassificerede og offentligt tilgængelige oplysninger fra forskellige interessenter vedrørende hybride trusler.

[110] ENISA, *National-level Risk Assessments: An Analysis Report*, november 2013.

[111] Europa-Kommissionen, *Impact assessment on the EU Cybersecurity Agency and Cybersecurity Act*, SWD(2017) 500 final (Part 1/6) af 13. september 2017.

[112] Europa-Kommissionen, ibid., SWD (2018) 403 final af 12. september 2017.

[113] Résaux IP Européens Network Coordination Centre, den regionale topdomæneadministrator for Europa, der varetager tildelingen og registreringen af internetnummerressourcer.

[114] ENISA, *EISAS Large-Scale Pilot Collaborative Awareness Raising for EU Citizens & SMEs*, november 2012.

[115] The Centre for Cyber Safety and Education, in partnership with Booz Allen Hamilton, Alta Associates and Frost & Sullivan, *2017 Global Information Security Workforce Study – Benchmarking Workforce Capacity and Response to Cyber Risk*.

[116] Det Europæiske Økonomiske og Sociale Udvalg, ibid., marts 2018.

[117] House of Lords, *House of Commons Joint Committee on the National Security Strategy, Cyber Security Skills and the UK's Critical National Infrastructure, Second Report of Session 2017–19*, 16. juli 2018.

[118] Europol/Eurojust, *Common challenges in combatting cybercrime*, 7021/17, 13. marts 2017.

[119] Europol/Eurojust, ibid., 7021/17, 13. marts 2017.

[120] Europa-Kommissionen, ibid., SWD (2018) 403 final af 12. september 2017.

[121] CEPOL, *Decision of the Management Board 33/2018/MB on the CEPOL Single Programming Document 2020-2022*, 20. november 2018.

[122] F.eks. samarbejde mellem EU-Udenrigstjenesten, medlemsstaterne, agenturer og organer såsom CEPOL, ECTEG eller EDSC.

[123] ENISA, *Stock-taking of information security training needs in critical sectors*, december 2017.

[124] Den Europæiske Uddannelsesgruppe vedrørende Cyberkriminalitet.

[125] Europa-Kommissionen, Trettende statusrapport om indførelsen af en effektiv og ægte sikkerhedsunion, COM(2018) 46 final af 24. januar 2017.

[126] Baseret på bemærkninger i særberetning nr. 14/2018, ibid.

[127] Europa-Parlamentets beslutning af 13. juni 2018 om cyberforsvar (2018/2004(INI)) Rådet for Den Europæiske Union, ibid., 15870/17, 19. december 2017.

[128] Schweiz, FYROM, Ukraine, Bosnien-Hercegovina, Kosovo (denne betegnelse indebærer ingen stillingtagen til Kosovos status, og den er i overensstemmelse med FN's Sikkerhedsråds resolution 1244 og Den Internationale Domstols udtalelse om Kosovos uafhængighedserklæring), Tyrkiet og USA).

[129] Europol, *Internet Organised Crime Threat Assessment 2018*.

[130] Europa-Kommissionen, ibid., SWD (2017) 295 final af 13. september 2017.

[131] B. Stanton, M. F. Theofanos, S. S. Prettyman and S. Furman, *Security Fatigue*, "IT Professional", bind 18, nr. 5, 2016, s. 26-32. Jf. også NIST.

[132] Europa-Kommissionen/EU-Udenrigstjenesten, *Increasing resilience and bolstering capabilities to address hybrid threats*, JOIN(2018) 16 final af 13. juni 2018.

[133] F.eks. lukningen af AlphaBay og Hansa i fælles operationer ledet af FBI og nederlandsk politi med støtte fra Europol. Det var de to største markedspladser for handel med ulovlige varer såsom narkotika, skydevåben og værktøjer til cyberkriminalitet, f.eks. malware. Kilde: Europol, *Crime on the Dark Web: Law Enforcement coordination is the only cure*, pressemeddelelse, 29. maj 2018.

