Rådet for
Den Europæiske Union

Bruxelles, den 8. juni 2017
(OR. en)

13204/1/16
REV 1 DCL 1

GENVAL 104
CYBER 113

AFKLASSIFICERING

af dokument:	13204/1/16 REV 1
af:	9. december 2016
ny status:	Offentlig
Vedr.:	Evalueringsrapport om syvende runde af gensidige evalueringer "Den praktiske gennemførelse af de europæiske politikker for forebyggelse og bekæmpelse af cyberkriminalitet og deres anvendelse" - Rapport om Danmark

Hermed følger til delegationerne den afklassificerede udgave af ovennævnte dokument.

Teksten til dokumentet er den samme som teksten til den foregående udgave.

Rådet for
Den Europæiske Union

Bruxelles, den 9. december 2016
(OR. en)

13204/1/16
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 104
CYBER 113

RAPPORT

Vedr.:	Evalueringsrapport om syvende runde af gensidige evalueringer "Den praktiske gennemførelse af de europæiske politikker for forebyggelse og bekæmpelse af cyberkriminalitet og deres anvendelse" - Rapport om Danmark

Indhold

1 RESUMÉ

- Evalueringsholdet har kunnet vurdere Danmarks generelle kapacitet til at forebygge, efterforske og retsforfølge cyberkriminalitet som høj, selv om der på den ene side er plads til forbedring på visse områder, og der på den anden side foreligger ubesvarede spørgsmål om den måde, hvorpå retsvæsenet (domstolene) er involveret i bekæmpelsen af cyberkriminalitet.

- Det generelle arbejdsmiljø i de kompetente enheder var uformelt, men meget effektivt. De danske myndigheder har givet tilsagn om løbende forbedring ved hjælp af en langsigtet tilgang til arbejdet, der sigter mod at opnå små, trinvise ændringer i processerne for at forbedre effektiviteten og kvaliteten, og regelmæssig gennemgang af fremskridt ("strømlinet tilgang").

- Fra 2014 har Danmark udvist stor politisk vilje til at forbedre håndteringen af cyberspørgsmål, og der er blevet afsat passende budgetmidler. Det blev konstateret under besøget på stedet , at de midler, der er afsat til både forebyggelse og bekæmpelsen af cyberkriminalitet, er anvendt fornuftigt og i høj grad kan gavne den nationale økonomi.

- Der er sket en solid tilpasning af reaktionen mellem det danske Center for Cybersikkerhed, efterretningstjenesterne og politiet sammen med andre nationale strukturer, der er oprettet for at imødegå kritiske hændelser. Rollerne er klare, og der deles relevante oplysninger.

- Nationalt Cyber Crime Center (NC3) har det overordnede ansvar for at forebygge, hindre og efterforske cyberkriminalitet og lovovertrædelser med forbindelse til cyberkriminalitet i Danmark. Det foretager kriminaltekniske undersøgelser og analyser og yder anden form for efterforskningsmæssig bistand til det lokale politi. NC3 beskæftiger højt kvalificerede politiefterforskere, IT-kriminaltekniske efterforskere og IT-eksperter. NC3 har været aktiv siden 2014, og der er opnået betydelige fremskridt i løbet af kort tid.

- Sammenlægningen af Rigspolitiet og anklagemyndigheden, der begge er underlagt Justitsministeriets myndighed, udgør et særligt træk ved det danske retssystem. I praksis resulterer dette i et reelt samarbejde mellem politifolk og anklagere og gør det betydelig lettere at sikre en vellykket retsforfølgning.

- Evalueringsholdet konstaterede, at der er plads til forbedring i det nationale sagsbehandlingssystem, hvilket afspejles i henstillingerne til Danmark, men fandt det positivt, at sagsbehandlingssystemet er fælles for politiet og anklagemyndigheden.

- I samarbejde med relevante interessenter, bl.a. de interessenter, der er involveret i beskyttelsen af de grundlæggende rettigheder, er Danmark i øjeblikket ved at ændre sine regler om opbevaring af internettrafikdata. I den forbindelse valgte man at prioritere en indsigtsfuld, sofistikeret model med optimal levetid til opbevaring af internetdata frem for en hurtigere, men mere kortsigtet løsning. Det henstilles dog til de nationale myndigheder, at de hurtigt vedtager og gennemfører den kommende lov.

- Danmarks bidrag til Europols/EC3's aktiviteter er væsentligt. Det faktum, at Danmark ikke længere vil være medlem af Europol som følge af den danske folkeafstemning den 3. december 2015, vil være til skade for begge parter.

- Det nationale medlem af Eurojust er velkendt blandt lokale fagfolk, både i politiet og anklagemyndigheden. De lokale fagfolk betragter det som nemt at kontakte Eurojust og få den nødvendige bistand. Danmark er begyndt at oprette fælles efterforskningshold og bør opmuntres i denne retning.

- Den private sektors rolle afspejles på flere måder inden for cybersamarbejde:
  - Større virksomheder og offentlige instanser kan abonnere på en tjeneste fra Center for Cybersikkerhed for at beskytte dem mod de værste 10 % af trusler, som ikke i tilstrækkelig grad kan håndteres af de private udbydere af internetsikkerhed.
  - NC3 samarbejder aktivt med politiet og den finansielle sektor.
  - Yderligere samarbejde mellem politiet og den private sektor (fortrolig udveksling af oplysninger blandt medlemmer og uddannelse af interessenter i infrastrukturen) er omfattet af NC3SKYT-samarbejdet.

- Uddannelse er et tilbagevendende positivt spørgsmål i forbindelse med evalueringen. Der blev på alle dage og på alle niveauer henvist til et omfattende program, der skal opdatere politiets og anklageres cyberfærdigheder. Grundlæggende uddannelse for anklagere og ansatte i politiet, der befinder sig i frontlinjen, er obligatorisk og gennemføres ved hjælp af e-læringsmoduler. Der findes yderligere to niveauer: "Avanceret", der består i en blanding af e-læring og undervisning, og "Ekspert", der består i udvikling af nøglefærdigheder i en international kontekst.

2 INDLEDNING

Efter vedtagelsen af fælles aktion 97/827/RIA af 5. december 1997[1] blev der indført en ordning for evaluering af, hvordan de internationale forpligtelser med hensyn til bekæmpelse af organiseret kriminalitet udmøntes og efterleves i de enkelte medlemsstater. I overensstemmelse med artikel 2 i den fælles aktion besluttede Gruppen vedrørende Generelle Anliggender, herunder evaluering (GENVAL), på mødet den 3. oktober 2013, at den syvende runde af gensidige evalueringer bør omhandle den praktiske gennemførelse af de europæiske politikker for forebyggelse og bekæmpelse af cyberkriminalitet og deres anvendelse.

Valget af cyberkriminalitet som emne for syvende runde af gensidig evaluering blev hilst velkommen af medlemsstaterne. Grundet den brede vifte af lovovertrædelser, som udtrykket "cyberkriminalitet" dækker over, blev det imidlertid vedtaget, at evalueringen skal fokusere på de lovovertrædelser, som i følge medlemsstaterne berettiger særlig opmærksomhed. Med henblik herpå vil evalueringen primært omfatte tre specifikke områder: cyberangreb, seksuelt misbrug af børn/pornografi online samt onlinesvindel med betalingskort, og den vil indebære en omfattende gennemgang af de juridiske og operationelle aspekter af håndteringen af cyberkriminalitet, samarbejdet på tværs af grænserne og samarbejdet med de relevante EU-agenturer. Direktiv 2011/93/EU om bekæmpelse af seksuelt misbrug og seksuel udnyttelse af børn og børnepornografi[2] (gennemførelsesdato: 18. december 2013) og direktiv 2013/40/EU[3] om angreb på informationssystemer (gennemførelsesdato: 4. september 2015) er særligt relevante i den forbindelse.

1 Fælles aktion af 5. december 1997 (97/827/RIA), EUT L 344 af 15.12.1997, s. 7.
2 EUT L 335 af 17.12.2011, s. 1.
3 EUT L 218 af 14.8.2013, s. 8.

I Rådets konklusioner om EU-strategien for cybersikkerhed fra juni 2013[4] gentages desuden målet om at få ratificeret Europarådets konvention om IT-kriminalitet (Budapestkonventionen)[5] af 23. november 2001 hurtigst muligt, og det understreges i præamblen, at EU ikke lægger op til, "at der skabes nye internationale retlige instrumenter for cyberspørgsmål". Denne konvention suppleres af en protokol om fremmedfjendske og racistiske handlinger begået gennem edb-systemer[6].

Erfaring fra tidligere evalueringer viser, at medlemsstaternes situation er forskellig, hvad angår gennemførelse af relevante retlige instrumenter, og den igangværende evalueringsproces kan vise sig at give nyttig input til de medlemsstater, der eventuelt ikke har gennemført alle aspekter af de forskellige instrumenter. Ikke desto mindre sigter evalueringen mod at være bred og tværfaglig og ikke mod at fokusere på gennemførelse af forskellige instrumenter i forbindelse med cyberkriminalitet, men snarere på de operationelle aspekter i medlemsstaterne.

Derfor vil den foruden samarbejdet med anklagemyndigheden også omhandle, hvordan politiet samarbejder med Eurojust, ENISA og Europol/EC3, og hvordan feedback fra de givne aktører formidles til de relevante polititjenester og sociale tjenester. Evalueringen fokuserer på gennemførelse af nationale politikker med henblik på at stoppe cyberangreb og -svindel samt børnepornografi. Evalueringen omfatter også medlemsstaternes operationelle praksis vedrørende internationalt samarbejde og støtten til personer, der bliver ofre for cyberkriminalitet.

[4] 12109/13 POLGEN 138 JAI 612 TELECOM 194 PROCIV 88 CSC 69 CIS 14 RELEX 633 JAIEX 55 RECH 338 COMPET 554 IND 204 COTER 85 ENFOPOL 232 DROIPEN 87 CYBER 15 COPS 276 POLMIL 39 COSI 93 DATAPROTECT 94.

[5] CETS nr. 185, der blev åbnet for undertegnelse den 23. november 2001 og trådte i kraft den 1. juli 2004.

[6] CETS nr. 189, der blev åbnet for undertegnelse den 28. januar 2003 og trådte i kraft den 1. marts 2006.

Rækkefølgen af besøg i medlemsstaterne blev vedtaget af GENVAL den 1. april 2014. Danmark var det 21. land, der blev evalueret i denne evalueringsrunde. I overensstemmelse med artikel 3 i den fælles aktion har formandskabet udarbejdet en liste over eksperter i de evalueringer, der skal foretages. Medlemsstaterne har udnævnt eksperter med væsentlig praktisk viden på området i medfør af en skriftlig anmodning af 28. januar 2014 til delegationerne fra formanden for GENVAL.

Evalueringsholdene består af tre nationale eksperter, der bistås af to medarbejdere fra Rådets Generalsekretariat og af observatører. For den syvende runde af gensidige evalueringer tilsluttede GENVAL sig formandskabets forslag om, at Europa-Kommissionen, Eurojust, ENISA og Europol/EC3 bør inviteres som observatører.

De eksperter, der fik til opgave at foretage evalueringen af Danmark, var Gert SEIDL (Østrig), Michael GUBBINS (Irland) og Timothy ZAMMIT (Malta). Timothy ZAMMIT afslog at deltage i besøget på stedet og bidrog ikke til evalueringsrapporten. To observatører var til stede: Reinhard SANTELER (Eurojust) og Tom ROBSON (Europol/EC3), sammen med Monika KOPCHEVA og Claire ROCHETEAU fra Rådets Generalsekretariat.