[134] Europa-Kommissionen, ibid., SWD (2018) 403 final af 12. september 2017.

[135] Rådet for Den Europæiske Union, ibid., 12711/1/17 REV 1, 9. oktober 2017.

[136] Europa-Kommissionen, ibid., SWD (2017) 295 final af 13. september 2017.

[137] Europa-Kommissionen/Tjenesten for EU's Optræden Udadtil, ibid., JOIN(2018) 16 af 13. juni 2018.

[138] Europa-Kommissionen, SWD (2017) 500 final af 13. september 2017.

[139] *Memorandum of Understanding – ENISA, EDA, Europol EC3, and CERT-EU*; 23. maj 2018.

[140] Europa-Kommissionen, udbud: *Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap*, 27. oktober 2017.

[141] Jean-Claude Juncker, Mission letter for the Commissioner for the Security Union, 2. august 2016. Forsvar er ikke omfattet af taskforcens mandat.

[142] Rådet for Den Europæiske Union, *EU cybersecurity roadmap*, 8901/17, 11. maj 2017.

[143] Friends of Europe, *Debating Security Plus: Crowdsourcing solutions to the world's security issues, 5. udg.*, november 2017.

[144] JRC Technical Reports, European Cybersecurity Centres of Expertise Map: *Definitions and Taxonomy.* Impact Assessment on the proposed Research Competence Centre and the Network of National Coordination Centres, SWD(2018) 403 final af 12. september 2018.

[145] Europa-Kommissionen, ibid., SWD (2017) 295 final af 13. september 2017.

[146] Europa-Kommissionen, ibid., SWD (2018) 403 final af 12. september 2017.

[147] F.eks. deltager repræsentanter for finanssektoren, nationale CERT'er, de retshåndhævende myndigheder, ENISA, Europol, Den Europæiske Centralbank, Det Europæiske Betalingsråd og Europa-Kommissionen i ISAC'en for finansielle institutioner i Europa.

[148] ENISA, *Information Sharing and Analysis Centres (ISACs) Cooperative models*, 14. februar 2018.

[149] Rådet for Den Europæiske Union, ibid., 12711/1/17 REV 1, 9. oktober 2017.

[150] https://www.europol.europa.eu/empact.

[151] En 2018-undersøgelse foretaget af Accenture i 15 lande viste, at 87 % af alle målrettede cyberangreb blev forhindret: *2018 State of Cyber Resilience*, 10. april 2018.

[152] P. Timmers, *Cybersecurity is Forcing a Rethink of Strategic Autonomy*, Oxford University Politics Blog, 14. september 2018.

[153] Caroline Preece, *Three reasons why cyber threat detection is still ineffective*, IT Pro, 14. juli 2017.

[154] Det Europæiske Økonomiske og Sociale Udvalg, *ibid.*, marts 2018.

[155] Europa-Kommissionen, *Ottende statusrapport om indførelsen af en effektiv og ægte sikkerhedsunion*, COM(2017) 354 final af 29. juni 2017.

[156] Jf. NIS-samarbejdsgruppens forskellige publikationer.

[157] ECB/FTM: Den Europæiske Centralbank/den fælles tilsynsmekanisme, Target2: Trans-European Automated Real-time Gross settlement Express Transfer system (2. generation), forordning nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked. Kilde: CEPS-ECRI Task Force, ibid., juni 2018.

[158] Europa-Kommissionen, *Henstilling om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser*, C(2017) 6100 final af 13. september 2017.

[159] Europa-Kommissionen, ibid., SWD (2017) 295 final af 13. september 2017. Der findes adskillige krisestyringsmekanismer, herunder de integrerede ordninger for politisk kriserespons (IPCR), Argus (Kommissionens krisereaktionsmekanisme), EU-Udenrigstjenestens krisereaktionsmekanisme, EU-civilbeskyttelsesmekanismen og EU's beredskabsprotokol i forbindelse med retshåndhævelse.

[160] Dette kan også føre til, at artikel 42, stk. 7, i traktaten om Den Europæiske Union (bestemmelsen om gensidigt forsvar) og artikel 222 i traktaten om Den Europæiske Unions funktionsmåde (solidaritetsbestemmelsen) gøres gældende.

[161] Europa-Kommissionen/Tjenesten for EU's Optræden Udadtil, ibid., JOIN(2018) 16 af 13. juni 2018. I december 2018 blev det rapporteret i medierne, at EU-Udenrigstjenestens diplomatiske kommunikationsnet, Coreu, angiveligt var blevet hacket (kilde: *New York Times, Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran*, 18. december 2018). Dette efterforskes på nuværende tidspunkt.

[162] Samarbejdet om tidlig varsling og gensidig bistand bør også udvikles yderligere: *Rådets konklusioner om en koordineret EU-reaktion på væsentlige cybersikkerhedshændelser og -kriser*, 10085/18 af 26. juni 2018.

[163] Europa-Parlamentets Forskningstjeneste, *Briefing EU Legislation in Progress: ENISA and a new cybersecurity act*, PE 614.643, september 2018.

[164] Det Europæiske Økonomiske og Sociale Udvalg, ibid., marts 2018.

[165] Rådet for Den Europæiske Union, *EU Law Enforcement Emergency Response Protocol (LE ERP) for Major Cross-Border Cyber-Attacks*, 14893/18, december 2018.

[166] Cyberberedskabshold og gensidig bistand inden for cybersikkerhed. Platform til informationsudveksling om reaktion på cybertrusler og -hændelser. Kilde: Rådet for Den Europæiske Union, *Permanent Structured Cooperation (PESCO) updated list of PESCO projects – Overview*, 19. november 2018.

[167] Rådet for Den Europæiske Union, Konklusioner om en ramme for EU's fælles diplomatiske reaktion på ondsindede cyberaktiviteter, 9916/17 af 7 juni 2017.

[168] Rådet for Den Europæiske Union, *Rådets konklusioner om cyberdiplomati*, 6122/55 af 11. februar 2015.

[169] Rådet for Den Europæiske Union, *Draft implementing guidelines for the Framework on a Joint Diplomatic Response to Malicious Cyber Activities*, 13007/17.

[170] Placeringen af ansvaret for en hændelse er en suveræn politisk afgørelse, der træffes af medlemsstaterne, og ikke alle værktøjskassens foranstaltninger kræver ansvarsplacering.

[171] Værktøjskassen førte ikke til en fælles indsats. Et antal medlemsstater tilsluttede sig individuelt USA's holdning.

[172] Rådet for Den Europæiske Union, *Rådets konklusioner om ondsindede cyberaktiviteter*, 7925/18 af 16. april 2018.

[173] Computersystemer til styring af processer i forskellige industrier, f.eks. forsyningstjenester, kemisk og industriel produktion, fødevareforarbejdning, transportsystemer og -knudepunkter og logistiktjenester.

[174] ENISA, ibid., december 2017.

[175] F.eks. offentlig administration, kemisk industri, nuklear industri, produktionsindustri, fødevareforarbejdningsindustri, turisme, logistik og civilbeskyttelse.

[176] Europa-Kommissionen, ibid., SWD (2017) 295 final af 13. september 2017.

[177] Tale af kommissær Věra Jourová på Europa-Parlamentets plenarmøde: *Increasing EU resilience against the influence of foreign actors on the upcoming EP election campaign*, 14. november 2018.

[178] Carnegie Endowment for International Peace, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*, 23. maj 2018.

[179] European Political and Strategy Centre (L. Past), "Cybersecurity of Election Technology: Inevitable Attacks and Variety of Responses", i: Election Interference in the Digital Age – Building Resilience to Cyber-Enabled Threats: A collection of think pieces of 35 leading practitioners and experts, 2018.

[180] Jf. Rådets direktiv 2008/114/EF om indkredsning og udpegning af europæisk kritisk infrastruktur og vurdering af behovet for at beskytte den bedre.

[181] Europa-Kommissionen, Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament, C(2018) 5949 final, 12. september 2018.