Denne rapport blev udarbejdet af ekspertholdet med bistand fra Rådets Generalsekretariat på grundlag af resultaterne fra det evalueringsbesøg, der fandt sted i Danmark mellem den 15. og 18. marts 2016, og af Danmarks detaljerede svar på evalueringens spørgeskema sammen med dets detaljerede svar på de efterfølgende opfølgende spørgsmål.

3 GENERELLE ANLIGGENDER OG STRUKTURER

3.1 Den nationale strategi for cybersikkerhed

I december forelagde den danske regering en national strategi for cyber- og informationssikkerhed, der indeholder en bred vifte af regeringsinitiativer for perioden 2015-2016. Den danske regering har sigtet mod at styrke beskyttelsen mod cyberangreb, samtidig med at den personlige frihed og retsstatsprincippet respekteres.

Strategien består af seks strategiske fokusområder, som 27 specifikke initiativer skal fokusere på. Nogle af de strategiske fokusområder, der vedrører bekæmpelse af cyberkriminalitet og styrkelse af cybersikkerhed, fremhæves nedenfor.

Følgende specifikke initiativer er blevet lanceret for at styrke efterforskning af cyberkriminalitet:
– udvidelsen af Rigspolitiets Nationale Cyber Crime Center (NC3)
– styrkelsen af cyberkapaciteten i den danske efterretnings- og sikkerhedsmyndighed (Politiets Efterretningstjeneste (PET))
– oprettelsen af en onlineplatform for indberetning af cyberkriminalitet og
– gennemførelsen af en undersøgelse vedrørende en tjeneste, der stiller oplysninger til rådighed om stjålne identitetsdokumenter.

Følgende specifikke initiativer er blevet lanceret for at styrke efterforskning af cybersikkerhed:
– oprettelsen af en enhed for vurdering af cybertrusler i Center for Cybersikkerhed, der er underlagt Forsvarsministeriet
– oprettelsen af en enhed, der skal efterforske større cyberhændelser i Center for Cybersikkerhed
– oprettelsen af en enhed med kendskab til SCADA i Center for Cybersikkerhed, den obligatoriske inddragelse af cybertrusler i statslige institutioners risikostyring og
– gennemførelsen af en undersøgelse vedrørende en eventuel sammenlægning af statslige internetforbindelser.

Link til en præsentation af den nationale strategi for cyber- og informationssikkerhed (*på engelsk*): http://www.fmn.dk/eng/news/Documents/Danish-Cyber-and-Information-Security-Strategy-ENvers.PDF
Link til den nationale strategi for cyber- og informationssikkerhed (*på dansk*): http://www.fmn.dk/nyheder/Documents/National-strategi-for-cyber-og-informationssikkerhed.pdf.

3.2 Nationale prioriteter vedrørende cyberkriminalitet

Rigspolitiet har vedtaget en overordnet strategi for 2016-2020, som både det nationale og lokale politi skal følge i deres arbejde. Et af strategiens primære formål er at forebygge og bekæmpe cyberkriminalitet.

Strategien for 2016-2020 suppleres af en vision og fem strategiske mål for det arbejde, der udføres i Rigspolitiets Nationale Cyber Crime Center (NC3). Visionen er, at Danmark bliver blandt de førende lande i samspillet mellem samfund og politi for at hindre og bekæmpe cyberkriminalitet. De fire strategiske mål dækker over "borgeren i centrum for indsatsen", "styrkelse af hele det danske politi", "samarbejde", "kvalitet og kompetence" og "forskningsbaseret innovation".

Desuden lancerede NC3 i januar 2016 et initiativ, der skal arbejde med forebyggelse og bekæmpelse af cyberkriminalitet. Dette strategiske arbejde vil i lyset af de nye uddannelsesprogrammer, nye teknologiske platforme og den generelle styrkelse af kompetencer og kapaciteter udstikke retningen for NC3's og politikredsenes indsats for at forebygge, hindre og bekæmpe cyberkriminalitet med fokus på, hvordan sagerne bedst håndteres.

3.3 Statistikker vedrørende cyberkriminalitet

3.3.1 Hovedtendenser, der peger i retning af cyberkriminalitet

Rigspolitiet har observeret en stigning i antallet af sager, der vedrører computerrelateret svindel eller forfalskning. De seneste tal fra en udbyder af finansiel infrastruktur viser en betydelig stigning i misbruget af betalingskort i forbindelse med onlinehandel. Svindel i forbindelse med onlinehandel mellem private enkeltpersoner peger også i retning af en stigning, selv om en del af stigningen også kan skyldes den voksende brug af onlineplatforme til handel.

I 2015 blev der rettet adskillige ransomwareangreb mod både offentlige institutioner, private virksomheder og enkelte borgere, mens der fra 2014-2015 er blevet indberettet færre sager til politiet om ulovlig adgang til informationssystemer og ulovligt indgreb i informationssystemer.

De danske myndigheder påpegede dog, at kun et lille antal af de hændelser, som virksomheder og privatpersoner oplever, indberettes til de retshåndhævende myndigheder, og med eksterne rapporter om stigende systemsårbarheder og tingenes internet betragtes faldet i antallet af indberetninger ikke som en indikation på en generel nedgang inden for denne type kriminalitet.

Sociale medieplatforme spiller i stigende grad en rolle som "skueplads" for kriminelle handlinger, der spænder fra sager om svindel til sager om ulovlig distribution af billeder og blufærdighedskrænkelse.

I forbindelse med seksuelt misbrug af børn på internettet har dansk politi i de seneste år behandlet de første sager om livestreaming af misbrug. Baseret på rapporter fra udlandet forventes antallet af denne type sager at stige.

I det danske statistiske system er det ikke muligt at sætte tal på cyberkriminalitet i modsætning til det samlede billede for kriminalitet, da registreringen af sager, der involverer brug af informations- og kommunikationsteknologi (IKT), i mange tilfælde ikke holdes adskilt fra sager, der ikke involverer denne måde at operere på.

3.3.2 Antallet af registrerede sager vedrørende cyberkriminalitet

Som nævnt ovenfor holdes sager om cyberkriminalitet i visse tilfælde ikke adskilt fra andre sager i de danske kriminalitetsstatistikker, da det er en fremgangsmåde, der går på tværs af flere kriminalitetsområder. **Det er derfor en udfordring at udlede et nationalt tal for cyberkriminalitet.**

De nationale statistikker om cyberkriminalitet, der offentliggøres af Rigspolitiet, bygger på politidata og fokuserer på de kriminalitetsområder, der er kendt for at have særlig tilknytning til brugen af IKT. Beskrivelsen af tendenserne inden for cyberkriminalitet, der indsamles af Rigspolitiet, bygger dog på foreliggende statistikker og analyser fra den private sektor og andre institutioner fra den offentlige sektor.

De statistikker, som holdet fik forelagt (se nedenfor), var ikke udtømmende og blev modtaget i små bidder efter anmodning under besøget på stedet. Dette blev i hvert fald delvist tilskrevet et forældet sagsbehandlingssystem, der ikke er fuldt ud egnet til formålet. Denne faktor viste sig hver dag under evalueringen i forhold til forskellige agenturer.

NB! Nedenstående tabel over alle sager vedrørende cyberkriminalitet, der indberettes til politiet, er ikke udtømmende.
Politiets statistikker er primært struktureret i overensstemmelse med straffeloven, og der vil, som i mange medlemsstater, være flere sager, der kan betegnes som cyberkriminalitet, end dem, der er afspejlet i de offentlige tal. Visse tilfælde af forsøg på grooming kan f.eks. registreres som blufærdighedskrænkelse, mens statistikker om blufærdighedskrænkelse også omfatter sager, der ikke er relateret til cyberkriminalitet.

Tabel - Registrerede sager, sigtelser og tiltaler

	2014	2015	2014	2015	2014	2015
	Registrerede sager		Sigtelser		Tiltaler	
Distribution af børnepornografi	71	110	72	118	41	103
Besiddelse af børnepornografi	106	122	106	127	75	128
Ulovlig adgang til dataoplysninger	180	133	110	173	141	75
Ulovlig adgang til virksomhedshemmeligheder	11	3	19	7	2	1
Ulovlig anvendelse af koder til informationssystemer	60	16	8	14	1	17
Datasvindel	5 628	15 399	4 992	10 808	6770	10 109

3.4 Nationalt budget bevilget til forebyggelse og bekæmpelse af cyberkriminalitet og støtte fra EU-midler

På alle de områder, der blev undersøgt, syntes det bevilgede budget til oprettelse og drift af strukturerne til bekæmpelse af cyberkriminalitet at være tilstrækkeligt med henblik på at forebygge og bekæmpe det pågældende fænomen. Navnlig har Rigspolitiets fornyede Nationale Cyber Crime Center (NC3) afsat tilstrækkelige ressourcer jævnført med en lignende enhed af gennemsnitlig størrelse i andre medlemsstater.

Danmark er berettiget til EU-midler til fælles projekter med andre medlemsstater, f.eks. det britiske KIRAT-redskab vedrørende seksuelt misbrug af børn, men ikke til at håndtere specifikke danske projekter vedrørende cyberkriminalitet.

3.5 Konklusioner

- **Det lader til, at Danmark har indført en stærk strategi for cybersikkerhed, som understøttes på regeringsniveau.**

- **Center for Cybersikkerhed, der er ansvarligt for cybersikkerhed i store kritiske infrastrukturer, fungerer som en IT-beredskabsenhed, der genererer reaktioner på cyberangreb. Centret er velstruktureret og har demonstreret, at det er yderst strategisk og proaktivt i sine løbende aktiviteter.**

- **Der findes en specifik strategi for cybersikkerhed i Danmark og alle interessenter er nøje indsat i deres egne ansvarsområder.**

- **I de seneste år har de danske myndigheder afsat betydelige midler til oprettelse af eller fornyelse af strukturer og værktøjer for bedre at tackle cybersikkerhed og spørgsmål vedrørende cyberkriminalitet. Evalueringsholdet hilste dette velkommen og opfordrer Danmark til fortsat at afsætte tilstrækkelige ressourcer for at holde trit med den hurtige udvikling inden for både informationsteknologi og kriminelt misbrug heraf.**

- **Danmark har stillet statistikker til rådighed. I lighed med andre medlemsstaters registreringssystemer skal politiets/anklagemyndighedens registreringssystem dog moderniseres, så det bedre kan tage højde for forbrydelsers cyberaspekt og dets udvikling.**

- **Som i mange medlemsstater holdes statistikker fra de retshåndhævende myndigheder adskilt fra domstolenes statistikker. Sidstnævnte blev ikke udleveret til evalueringsholdet. En række eksempler på domme fra domstolene blev dog stillet til rådighed. De danske myndigheder betegnede dommenes længde i sager om cyberkriminalitet som "ensartet".**

4 NATIONALE STRUKTURER

4.1 Retsvæsenet (anklagemyndighed og domstole)

4.1.1 Intern struktur

I henhold til dansk lov har politiet til opgave at foretage strafferetlige efterforskninger. Anklagemyndighedens rolle er at føre tilsyn med efterforskningerne og sikre, at efterforskningerne sker i overensstemmelse med loven. På lokalt plan er der – grundet den integrerede struktur – almindeligvis et tæt samarbejde mellem politiet og anklagemyndigheden i løbet af efterforskningerne.

Det er evalueringsholdets opfattelse, at kombinationen af politi og anklagemyndighed overordnet set afspejler, hvordan kriminalitetsbekæmpelsen ledes. De danske fagfolk udtalte, at sager med en chance for et positivt udfald, prioriteres. Holdet fik også af vide, at risikoen for eventuelle proceduremæssige fejl minimeres i kraft af det tætte samarbejde med anklagere og deres tidlige inddragelse i sagerne. Generelt kan dette betragtes som model for bedste praksis.

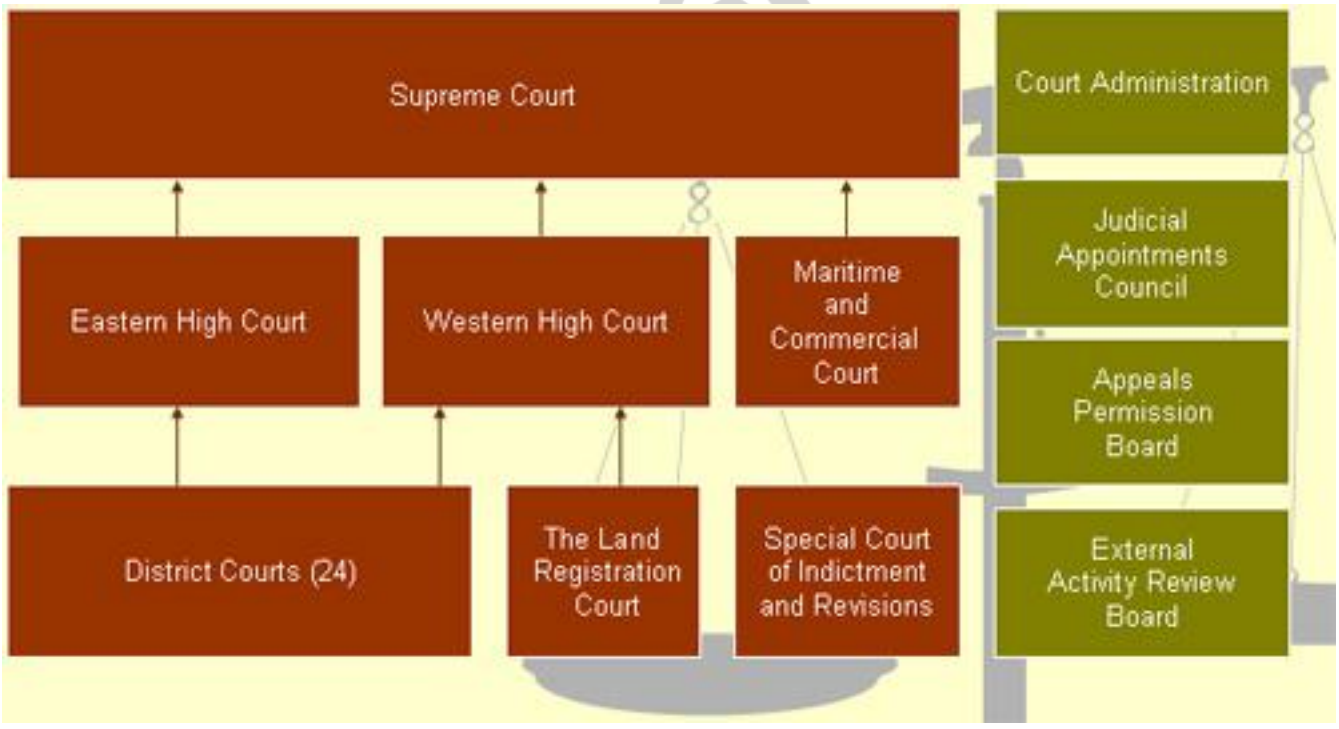
Det er anklageren, der skal træffe afgørelse om eventuelle efterforskningsmæssige skridt, der kræver en retskendelse (tvangsforanstaltning), og som forelægger anmodningen for retten. Efter den efterforskningsmæssige fase af sagen vurderer anklageren beviset og træffer afgørelse om, hvorvidt der skal rejses tiltale eller ej. Anklageren forelægger i så fald sagen for retten under retssagen.

Sager om cyberkriminalitet efterforskes i 12 lokale politikredse og af anklagerne i disse. En undtagelse er sager om overtrædelse af IP-rettigheder, som kan efterforskes og retsforfølges af Statsanklageren for Særlig Økonomisk og International Kriminalitet – der varetager straffesager ved landsretterne.

Cyberangreb. Nationalt Cyber Crime Center har også ansvaret for at bistå de lokale politikredse med efterforskningen af cyberangreb for at pågribe og retsforfølge gerningsmændene bag cyberangrebene. I december 2012 blev Center for Cybersikkerhed oprettet som en sektor i Forsvarets Efterretningstjeneste (FE).

Center for Cybersikkerhed har bl.a. til opgave at anvende dets ekspertise til i forbindelse med IT-sikkerhed at foretage tekniske analyser af avancerede cyberangreb for at afbøde cyberangrebene og skaffe klarhed over angrebsmetoden. Rigspolitiet/Politiets Efterretningstjeneste (PET) og Center for Cybersikkerhed/Forsvarets Efterretningstjeneste (FE) arbejder tæt sammen, herunder om indbyrdes udveksling af oplysninger vedrørende cyberangreb samt operationelt samarbejde i forbindelse med specifikke cyberangreb.

Hverken i de danske svar på spørgeskemaet fra GENVAL eller ved besøget på stedet fik evalueringsholdet væsentlige oplysninger om retsvæsenet. Der findes ingen dommere med speciale i cyberkriminalitet. Retsvæsenet er organiseret som følger:



4.1.2 Kapacitet til og hindringer for vellykket retsforfølgelse

Nationalt **Cyber Crime Center (NC3)** blev oprettet (på basis af to tidligere enheder) under Rigspolitiet i 2014. NC3 udvider og styrker politikredsenes arbejde på efterforskningsmæssige, forebyggende og forskningsmæssige områder, der vedrører cyberkriminalitet, i form af bedre kvalifikationer og større kapacitet samt væsentlige investeringer i teknologi. NC3 beskæftiger omkring 100 personer, bl.a. specialiserede politiefterforskere, IT-fagfolk, analytikere, advokater, osv.

Der er også blevet udpeget IT-ingeniører til de lokale politikredse.

Anklagemyndigheden. De mest gængse sager om cyberkriminalitet behandles af almindelige anklagere. I 2014 besluttede Rigsadvokaten imidlertid at løfte anklagernes kompetencer på tre niveauer:

– alle anklagere bør være i stand til at behandle enkle eller mere gængse sager vedrørende cyberkriminalitet, f.eks. sager om computerrelateret svindel eller forfalskning
– i alle anklagemyndighedens afdelinger er der udpeget specialister i cyberkriminalitet. Specialisterne bør være i stand til at behandle større og mere komplicerede sager om cyberkriminalitet
– på nationalt plan er der udpeget fire eksperter i cyberkriminalitet. Disse eksperter bør være i stand til at behandle de mest omfattende og komplicerede sager om cyberkriminalitet. De inddrages også i uddannelse, indsamling og formidling af oplysninger.

Kompetencerne inden for retsforfølgning af sager om cyberkriminalitet styrkes ved at udsende standarder, retningslinjer samt gennem uddannelse og oprettelse af netværk.

Anklagemyndigheden tilbyder to kurser om cyberkriminalitet. Cybercrime I og II.

– kurset "*Cybercrime I*" består af e-læring og henvender sig til alle anklagere. I øjeblikket findes der fire moduler online, og i foråret 2016 vil flere moduler være tilgængelige. Kurset er udarbejdet i samarbejde med Rigspolitiet.

– kurset "*Cybercrime II*" henvender sig til specialister/eksperter og er et kursus over fire dage, der fokuserer på national og international lovgivning og nationale og internationale forskrifter og på tekniske aspekter.

Rigsadvokaten har udsendt retningslinjer til anklagemyndigheden om sager vedrørende børnepornografi, osv. samt retningslinjer, der dækker alle områder af cyberkriminalitet.

– Retningslinjer vedrørende besiddelse af børnepornografisk materiale

– Retningslinjer for politiets behandling af sager vedrørende it-kriminalitet

– Beskrivelse af kurserne, Cybercrime I og II (side 38 og 41 i kataloget)

– E-læringsmodul: "Forbrydelser, påtale og værneting" (skærmprint)

– Skrivelse fra Rigsadvokaten af 17. december 2014

En standard for bedste praksis vedrørende computerrelateret svindel eller forfalskning er under udarbejdelse.

Dokumenterne er udelukkende til intern brug i politiet og anklagemyndigheden.

Rigsadvokaten vurderer, at de primære hindringer for efterforskninger og retsforfølgning af cyberkriminalitet er:

– vanskeligheden ved at sikre et overblik over de mange mindre lovovertrædelser, der begås, f.eks. via internettet (organiseret småkriminalitet)

– den tekniske kompleksitet i mange sager om cyberkriminalitet.

Besøget på stedet gjorde det temmelig klart, at den nuværende struktur i det nationale sagsbehandlingssystem skal revideres for at gøre det mere effektiv. Opdatering af sagsbehandlingssystemer er sandsynligvis et udbredt problem i mange medlemsstater.

Desuden kan det være en hindring at skaffe digitale beviser på grund af internettets struktur og bevisernes flygtighed.

De danske myndigheder anførte, at der ikke er nogen formaliseret interaktion med dommere i fuld respekt for deres uafhængighed. Der føres dog en åben dialog med domstolens forvaltning og en daglig dialog mellem lokale anklagere og dommere.

4.2. Retshåndhævende myndigheder

I Danmark er der én samlet politistyrke, Rigspolitiet.
De enkelte politikredse er ansvarlige for forebyggelsen, efterforskningen og retsforfølgningen af cyberkriminalitet. **Politikredsene råder over særligt udpegede IT-efterforskere og IT-ingeniører, der skal støtte efterforskningen.**

På nationalt plan varetager Nationalt Cyber Crime Center (NC3) det overordnede tilsyn og ansvar for koordinering (nationalt og internationalt) og instrukser vedrørende efterforskningen. NC3 yder også bistand til politikredsene i sager om cyberangreb, indholdsrelaterede handlinger, der muliggøres ved hjælp af IT, handlinger, der involverer computere eller IT-systemer som redskab eller mål, og alle typer sager, hvor der skal skaffes og analyseres digitale beviser.

Rigspolitiet anførte, at det ikke kan pege på nogen hindringer for vellykket efterforskning af cyberkriminalitet, der er unikke eller særlig relevante for Danmark. Som sådan er de primære hindringer blandt andre den hurtige teknologiske udviklinger, cyberkriminelles stigende professionalisme og ekspertiseniveau, det faktum, at cyberkriminalitet nemt kan spænde over flere landes retlige kompetence, bevisernes flygtighed i forbindelse med cyberkriminalitet og den udbredte anvendelse af kryptering, Tor og andre veje til anonymitet.

Nationalt Efterforskningscenter (NEC), der hører under Rigspolitiet, driver Vagt- og Kommunikationscentret, der er åbent døgnet rundt hele året, som et fælles kontaktpunkt (SPOC) for den samlede danske politistyrke. Dette omfatter anmodninger inden for rammerne af Europol, Schengensamarbejdet, Taskforcen for Østersøområdet, Frontex, INTERPOL, Det Nordiske Politi- og Toldsamarbejde (PTN), bilateralt samarbejde med retshåndhævende myndigheder i andre lande, tilsyn på tværs af grænser og kontrollede leverancer. Det håndterer desuden hastende anmodninger i henhold til Budapestkonventionen om It-kriminalitet. Det indebærer, at der er ét enkelt kontaktpunkt i hele det danske politi og ingen bureaukrati i den indledende fase af samarbejdet med andre lande. Der er indført proceduremæssige skridt til at sikre, at anmodninger, der sendes til SPOC, straks videresendes til Nationalt Cyber Crime Center (NC3) med henblik på at træffe passende efterforskningsmæssige foranstaltninger og inddrage anklagemyndigheden og retsvæsenet, når det er nødvendigt.