[182] Det Europæiske Råds konklusioner, EUCO 11/15, 20. marts 2015. Der er siden blevet oprettet to taskforcer for henholdsvis Vestbalkan og Naboskab Syd.

[183] Det Atlantiske Råd opfordrede i en rapport EU til at anmode alle medlemsstater om at udsende nationale eksperter til taskforcen. Jf.: D. Fried and A. Polyakova, *Democratic Defense Against Disinformation*, 5. marts 2018.

[184] Oprindelig havde taskforcen ikke sit eget budget, men den fik i 2018 en tildeling fra Europa-Parlamentet på 1,1 million euro til en forberedende foranstaltning kaldet "StratCom Plus".

[185] Carnegie Endowment for International Peace (E. Brattberg, T. Maurer), ibid., 23. maj 2018.

[186] Europa-Kommissionen, Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik, *Handlingsplan for bekæmpelse af desinformation*, JOIN(2018) 36 final. Planen fokuserer på: forbedring af EU-institutionernes evne til at opdage, analysere og blotlægge desinformation, styrkelse af den koordinerede fælles indsats, mobilisering af den private sektor og øget kendskab til desinformation og forbedring af samfundets modstandsdygtighed.

[187] Europa-Kommissionen, *Bekæmpelse af desinformation på internettet: en europæisk tilgang*, COM(2018) 236 final af 26. april 2018.

[188] Må ikke forveksles med adfærdskodeksen til bekæmpelse af ulovlig hadefuld tale online.

[189] JRC, *The digital transformation of news media and the rise of disinformation and fake news*, JRC Technical Reports, JRC Digital Economy Working Paper 2018-02, april 2018.

[190] ENISA, *Strengthening Network & Information Security & Protecting Against Online Disinformation ("Fake News"),* april 2018.

[191] European Political and Strategy Centre (C. Frutos López), *A Responsibility to Support Electoral Organisations in Anticipating and Countering Cyber Threats*, ibid, 2018.

[192] Europa-Kommissionen, ibid., SWD (2018) 403 final, 12. september 2018.

[193] Den foreslåede forordning (COM(2017) 487 final af 13. september 2018) om screening af udenlandske direkte investeringer, som blev forelagt i september 2017, er stadig under lovgivningsmæssig behandling. Den omfatter specifikt kritiske teknologier, herunder kunstig intelligens, cybersikkerhed og teknologier med dobbelt anvendelse.

[194] Europa-Kommissionen/Tjenesten for EU's Optræden Udadtil, ibid., JOIN(2017) 450 finalaf 13. juni 2018.

Holdet bag

Dette briefingpapir *Udfordringer for en effektiv cybersikkerhedspolitik i EU* blev vedtaget af Afdeling III - Foranstaltninger udadtil/Sikkerhed og retfærdighed, der ledes af Bettina Jakobsen, medlem af Revisionsretten. Arbejdet blev udført under ledelse af Baudilio Tomé Muguruza, medlem af Revisionsretten, med støtte fra kabinetschef Daniel Costa de Magalhaes, attaché Ignacio Garcia de Parada, ledende administrator Alejandro Ballester-Gallardo, opgaveansvarlig Michiel Sweerts, revisorerne Simon Dennett, Aurelia Petliza, Mirko Iaconisi, Michele Scardone og Silvia Monteiro Da Cunha samt praktikanten Johannes Bolkart. Hannah Critoph ydede sproglig støtte.

Fra venstre til højre: Ignacio Garcia de Parada, Silvia Monteiro Da Cunha, Michele Scardone, Michiel Sweerts, Mirko Iaconisi, Baudilio Tomé Muguruza, Simon Dennett, Hannah Critoph, Daniel Costa de Magalhaes.

DEN
EUROPÆISKE
REVISIONSRET

Publikationskontoret

DEN EUROPÆISKE REVISIONSRET
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Tlf. +352 4398-1

Kontakt: eca.europa.eu/da/Pages/ContactForm.aspx
Websted: eca.europa.eu
Twitter: @EUAuditors