4.3. Øvrige myndigheder/institutioner/offentlige-private partnerskaber

Politiets Efterretningstjeneste (PET), der hører under Rigspolitiet, er ansvarlig for at forebygge, efterforske og imødegå handlinger, der udgør eller kan udgøre en trussel mod Danmark som et uafhængigt, demokratisk og sikkert samfund. Det gælder også trusler mod informations- og kommunikationssystemer eller anvendelsen af informations- og kommunikationssystemer, hvor truslerne også er til fare for den nationale sikkerhed.

Center for Cybersikkerhed, der blev oprettet i 2012 som en del af Forsvarets Efterretningstjeneste (FE), yder bistand til myndighederne og virksomheder af væsentlig betydning for det danske samfund. Politiets Efterretningstjeneste (PET), der hører under Rigspolitiet, er ansvarlig for at forebygge, efterforske og bekæmpe enheder og handlinger, der udgør eller kan udgøre en trussel mod Danmark som et uafhængigt, demokratisk og sikkert samfund. Det gælder også trusler mod informations- og kommunikationssystemer eller anvendelsen af informations- og kommunikationssystemer, hvor truslerne også er til fare for den nationale sikkerhed.

I visse sager om cyberkriminalitet yder Center for Cybersikkerhed teknisk bistand til Nationalt Cyber Crime Center (NC3). I andre sager om cyberkriminalitet yder NC3 bistand i forbindelse med efterforskninger, der ledes af Politiets Efterretningstjeneste (PET).

Center for Cybersikkerhed foretager IT-sikkerhedsrelaterede tekniske undersøgelser af cyberangreb mod statslige institutioner og kritisk infrastruktur både for at bringe de enkelte angreb til ophør og for at skaffe klarhed over angrebsmetoder og -redskaber, så beskyttelsen mod lignende angreb kan blive styrket i samfundet som helhed. Disse undersøgelser udføres i tæt samarbejde med den berørte myndighed.

For mange cyberangrebs vedkommende er det nødvendigt at foretage både efterforskninger og IT-sikkerhedsrelaterede tekniske undersøgelser. Der finder dermed et tæt samarbejde sted både på strategisk og operationelt plan mellem Politiets Efterretningstjeneste (PET), NC3 og Center for Cybersikkerhed.

4.4. Samarbejde og koordination på nationalt plan

4.4.1 Retlige eller politiske forpligtelser

Den private sektor er ikke forpligtet til at indberette nogen form for cyberkriminalitet, bl.a. cyberangreb, til politiet. De danske myndigheder fremmer dog samarbejdsforbindelser til den private sektor.

Alle statslige myndigheder, herunder institutioner med kritisk statslig infrastruktur, indberetter cyberangreb til Center for Cybersikkerhed. *(se detaljer i 6.1.2 nedenfor)*.

4.4.2 Ressourcer, der bevilges til forbedring af samarbejdet

Da samarbejde med den private sektor er et særligt fokusområde inden for NC3's strategiske mål, bevilges der ressourcer hertil, og der udvikles løbende muligheder for yderligere styrkelse af samarbejdet.

4.5. Konklusioner

- **De danske myndigheder har indført principperne for "*Lean management*" (strømlinet forvaltning), så de kan fungere mere effektivt. Dette kan betragtes som god praksis for opbygning af kapacitet til at forebygge og bekæmpe cyberkriminalitet.**

- **Der foreligger dokumentation for godt samarbejde mellem efterretningstjenester, retshåndhævende myndigheder og Center for Cybersikkerhed.**

- **Det tætte samarbejde mellem anklagere og politiet (der begge er underlagt det samme ministeriums myndighed - Justitsministeriet) har en klar indflydelse på kvaliteten: fordi anklagerne kender sagen fra begyndelsen, er de systematisk velforberedte til at føre den ved domstolen. De kan også på et meget tidligt stadium påpege over for efterforskerne, at der mangler fakta eller beviser.**

- **Som i visse andre medlemsstater er domstolene adskilt fra anklagemyndigheden som "uvildige søjler", hvilket kan resultere i forskellige grader af bevidsthed om og generelt kendskab til cyberkriminalitet.**

- **På nuværende tidspunkt kan man via det nationale sagsbehandlingssystem ikke få et overblik over alle kategorier af cyberrelateret kriminalitet eller tidlig identifikation af flere forbundne sager eller parallelle efterforskninger og retsforfølgninger på nationalt plan.**

- **De danske retshåndhævende myndigheder viste eksempler på effektivt samarbejde med den private sektor på grundlag af aftalememoranda. NC3 samarbejder navnlig med**
  – private partnerskaber gennem det såkaldte "Netfilter"-program, som har til formål at blokere adgangen til materiale med seksuelt misbrug af børn på internettet
  – danske banker og private IT-virksomheder om at bekæmpe banksvindel over internettet.

- **Justitsministeriet forelagde en oversigt over retssystemet for evalueringsholdet. Holdet fik dog ikke mulighed for at indgå i en dialog med retsvæsenet og dokumentere dets erfaring med cyberkriminalitet.**

5 RETLIGE ASPEKTER

5.1 Materiel strafferet vedrørende cyberkriminalitet

5.1.1 Europarådets konvention om IT-kriminalitet

Danmark ratificerede konventionen om cyberkriminalitet (CETS nr. 185) den 21. juni 2005, og konventionen trådte i kraft den 1. oktober 2005.

5.1.2 Beskrivelse af national lovgivning

Generelle principper af relevans for lovovertrædelser i den danske straffelov

I overensstemmelse med § 19 i den danske straffelov straffes lovovertrædelser, der er omhandlet i loven, og som er begået af uagtsomhed, kun, når det er særligt hjemlet. Det betyder, at kun forsætlige lovovertrædelser er omfattet af de kapitler, der nævnes nedenfor, medmindre det modsatte har særlig hjemmel.

Forsæt dækker i denne forbindelse en række variationer, dvs. direkte forsæt, sandsynlighedsforsæt og positiv indvilligelse/bevidst uagtsomhed. Der er tale om direkte forsæt, når handlingen og resultatet heraf osv. var (udtrykkeligt) tilsigtet. Der er tale om sandsynlighedsforsæt, når den ansvarlige handlede, på trods af at en kriminel handling og dens følge osv. var det mest sandsynlige udfald. Der er tale om positiv indvilligelse/bevidst uagtsomhed, når den ansvarlige opnåede et bestemt resultat (ved at foretage handlingen) og accepterede denne mulighed som en risiko ved den specifikke handling.

Straffelovens 10. kapitel omhandler de almindelige principper, der finder anvendelse for straffens fastsættelse, f.eks. fængslingsvilkår. I § 81 foreligger en ikkeudtømmende liste over en række skærpende omstændigheder. Der skal tages højde for disse omstændigheder ved strafudmålingen for en lovovertrædelse. F.eks. kan det betragtes som en skærpende omstændighed, at gerningsmanden tidligere er straffet af betydning for den pågældende sag. I straffelovens § 82 foreligger en ikkeudtømmende liste over en række formildende omstændigheder ved strafudmåling for en lovovertrædelse. F.eks. kan det betragtes som en formildende omstændighed, hvis gerningsmanden frivilligt har angivet sig selv til myndighederne og aflagt fuldstændig tilståelse.

Hvis der er begået flere lovovertrædelser, skal der fastsættes en fælles straf for sådanne lovovertrædelser inden for de foreskrevne mildeste og strengeste strafferammer i medfør af § 88. Det bør derfor tages i betragtning, at anvendelsen af den mildeste strafferamme i straffeloven som regel betyder, at muligheden for at pålægge en bøde som straf forsvinder, dvs. at ganske få lovovertrædelser indebærer reelle krav om en minimumsperiode for fængsling (eksempelvis kan manddrab, jf. straffelovens § 237, straffes med fængsel i en periode på mindst 5 år).
Offentlig tilskyndelse til forbrydelse er en lovovertrædelse i medfør af straffelovens § 136, stk. 1. Desuden udgør medvirken til en gerning ved tilskyndelse, råd eller dåd en lovovertrædelse i medfør af straffelovens § 23. Forsøg på at fremme eller bevirke udførelsen af forbrydelse er strafbart i medfør af § 21.

Følgende handlinger relateret til cyberkriminalitet, der er opført på listen i tabel 2 i GENVAL's spørgeskema, er strafbare i Danmark.

– Handlinger, der udelukkende er rettet mod informationssystemer

Ulovlig adgang til informationssystemer er strafbar i medfør af følgende artikler i straffeloven:
– § 263, stk. 2, der omhandler uretmæssig (uberettiget) tilegnelse af adgang til en andens oplysninger
eller programmer, der er bestemt til at bruges i et informationssystem
– § 263 a, der omhandler uretmæssig erhvervsmæssig salg eller udbredelse i en videre kreds af en kode eller andet adgangsmiddel til et ikkeoffentligt tilgængeligt informationssystem hvortil adgangen er beskyttet med kode eller anden særlig adgangsbegrænsning samt videregivelse af et større antal koder eller andre adgangsmidler (vedrører ikke erhvervsmæssige systemer)

– § 301 a, der omhandler uretmæssig erhvervelse eller videregivelse af koder eller andre adgangsmidler til informationssystemer, hvortil adgangen er forbeholdt betalende brugere, og som er beskyttet med kode eller anden særlig adgangsbegrænsning (vedrører erhvervsmæssige systemer). De (erhvervsmæssige) informationssystemer i straffelovens § 301a omfatter bl.a. såkaldte efterspørgselsstyrede systemer og informationssamlinger såsom avisdatabaser, hvortil adgang er forbeholdt betalende medlemmer, og som er beskyttet med en kode, osv. Eksempler på koder eller andre særlige adgangsbegrænsninger som omhandlet i § 301 a er identifikationskoder for netbrugere, afkodningskort og telekort (PIN-koder til telefoner).

Det kræver generelt 10 eller flere koder m.v. for at konstatere eksistensen af "et større antal koder" til informationssystemer eller adgangsmidler, jf. straffelovens § 263 a, stk. 2. Den strengeste straf for overtrædelser af straffelovens § 263, stk. 2, § 263 a eller § 301 a er 1 år og 6 måneder. Hvis en person begår en af de lovovertrædelser, der er omhandlet i § 263, stk. 2, med forsæt til at skaffe sig eller gøre sig bekendt med en virksomheds erhvervshemmeligheder, eller under andre skærpende omstændigheder, kan straffen stige til fængsel i indtil 6 år. På samme måde straffes de lovovertrædelser, der er omhandlet i stk. 2), og som begås på systematisk eller organiseret vis.

Hvis der sker videregivelse m.v. som omhandlet i straffelovens § 263 a under særligt skærpende omstændigheder, er straffen i medfør af stk. 4 fængsel indtil 6 år. Som særligt skærpende omstændigheder anses navnlig tilfælde, hvor oplysninger videregives eller på anden vis udbredes i en videre kreds, eller hvor videregivelsen indebærer særlig risiko for betydelig skade.

Hvis der sker videregivelse m.v. som omhandlet i straffelovens § 301a under særligt skærpende omstændigheder, er straffen i medfør af stk. 2 fængsel indtil 6 år. Som særligt skærpende omstændigheder anses navnlig tilfælde, hvor oplysninger videregives eller på anden vis udbredes erhvervsmæssigt i en videre kreds eller under omstændigheder, hvor der er særlig risiko for omfattende misbrug.

Ulovligt indgreb i informationssystemer er strafbart i medfør af følgende artikler i straffeloven:
– § 193, stk. 1, der omhandler fremkaldelse af omfattende forstyrrelse i driften af almindelige samfærdselsmidler, offentlig postbesørgelse, telegraf- eller telefonanlæg, radio- eller fjernsynsanlæg, informationssystemer eller anlæg, der tjener til almindelig forsyning med vand, gas, elektrisk strøm eller varme
– § 291, stk. 1, der omhandler ødelæggelse, beskadigelse eller bortskaffelse af ting, der tilhører en anden
– § 293, stk. 2, der omhandler uberettiget hindring af en anden i helt eller delvis at råde over ting. Sletning, beskadigelse, forringelse, ændring eller bortskaffelse af elektroniske data er omfattet af straffelovens § 291. Benægtelse af angreb på tjenester, der hindrer normal anvendelse eller adgang til informationssystemer ved overbelastning eller ved at forårsage et sammenbrud er strafbar i medfør af § 293, stk. 2.

Udtrykket "omfattende forstyrrelse" i straffelovens § 193 anvendes for handlinger, der potentielt kan påvirke den brede offentlighed med hensyn til informationssystemer m.v. Ét eksempel på en sådan handling er sletning af en internetudbyders informationssystem eller anden form for hacking, der forårsager forstyrrelse i et informationssystem med kritisk infrastruktur.

Den strengeste straf for overtrædelser af straffelovens § 193 er 6 år, mens den strengeste straf for overtrædelser af § 293, stk. 2, er 1 år. Straffen i medfør af § 293, stk. 2, kan dog stige til 2 års fængsel, hvis lovovertrædelsen begås på systematisk eller organiseret vis eller der i øvrigt foreligger særligt skærpende omstændigheder.

Den strengeste straf for lovovertrædelser i medfør af straffelovens § 291, stk. 1, er 1 år og 6 måneder. I tilfælde af hærværk af betydeligt omfang eller af systematisk eller organiseret karakter, eller hvis gerningsmanden tidligere er fundet skyldig efter § 291 eller § 180, 181, § 183, stk. 1 og 2, § 184, stk. 1, § 193 eller 194, kan straffen stige til fængsel i 6 år.

Ulovligt indgreb i data er strafbart i medfør af de samme artikler i straffeloven som dem, der nævnes i forbindelse med ulovligt indgreb i informationssystemer, f.eks. sletning, beskadigelse af, m.v. af elektroniske data.

Ulovlig opfangning af elektroniske data er strafbar i medfør af straffelovens § 263, stk. 2, der omhandler uretmæssig (uberettiget) tilegnelse af adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et informationssystem. Der henvises til bemærkningerne om § 263, stk. 2, om ulovlig adgang til oplysninger.

Misbrug af enheder – fremstilling, distribution eller erhvervelse med henblik på at bruge, importere eller på anden måde stille til rådighed eller besiddelse af værktøjer til IT-misbrug er ikke strafbart som sådan. Dog er fremstilling, erhvervelse, osv. af enheder eller værktøjer, der kan misbruges til at begå lovovertrædelser, strafbar som tilskyndelse til, råd eller dåd i forbindelse med en lovovertrædelse (§ 23) eller forsøg på at udføre en forbrydelse. Derfor er det at planlægge udformningen af et program med det formål at anvende det til at udføre et cyberangreb strafbart som et forsøg på at foretage bl.a. ulovligt indgreb i data i medfør af § 293, stk. 2.

– Indholdsrelaterede handlinger, navnlig i forbindelse med seksuelt misbrug af børn online og børneporno

Computerrelateret fremstilling af børneporno, der involverer børn under den seksuelle lavalder (under 15 år), er strafbar i medfør af følgende artikler i straffeloven:

– § 216, stk. 2, der omhandler samleje med et barn under 12 år (§ 225, hvis den seksuelle handling vedrører andet seksuelt forhold end samleje)

– § 222, der omhandler samleje med et barn under den seksuelle lavalder (§ 225, hvis den seksuelle handling vedrører andet seksuelt forhold end samleje)

– § 226, der omhandler optagelse af pornografiske fotografier, film el. lign. af en person under 18 år med forsæt til at sælge eller på anden måde udbrede materialet

– § 232, der omhandler blufærdighedskrænkelse.

Fremstilling af computergenerede af børnepornografiske billeder er strafbar i medfør af følgende artikler i straffeloven:

– § 235, stk. 2, der omhandler besiddelse eller gennemsyn mod vederlag gennem internettet eller et lignende system af pornografiske fotografier eller film, andre pornografiske visuelle gengivelser eller lignende af personer under 18 år

– § 226, der omhandler optagelse af pornografiske fotografier, film, el.
lign. af en person under 18 år med forsæt til at sælge eller på anden måde
udbrede materialet

– computerrelateret udbredelse af børnepornografi er strafbar i medfør af straffelovens § 235, stk. 1, der omhandler udbredelse af pornografiske fotografier eller film, andre pornografiske visuelle gengivelser eller lignende af personer under 18 år.

Computerrelateret besiddelse af børneporno er strafbar i medfør af straffelovens § 235, stk. 2, der omhandler besiddelse eller gennemsyn mod vederlag gennem internettet eller et lignende system af pornografiske fotografier eller film, andre pornografiske visuelle gengivelser eller lignende af personer under 18 år. I medfør af straffelovens § 235, stk. 3, gælder det imidlertid, at besiddelse af materiale, der inddrager et barn, som er ældre end den seksuelle lavalder, og som samtykker i besiddelsen, ikke er omfattet af § 235, stk. 2.

Udtrykket "pornografiske fotografier eller film, andre pornografiske visuelle gengivelser eller lignende af personer under 18 år" omfatter personer, der lader til at være børn. Hvis den afbildede person, der fremtræder som et barn, reelt var 18 år eller ældre på tidspunktet for afbildningen, betragtes materialet ikke som børnepornografi. Udtrykket "pornografiske visuelle gengivelser eller lignende af personer under 18 år" omfatter især computergenerede billeder, der ikke gengiver en reel person under 18 år, men som bortset fra det fiktive aspekt fuldstændig ligner et fotografi. Den fiktive fremstilling skal derfor være nogenlunde identisk med fotografier osv.

Strafansvar ved ovennævnte lovovertrædelser kræver forsæt (straffelovens § 19, jf. § 216, stk. 2, § 222, 226 og 235). Dog kan overtrædelser af § 222 og 226 i medfør af straffelovens § 228 medføre strafansvar på trods af manglende kendskab til offerets alder, hvis gerningsmanden har handlet uagtsomt med hensyn til offerets alder. Den strengeste straf for overtrædelser af straffelovens § 216, stk. 2, er 12 år.

Den strengeste straf for overtrædelser af straffelovens § 222 er fængsel indtil 8 år. Hvis gerningsmanden har anvendt tvang eller trusler, er den strengeste straf fængsel indtil 12 år. Den strengeste straf for overtrædelser af straffelovens § 226 er fængsel indtil 6 år. Den strengeste straf for overtrædelser af § 232 er fængsel indtil 4 år, hvis barnet er under 15 år, og fængsel i indtil 2 år, hvis barnet er 15 år eller derover. Den strengeste straf for overtrædelser af § 235, stk. 1, er fængsel indtil 2 år, eller under særligt skærpende omstændigheder indtil 6 år. Den strengeste straf for overtrædelser af § 235, stk. 2, er fængsel indtil 1 år.

Computerrelateret "grooming" er strafbart som forsøg (§ 21) på at begå en seksualforbrydelse mod et barn i medfør af straffelovens 24. kapitel, f.eks. forsøg på at skaffe sig samleje med et barn, som ikke har nået den seksuelle lavalder, eller på at fremstille børnepornografi. Da "grooming" er strafbart som forsøg på at begå en seksualforbrydelse, er "grooming" ikke defineret i straffeloven. Strafansvar for forsøg omfatter dog i princippet enhver form for forberedende handling, uanset om selve handlingen er harmløs eller uegnet som middel til at begå den påtænkte forbrydelse. Derfor kan computerrelateret "grooming" være strafbart fra det tidspunkt, hvor gerningsmanden første gang kontakter barnet med forsæt til at begå seksualforbrydelsen, uanset om kontakten indledes ved hjælp af informations- og kommunikationsteknologi, eller om gerningsmanden har foreslået at mødes med barnet og har taget konkrete skridt, der fører til et sådant møde.

Den strengeste straf for computerrelateret "grooming" vedrører den forbrydelse, som gerningsmanden forsøgte at begå. F.eks. er den strengeste straf for computerrelateret "grooming" med forsæt til at optage børnepornografi med henblik på udbredelse (straffelovens § 21 og 226) den samme som den strengeste straf for fremstilling af børnepornografi med forsæt til at udbrede materialet, dvs. fængsel indtil 6 år.

Efter evalueringsholdets opfattelse omfatter konceptet, hvor forsøgsfasen begynder meget tidligt, givetvis de fleste sager om "grooming", især hvis det nødvendige forsæt kan bevises. I mange sager er dette sandsynligvis ikke vanskeligt i betragtning af forbrydelsens særlige karakter. Det kan dog være værd at huske på, at der kan opstå situationer, hvor forsæt er vanskeligt at bevise, eller hvor mistænkte frivilligt opgiver deres forsøg, hvilket kan føre til, at der ikke foreligger strafansvar. Det faktum, at "grooming" kun betragtes som forsøg, kan også mindske den sociale stigmatisering af forbrydelsen. I mange lande ville et sådant forsøg endda blive betragtet som en formildende omstændighed.

– **Handlinger, hvor computer-/IT-systemer er involveret som værktøj eller mål**:

Computerrelateret svindel er strafbar i medfør af straffelovens § 279 a, der omhandler databedrageri. Denne artikel blev indført i 1985 for at sikre strafansvar i sager om bedrageri, hvor intet menneske vildledes, fordi behandlingen af oplysninger/data foretages af et informationssystem.

Den strengeste straf for overtrædelse af § 279 a er fængsel indtil 1 år og 6 måneder. Hvis databedrageriet er af særlig grov beskaffenhed, navnlig på grund af udførelsesmåden, eller fordi forbrydelsen er udført af flere i forening, eller som følge omfanget af den opnåede eller tilsigtede virkning, eller når et større antal forbrydelser er begået, kan straffen stige til fængsel indtil 8 år (§ 286, stk. 2).

Computerrelateret forfalskning er strafbar i medfør af § 171, der omhandler dokumentfalsk. Denne artikel finder anvendelse på forfalskning af elektronisk data. Forbrydelsen omfatter derfor alle elektroniske data, der indgår i en kontrol, herunder e-mails, voice mails osv.

Den strengeste staf for overtrædelser af § 171 er 2 års fængsel. Hvis forfalskningen er af særlig grov beskaffenhed, eller hvis der er begået et større antal forbrydelser af samme karakter, kan straffen stige til fængsel indtil 6 år.

Hvad angår computerrelaterede identitetsforbrydelser, bør det bemærkes, at der ikke er en særskilt straf for identitetstyveri. Men på grund af det brede anvendelsesområde for reglerne om forsøg samt tilskyndelse, råd og dåd vil identitetstyveri ofte blive betragtet som forsøg på at begå en anden forbrydelse, f.eks. bedrageri, og vil dermed resultere i strafansvar.

Følgende er eksempler på forbrydelser, hvori identitetsmisbrug kan være den primære måde at operere på - foruden ovennævnte måder:
– uberettiget videregivelse af meddelelser eller billeder vedrørende en andens private forhold (identitetens retmæssige ejer) i medfør af § 26 d eller
– krænkelse af en anden persons agtelse (den retmæssige ejers agtelse) ved fornærmelige
ord eller handlinger eller ved at fremsætte eller udbrede beskyldninger om handlinger, der er egnede til at nedsætte den
agtelse, som en sådan person nyder blandt sine medborgere (§ 267).

Der er ikke en særskilt straf for afsendelse eller kontrol med afsendelse af spam. Men på grund af det brede anvendelsesområde for reglerne om forsøg samt tilskyndelse, råd og dåd vil spam ofte blive betragtet som forsøg på at begå en anden forbrydelse og vil dermed resultere i strafansvar. Hvis afsendelse af spam bevirker, at en internettjeneste, f.eks. en e-mail-konto, bliver utilgængelig, kan dette udgøre en overtrædelse af straffelovens § 293, stk. 2, og det at kontrollere afsendelse af spam kan dermed betragtes som tilskyndelse, råd eller dåd i forbindelse med forøvelse af forbrydelsen. Hvis spam resulterer i nogen form for beskadigelse, sletning eller forringelse af data kan dette udgøre en overtrædelse af § 291 (hærværk).

Juridiske personer er omfattet af strafansvar i overensstemmelse med straffelovens § 306 (jf. § 25-27) for overtrædelse af straffelovens artikler, herunder bestemmelser, der omhandler strafbare handlinger, der begås som cyberkriminalitet. Juridiske personer kan straffes med bøder i overensstemmelse med straffelovens § 50-51. Der er i teorien ikke nogen øvre grænse for bøder, der pålægges i henhold til straffeloven.

Straffeloven indeholder ikke nogen generelle kriterier for, hvad der skal betragtes som "grov lovovertrædelse". Der fastsættes heller ingen juridiske definitioner. Sådanne kriterier er imidlertid typisk indarbejdet i de enkelte artikler om de pågældende lovovertrædelser, og kriterierne er således væsentlige, når de fastsætter den strengeste straf, der finder anvendelse i et specifikt tilfælde.

F.eks. kan systematisk og længerevarende benægtelse af et angreb på en server betragtes som strafbar med den strengeste straf i henhold til § 293, stk. 2. Vurderingen af, hvorvidt en række af sådanne angreb skal betragtes som systematiske eller længerevarende tilfalder i det hele taget retterne.

Mindre lovovertrædelser, der resulterer i bødestraf, kan behandles af politiet uden inddragelse af retten, på betingelse af at gerningsmanden tilstår lovovertrædelsen og er rede til at løse tvisten ved hjælp af en bøde.

A/ Rådets rammeafgørelse 2005/222/RIA om angreb på informationssystemer og Europa-Parlamentets og Rådets direktiv 2013/40/EU om angreb på informationssystemer

Danmark har ikke gennemført direktiv 2013/40/EU om angreb på informationssystemer, som ikke er bindende for Danmark i overensstemmelse med § 1-2 i protokol nr. 22 om Danmarks stilling, der foreligger som bilag til traktaten om Den Europæiske Union og til traktaten om Den Europæiske Unions funktionsmåde.

I forbindelse med en folkeafstemning vedrørende bl.a. Europol, der fandt sted i Danmark den 3. december 2015, foretog Justitsministeriet dog en analyse af Danmarks overholdelse af direktivet. Justitsministeriet har anført, at dansk lovgivning i overvejende grad er i overensstemmelse med direktivet med følgende undtagelser:

- med hensyn til § 9, stk. 3-4, om mindstekrav til den strengeste straf skal der foretages en mindre ændring af § 291, stk. 2, for at sikre, at ulovlig forstyrrelse af et informationssystem med kritisk infrastruktur som følge af sletning, beskadigelse, forringelse, osv., kan straffes med mindst 5 års fængsel
- samme mindre ændring er nødvendig i § 293, stk. 2, sammen med en skærpelse af den strengeste straf til mindst 5 års fængsel, således at den bringes i overensstemmelse med § 9, stk. 3-4. Derudover bør der der i straffeloven fastsættes regler om misbrug af personoplysninger med det formål at vinde en tredjeparts tillid, hvorved den, som identiteten egentlig tilhører, skades, som en skærpende omstændighed med hensyn til samtlige lovovertrædelser med relevans for § 4-5.

B/ Europa-Parlamentets og Rådets direktiv 2011/93/EU om bekæmpelse af seksuelt misbrug af børn og børnepornografi

Danmark har ikke gennemført direktiv 2011/93/EU om bekæmpelse af seksuelt misbrug af børn og børnepornografi, som ikke er bindende for og ikke finder anvendelse i Danmark, i overensstemmelse med § 1-2 i protokol nr. 22 om Danmarks stilling, der foreligger som bilag til traktaten om Den Europæiske Union og til traktaten om Den Europæiske Unions funktionsmåde.

Ved lov nr. 633 af 12. juni 2013 blev straffelovens 24. kapitel om seksualforbrydelser dog ændret. Ændringen omfattede en skærpelse af den strengeste straf for overværelse af pornografisk optræden, hvori der deltager et barn, fra indtil 1 års fængsel til indtil 2 års fængsel, og bragte dermed dansk lovgivning i overensstemmelse med § 4, stk. 4, i direktivet. Derudover blev forældelsesfristen, i tilfælde hvor et barn under den seksuelle lavalder tilskyndes til at overvære seksuelt misbrug uden at deltage (strafbart som blufærdighedskrænkelse i den danske straffelov), ændret, så forældelsesfristen tidligst beregnes fra den dato, hvor barnet fylder 21 år, således at der kan ske retsforfølgning i en tilstrækkelig lang periode, efter at ofret har nået myndighedsalderen.

I forbindelse med en folkeafstemning vedrørende bl.a. Europol, der fandt sted i Danmark den 3. december 2015, foretog Justitsministeriet en analyse af Danmarks overholdelse af direktivet. Analysen viste, at dansk lovgivning i overvejende grad er i overensstemmelse med direktivet.
Med hensyn til § 5, stk. 6, i direktivet, der omhandler fremstilling af børnepornografi, er den strengeste straf i henhold til den danske straffelov ikke i overensstemmelse med direktivet, i tilfælde hvor barnet er ældre end den seksuelle lavalder (15 år), og hvor gerningsmanden ikke har til hensigt at udbrede pornografien.

C/ Onlinesvindel med betalingskort

Nationalt Cyber Crime Center (NC3) er vært for et mødeforum med deltagelse af den største udbyder af digitale betalingsløsninger, flere af de største banker og Finansrådet.

I dette forum deles trends og tendenser – f.eks. nye værktøjer og måder at operere på – og modforanstaltninger drøftes.

D/ Andre fænomener inden for cyberkriminalitet

Det danske politi kæmper for at holde trit med cyberkriminelle, som konstant opfinder og udvikler nye strategier og værktøjer. For at afværge dette problem indfører Nationalt Cyber Crime Center (NC3) konstant nyt software, herunder både kommercielle værktøjer og værktøjer, det selv udvikler. Endvidere ansatte NC3 for nylig højt kvalificerede IT-ingeniører, der skal arbejde ude i de enkelte politikredse.

Nationalt Cyber Crime Center (NC3) deltager i det samarbejde om efterforskning og forebyggelse af svindel med betalingskort, der ledes af Europol. Finansrådet samarbejder med lignende institutioner i hele Europa, ligesom de fleste af de større danske banker indgår i en international finansiel institution. Via disse netværk modtager og sender den danske finansielle sektor oplysninger om grænseoverskridende onlinesvindel med betalingskort.

5.2 Proceduremæssige spørgsmål

5.2.1 Efterforskningsteknikker

Med henblik på efterforskning af lovovertrædelser kan politiet gøre personer - primært mistænkte personer - til genstand for en række tvangsforanstaltninger og midlertidige foranstaltninger.

– Ransagning og beslaglæggelse af oplysninger er mulig under en efterforskning af en lovovertrædelse af cyberkriminel art i overensstemmelse med kapitel 73-74 i retsplejeloven. § 793-806 indeholder almindelige bestemmelser om eftersøgning, ransagning, beslaglæggelse og indefrysning. I § 793 fastsættes anvendelsesområdet for reglerne om ransagning. Med hensyn til efterforskninger af alle de lovovertrædelser, der nævnes i afsnit 2.A., kan der gives tilladelse til ransagning, forudsat at der er rimelig grund til at mistænke den person, hvis ejendom er genstand for ransagningen, for at begå forbrydelsen, og forudsat at ransagningen antages at være af væsentlig betydning for efterforskningen. Ransagning af en tredjeparts (en ikkemistænkts) ejendom kan ske, når der er grund til at antage, at der kan findes beviser eller genstande, der skal beslaglægges. Reglerne om behovet for en retskendelse vedrørende ransagning og de generelle betingelser for en ransagning findes i § 793-798.

I § 801 fastsættes det generelle anvendelsesområde for bestemmelserne om beslaglæggelse og beskrives formålet med beslaglæggelse. Den mest almindelig grund til beslaglæggelse i henhold til § 802 er grunden til at antage, at genstanden kan tjene som bevis eller bør konfiskeres på grundlag af en rimelig grund til at mistænke ejeren eller indehaveren. Der kan også ske beslaglæggelse af en tredjeparts genstande og ejendom på samme betingelser som for en mistænkt person. Reglerne om de generelle betingelser om beslaglæggelse findes i § 805-807.

– Anskaffelse af adgang til websteder, der har blokeret offentlig adgang, bl.a. ved hjælp af en kodeord, betragtes i juridisk henseende som en ransagning i overensstemmelse med retsplejeloven. Et elektronisk dokument betragtes i juridisk henseende som en genstand i forbindelse med ransagning og beslaglæggelse. Det betyder, at et websted med ulovligt indhold kan beslaglægges i overensstemmelse med reglerne om beslaglæggelse i retsplejeloven.

– Anvendelsen af aflytning i realtid af trafik- og indholdsdata er i medfør af § 791 b begrænset til grove lovovertrædelser med hensyn til cyberkriminalitet, som kan straffes med 6 års fængsel. Dermed er aflytning ikke mulig som led i en efterforskning af en person, der på ulovlig vis hindrer en anden i at anvende eller råde over elektroniske data, osv., f.eks. et "denial of service attack" på tjenester i overensstemmelse med straffelovens § 293, stk. 2. Foruden denne grundlæggende betingelse skal der foreligge rimelig grund til at antage, at en mistænkt anvender eller foretager forsendelse af oplysninger, eller en antagelse om, at aflytningen er afgørende for efterforskningen.

– I henhold til retsplejelovens § 781 kan der også foretages aflytning af telekommunikation i forbindelse med grove lovovertrædelser med hensyn til cyberkriminalitet, som kan straffes med mindst 6 års fængsel, og ved en række andre nærmere angivne lovovertrædelser, hvis der er rimelig grund til at antage, at en mistænkt anvender eller foretager forsendelse af oplysningerne, eller hvis det antages, at aflytningen er af afgørende betydning for efterforskningen. Denne foranstaltning omfatter udbredelse af e-mail-korrespondance og andet tilgængeligt indhold. Denne artikel omhandler aflytning af telekommunikation gennem udbydere af teletjenesters faciliteter i modsætning til aflytning i henhold til § 791 b, som omfatter "aflæsning" ved hjælp af computere (eller andre informationssystemer).

Udbydere af telekommunikationstjenester kan blive pålagt at foretage hastesikring af elektroniske data i henhold til § 786 a. Et pålæg om hastesikring forpligter udbydere til at opbevare data indtil 90 dage. Inden for denne periode kan politimyndighederne sikre disse data ved beslaglæggelse i henhold til § 801-802.

Derudover kan en udbyder af teletjenester kun blive pålagt at udlevere kundeoplysninger, der er nødvendige for dynamiske IP-adresser, i overensstemmelse med § 804, forudsat at pålægget meddeles som led i en efterforskning af en lovovertrædelse, og forudsat at der er rimelig grund til bl.a. at antage, at genstanden eller oplysningen kan tjene som bevis.

Politiet kan anmode om oplysninger om statistiske IP-adresser uden en retskendelse.

Udbydere af telekommunikationstjenester har pligt til at opbevare trafikdata i mindst 1 år i overensstemmelse med § 786, stk. 4, og ministeriel bekendtgørelse nr. 988, udstedt den 28. september 2006. Bestemmelserne forpligter udbydere af telekommunikationstjenester til at opbevare en bred vifte af oplysninger om telekommunikationstrafik, således at de efterfølgende kan udleveres til politiet som led i efterforskningen, og hvis der foreligger en retskendelse. Oplysninger om internettrafikdata med undtagelse af basisoplysninger om abonnenten er ikke længere et krav i henhold til 786, stk. 4, og ovennævnte ministerielle bekendtgørelse.

Et pålæg om opbevaring af trafik- og indholdsdata kan udstedes af en ret i medfør af § 783, jf. § 781-782. Som for aflytning af kommunikation er udlevering af trafik- og indholdsdata begrænset til grove lovovertrædelser med hensyn til cyberkriminalitet, som kan straffes med mindst 6 års fængsel. En særlig undtagelse fra den 6-årige fængselsstraf finder anvendelse i forbindelse med overtrædelse af straffelovens § 235 og § 263, stk. 2, jf. retsplejelovens § 781, stk. 2. Denne artikel omhandler tilegnelse af ulovlig adgang til data eller programmer, der er bestemt til brug i et informationssystem ("traditionel hacking"). En lignende undtagelse finder anvendelse i forbindelse med efterforskninger af databedrageri i henhold til straffelovens § 279 a, jf. retsplejelovens § 781, stk. 3.

Foruden denne grundlæggende betingelse skal der foreligge rimelig grund til at antage, at en mistænkt anvender eller foretager forsendelse af oplysninger, og at aflytningen er af afgørende betydning for efterforskningen.

I henhold til § 781, stk. 3, afsnit 1), er opbevarede trafikdata, der kan kræves udleveret i overensstemmelse med § 781 oplysninger om telekommunikationstrafik, der vedrører et specifikt telefonnummer eller en specifik IP-adresse, og i henhold til stk. 4 oplysninger om al telekommunikationstrafik inden for en nærmere angivet radius af en beliggenhed. Der kan meddeles pålæg om udlevering af brugeroplysninger i medfør af § 804. I forbindelse med IP-adresser er en retskendelse om udlevering kun nødvendig for dynamiske IP-adresser. Udbydere af telekommunikationstjenester har pligt til at udlevere brugeroplysninger om statiske IP-adresser til politiet.

Under besøget på stedet blev evalueringsholdet orienteret om situationen vedrørende opbevaring af trafikdata, der anvendes i forbindelse med efterforskning:

Danmark indførte lovgivningsmæssige bestemmelser for så vidt angår telekommunikation og opbevaring af internettrafikdata i 2002. I 2007 blev den nationale lovgivning ændret i overensstemmelse med EU-direktivet. Under hensyntagen til Domstolens dom i 2014 konkluderede Danmark, at den nationale lovgivning om opbevaring af data bør opretholdes for så vidt angår eksisterende retsgarantier. Reglerne om opbevaring af internettrafikdata viste sig imidlertid ikke at være tilpasset i praksis. Danmark valgte at ophæve og ændre dem efter samråd med leverandører af tjenesteydelser og andre interessegrupper, herunder NGO'er, der beskæftiger sig med grundlæggende rettigheder. Et nyt lovgivningsforslag er under udarbejdelse med henblik på vedtagelse i løbet af de kommende måneder.

De særlige efterforskningsteknikker, der anvendes. Nationalt Cyber Crime Center (NC3) anvender analyser af log-/trafikdata og prøver på malware til at bedømme angrebets/malwarens oprindelse samt de stjålne datas bestemmelsessted. NC3 benytter sig endvidere af aflytning for at profilere en mistænkt inden en eventuel anholdelse, hvilket blandt andet kan afsløre, hvorvidt han/hun anvender VPS. Endelig anvender NC3 menneskelige kilder og åbne kilder med henblik på at indsamle efterretninger og beviser.

5.2.2 Kriminaltekniske undersøgelser og kryptering

Eftersom kryptering er standard i mange applikationer, støder det danske politi ofte på problemer med krypterede data. Krypteringen gør det vanskeligt at få adgang til indholdet på beslaglagte enheder.
For så vidt angår aflytning er politiet begrænset til trafikdata, eftersom krypteringen forhindrer adgang til indholdet.

Nationalt Cyber Crime Center (NC3) har erfaring med, at kryptering anvendes til en bred vifte af overtrædelser. Centret imødegår udfordringen ved hjælp af "brute force" og indsamling af efterretninger, f.eks. afhøring af gerningsmanden og indsamling af kodeord fra dennes andre enheder.

På strategisk niveau drøfter de retshåndhævende myndigheder i Danmark udfordringerne ved cyberkriminalitet, f.eks. kryptering. På det efterforskningsmæssige plan kan de forskellige retshåndhævende myndigheder anmode hinanden om hjælp i specifikke sager.

NC3 er et kriminalteknisk center, der støtter de lokale politikredse. I Danmark foregår de retshåndhævende myndigheders dekryptering ikke i samarbejde med private virksomheder. NC3 har stadig kun haft begrænset succes med enkelte sager. NC3 har udført elektroniske kriminaltekniske undersøgelser ved hjælp af Encase. Det er muligt at udføre kriminaltekniske undersøgelser af en bred vifte af udstyr spændende fra USB-nøgler og mobiltelefoner til serveranlæg.

NC3 kan også udføre kriminaltekniske undersøgelser for så vidt angår både cloudtjenester og fysiske servere, som man kan få adgang til via internettet. Kriminaltekniske undersøgelser via fjernadgang kan udføres på flere forskellige måder, f.eks. ved kildebaseret aflytning eller ved at udnytte en servers svaghed til at få adgang til filsystemet osv. Disse metoder kræver, at politiet forinden får en retskendelse.

Endelig har NC3 adgang til et værktøj til efterretninger indhentet fra åbne kilder, der kan anvendes til at indhente data fra åbne kilder såsom aviser og offentlige Facebooksider osv., og som kan overvåge sådanne sider løbende.

5.2.3 Elektronisk bevismateriale

Den nationale lovgivning indeholder ingen juridiske definitioner på termerne *computerdata, indholdsdata, trafikdata, kendelser om ransagning/beslaglæggelse af informationssystemer eller netværker, der styres eller kontrolleres af personer under mistanke for cyberkriminalitet*.

Danmark har ingen juridisk definition af elektronisk bevismateriale. **De danske domstole opererer dog med et begreb, der kaldes "fri bevisdømmelse".** Det indebærer, at bevismateriale, der fremlægges for retten, kan benyttes. Domstolene vil herefter vurdere fra sag til sag, hvor meget værdi hvert enkelt stykke bevismateriale skal tillægges. Enhver fejl i forhold til erhvervelsen af bevismateriale eller ethvert udokumenteret trin i beviskæden vil føre til, at det pågældende bevismateriale tillægges mindre værdi i forbindelse med domstolenes afgørelse.

Politiet kan erhverve elektronisk bevismateriale i henhold til de generelle regler i den danske retsplejelov. De gav udtryk for, at det i forbindelse med cybersager er meget vigtigt, at beviskæden er veldokumenteret med hensyn til, hvordan bevismaterialet blev erhvervet fra starten, hvem der har håndteret det og hvordan – herunder hvorvidt det på nogen måde er blevet ændret – helt frem til det tidspunkt, hvor bevismaterialet anvendes ved en domstol.

De vigtigste udestående juridiske spørgsmål vedrører den juridiske status for tjenesteydernes opbevaring og de retshåndhævende myndigheders brug af internettrafikdata. Som beskrevet i punkt 5.2.1 ovenfor afventes der en juridisk afgørelse desangående – hvilket for øjeblikket efterlader de retshåndhævende myndigheder med en ubehagelig uvished.

5.3 Beskyttelse af menneskerettigheder/grundlæggende rettigheder

I Danmark har udbyderne af kommunikationstjenester pligt til at opbevare telekommunikationsdata samt abonnentoplysninger i 12 måneder. Det danske politi har kun adgang til og kan kun anvende de opbevarede data, hvis der foreligger en relevant retskendelse fra de danske domstole. Det bør dog bemærkes, at en sådan retskendelse ikke er nødvendig, hvis den registrerede giver sit samtykke.

Nationalt Cyber Crime Center (NC3) har udarbejdet en intern politik vedrørende alle dets databaser og registre med personlige identifikationsdata. Denne interne politik omfatter regler vedrørende sikkerhedsforanstaltninger, adgang til data i databaserne osv. samt regler vedrørende sletning af data.

I henhold til § 263, stk. 2, er det ulovligt at skaffe sig adgang til en andens data eller programmer i et informationssystem uden tilladelse. Dette kan eventuelt omfatte internettet.

Endvidere regulerer den danske lov om behandling af personoplysninger forvaltningen af personoplysninger i informationssystemer underlagt Datatilsynets myndighed. Sidstnævnte kan træffe beslutning om, hvorvidt en eventuel behandling er i overensstemmelse med reglerne i loven om behandling af personoplysninger.

Hvis Datatilsynet afdækker strafbare overtrædelser af loven om behandling af personoplysninger i forbindelse med behandlingen af en klage eller en inspektion, er Datatilsynet bemyndiget til at udstede et forbud eller et påkrav eller anmelde overtrædelsen til politiet.

Det danske politis efterforskninger udføres i henhold til den danske retsplejelov.

5.4 Retlig kompetence

5.4.1 De principper, der anvendes til efterforskning af cyberkriminalitet

De danske kompetenceregler i § 6-9 i straffeloven fastsætter den retlige kompetence med hensyn til bl.a. cyberkriminalitet begået enten helt eller delvist i Danmark.

Straffelovens § 6 fastsætter: "Under dansk straffemyndighed hører handlinger, som foretages –
1) i den danske stat,
2) på dansk fartøj, som befinder sig inden for et fremmed myndighedsområde, af en person, der hører til fartøjet eller som rejsende følger med dette, eller
3) på dansk fartøj, som befinder sig uden for et myndighedsområde."
Der henvises til § 9, stk. 2, i straffeloven.
I § 9 fastsættes følgende:
"Handlinger anses for foretaget, hvor gerningsmanden befandt sig ved handlingens foretagelse. For så vidt angår juridiske personer, anses handlinger for foretaget, hvor den eller de handlinger, som medfører ansvar for den juridiske person, er foretaget.
Stk. 2. Hvis en handlings strafbarhed afhænger af eller påvirkes af en indtrådt eller tilsigtet følge, anses handlingen tillige for foretaget, hvor virkningen er indtrådt, eller hvor gerningsmanden har forsæt til, at virkningen skulle indtræde.
Stk. 3. Forsøg- og medvirkenshandlinger anses for foretaget i den danske stat, hvis gerningsmanden befandt sig [i Danmark] ved handlingens foretagelse, uanset om lovovertrædelsen fuldbyrdes eller tilsigtes fuldbyrdet uden for den danske stat.
Stk. 4. Når en del af en lovovertrædelse er begået i den danske stat, anses lovovertrædelsen i sin helhed for at være begået [i Danmark]."

Straffelovens § 7 omhandler princippet om den aktive person. § 7 fastsætter at:

"Under dansk straffemyndighed hører handlinger, som foretages inden for et fremmed myndighedsområde af en person, der på tidspunktet for sigtelsen har dansk indfødsret, er bosat i den danske stat eller har lignende fast ophold [i Danmark], hvis

1) handlingen også er strafbar efter lovgivningen på gerningsstedet (dobbelt strafbarhed) eller

2) gerningsmanden også på gerningstidspunktet har den nævnte tilknytning [til Danmark] og handlingen

a) omfatter seksuel udnyttelse af børn, menneskehandel eller kvindelig omskæring eller

b) er rettet mod nogen, der på gerningstidspunktet har den nævnte tilknytning [til Danmark].

Stk. 2. Under dansk straffemyndighed hører endvidere handlinger, som foretages uden for et myndighedsområde af en person, der på tidspunktet for sigtelsen har den i stk. 1 nævnte tilknytning [til Danmark], hvis handlinger af den pågældende art kan medføre højere straf
end fængsel i 4 måneder.

Stk. 3. Stk. 1, nr. 1, og stk. 2 finder tilsvarende anvendelse med hensyn til handlinger foretaget af en person, som på tidspunktet for sigtelsen har indfødsret eller er bosat i Finland, Island, Norge eller Sverige, og som opholder sig [i Danmark]."

For så vidt angår princippet om den passive person henvises der til straffelovens § 7 a. I § 7 a fastsættes det at:

"Under dansk straffemyndighed hører handlinger, som foretages inden for et fremmed myndighedsområde, og som er rettet mod nogen, der på gerningstidspunktet har dansk indfødsret, er bosat i den danske stat eller har lignende fast ophold her [i Danmark], hvis handlingen også er strafbar efter lovgivningen på gerningsstedet (dobbelt strafbarhed) og efter dansk lovgivning kan medføre straf af fængsel i mindst 6 år.

Stk. 2. Dansk straffemyndighed efter stk. 1 er betinget af, at handlingen omfatter

1) forsætligt drab,

2) grov vold, frihedsberøvelse eller røveri,

3) en almenfarlig forbrydelse,

4) en seksualforbrydelse eller incest eller

5) kvindelig omskæring.

Stk. 3. Under dansk straffemyndighed hører endvidere handlinger, som foretages uden for et myndighedsområde, og som er rettet mod nogen, der på gerningstidspunktet har den i stk. 1 nævnte tilknytning [til Danmark], hvis handlinger af den pågældende art kan medføre højere straf end fængsel i 4 måneder."

For så vidt angår juridiske personer henvises der til straffelovens § 7 b:
"Når dansk straffemyndighed over for en juridisk person er betinget af dobbelt strafbarhed, omfatter det ikke et krav om, at lovgivningen på gerningsstedet hjemler strafansvar for en juridisk person."

5.4.2 Regler vedrørende kompetencekonflikter og henvisning til Eurojust

Danmark har ikke en lov vedrørende kompetencekonflikter i tilfælde, hvor en eller flere medlemsstater efterforsker og retsforfølger den samme gerningsmand. De danske myndigheder udtalte dog, at anklagemyndighedens beslutning om at retsforfølge visse sager eller ej afhænger af sådanne spørgsmål. Beslutningen baseres bl.a. på den juridiske teori om ne bis in idem-princippet.

Rigsadvokaten har ingen oplysninger om, hvorvidt Danmark har oplevet kompetencekonflikter i sager vedrørende cyberkriminalitet. I forbindelse med ikrafttrædelsen af Rådets rammeafgørelse 2009/948/RIA af 30. november 2009 om forebyggelse og bilæggelse af konflikter om udøvelse af jurisdiktion i straffesager overvejede det danske justitsministerium, om principperne i rammeafgørelsen allerede var i brug af den danske anklagemyndighed i sager om kompetencekonflikter.

Med henblik på at sikre rammeafgørelsens fulde gennemførelse i dansk lovgivning har justitsministeriet dog anmodet Rigsadvokaten om at udstede en instruks til anklagemyndigheden, ifølge hvilken sager med kompetencekonflikter bør håndteres i overensstemmelse med rammeafgørelsen.
Denne instruks er under udarbejdelse af Rigsadvokaten.

5.4.3 Kompetence i forbindelse med cyberkriminalitet begået i "skyen"

Den 10. maj 2012 afsagde Højesteret dom i en sag vedrørende erhvervelse af data fra en Facebook- og Messengerprofil tilhørende en mistænkt i en strafferetlig efterforskning. Højesteret fastslog, at det danske politi havde lov til at skaffe sig adgang til Facebook- og Messengerprofilerne via internettet med profilernes korrekte kodeord, som var kommet i deres besiddelse ved hjælp af andre efterforskningsmæssige foranstaltninger. Baggrunden herfor var, at den efterforskede lovovertrædelse var underlagt dansk kompetence, og at det var muligt at få adgang til profilerne uden at skulle involvere udenlandske myndigheder.

5.4.4 Opfattelsen af Danmark for så vidt angår de retlige rammer til bekæmpelse af cyberkriminalitet

På side 69 i spørgeskemaet fra GENVAL anerkendte Danmark generelt behovet for yderligere lovgivningsmæssige fremskridt. *De danske myndigheder opfordres af evalueringsholdet til at oplyse flere detaljer om de nuværende overvejelser og hvilke fremskridt, der er gjort på dette område.*

Se punkt 9.5 nedenfor for så vidt angår vurderingen af og forslag fra Danmark vedrørende EU-lovgivning.

5.5 Konklusioner

- **Den danske straffelov er generelt nøje tilpasset hele området for efterforskning af cyberkriminalitet. De danske myndigheder kan tiltvinge sig adgang til og opsnappe oplysninger osv. i henhold til dansk lovgivning, der beskytter de danske borgeres rettigheder.**

- **Det er værd at nævne, at når Danmark ikke deltager i EU-lovgivning på det strafferetlige område, gennemgår Justitsministeriet systematisk denne lovgivning og søger så vidt muligt at tilpasse den nationale lovgivning til EU-krav. Nogle huller kan udfyldes ved hjælp af instrukser til anklagere.**

- **Lovgivning vedrørende den obligatoriske opbevaring af teletrafikdata er på plads. Regler vedrørende internettrafikdata mangler dog og er under udarbejdelse (tidsfrist folketingsåret 2016-2017).**

- **Som mange andre medlemsstater mangler Danmark tydelige regler til løsning af konflikter med andre lande om kompetence i cyberspace, men Rigsadvokaten er ved at udarbejde en instruks til anklagemyndigheden.**

6 OPERATIONELLE ASPEKTER

6.1 Cyberangreb

6.1.1 Cyberangrebs natur

Cyberangreb mod kritisk infrastruktur tilhørende offentlige og private danske institutioner af væsentlig betydning for samfundet overvåges af Center for Cybersikkerhed. En nylig trusselsvurdering fra Center for Cybersikkerhed peger mod spionage og kriminalitet for så vidt angår svindel og afpresning (f.eks. ransomware) som den største trussel mod danske myndigheder og virksomheder.

Rigspolitiet har dog ikke statistikker over antallet af angreb.
Med hensyn til spionage har der været statssponsorerede angreb mod de danske myndigheder og den private sektor. Et nyligt angreb mod det danske udenrigsministerium varede ca. syv måneder og bestod af 47 e-mails til ni forskellige konti i ministeriet. E-mailene kom fra 21 adresser. Angrebene var veludførte, men mislykkedes, idet de enten blev blokeret af ministeriets mailscanner, eller sikkerhedssystemet blokerede kommunikationen mellem malwaren og den eksterne aktør. Konklusionen fra dette angreb og andre lignende angreb er, at et aktivt forsvar tager hensyn til både ledelsen og medarbejderne med fokus på passende tekniske løsninger. De teknikker, der bruges til social engineering, bliver mere og mere sofistikerede, og det er meget vigtigt, at alle medarbejdere er opmærksomme på sikkerheden.

For så vidt angår cyberkriminalitet stiger antallet af sager med svindel og afpresning. I løbet af 2015 var der flere "bølger" af ransomwareangreb rettet mod private borgere, virksomheder og offentlige institutioner. Rigspolitiet håndterer endvidere et stigende antal sager vedrørende svindel med betalingskort.

Trusler fra aktører, der er politisk motiverede, vurderes af Center for Cybersikkerhed som en mellemstor trussel. Der har ikke været mange seriøse angreb af denne type, men evnen og viljen til at angribe en virksomhed eller et forretningsområde, der har fået negativ opmærksomhed, er til stede.

6.1.2 Mekanisme til at reagere på cyberangreb

Den danske regering har besluttet, at alle statslige myndigheder skal indberette alle væsentlige cyberangreb til Center for Cybersikkerhed med henblik på at sikre situationskendskabet og det bedst mulige overblik over den nuværende sikkerhedssituation. Hvis Danmark udsættes for eller trues af et cyberangreb med store konsekvenser for dele af samfundet, aktiveres krisestyringsorganisationen under Statsministeriet ved hjælp af de generelle procedurer, der er fastsat i den nationale beredskabsplan.

Formålet med Center for Cybersikkerhed er at bidrage til Danmarks beskyttelse mod cybertrusler. En af dets vigtigste opgaver er at indberette og bekæmpe cyberangreb rettet mod Danmarks nationale sikkerhed og danske interesser.

Det danske Center for Cybersikkerhed tager føringen med hensyn til spørgsmål vedrørende cyberangreb og virker til at være godt rustet til at udføre denne opgave. Det samarbejder både med efterretnings- og sikkerhedstjenesterne og NC3. Center for Cybersikkerhed vurderer de modtagne oplysninger inden videreformidling til den rette aktør. Den Nationale Operative Stab (NOST) er en koordineret tværfaglig mekanisme, der kan aktiveres i tilfælde af et alvorligt cyberangreb. Rigspolitiet, Politiets Efterretningstjeneste (PET) og Center for Cybersikkerhed/Forsvarets Efterretningstjeneste (FE) er permanente medlemmer af Den Nationale Operative Stab (NOST).

6.2 Foranstaltninger mod børnepornografi og seksuel udnyttelse online

Nationalt Cyber Crime Center (NC3) har en afdeling med 15 medarbejdere, der udelukkende tager sig af sager med seksuel udnyttelse af børn: 9 IT-kriminaltekniske efterforskere, 2 online-efterforskere, 2 proaktive efterforskere, 1 specialist i offeridentifikation og 1 holdleder.

NC3 arbejder med efterforskning af seksuel udnyttelse af børn på nationalt og koordinerende plan, og i hver enkelt sag ligger kompetencen hos den lokale politikreds.
Dette betyder, at anholdelser, ransagninger, afhøringer osv. er politikredsenes ansvar. NC3 udfører sin efterforskning i samarbejde med de 12 politikredse i Danmark.

Alle kriminaltekniske undersøgelser af beslaglagt digitalt udstyr udføres af NC3.

6.2.1 Softwaredatabaser, der kan identificere ofre, og foranstaltninger, der har til formål at undgå fornyet viktimisering

Nationalt Cyber Crime Center (NC3) bruger sin egen database og Interpols ICSE-database til at identificere ofre i Danmark. Endvidere har NC3 udviklet en lignende software som teknisk backup til identificeringsindsatsen.

Nationalt Cyber Crime Center (NC3) har gode erfaringer med at blokere for websteder med ulovligt materiale indeholdende seksuel udnyttelse af børn.

NC3 samarbejder med NGO'en *Red Barnet* og flertallet af danske internetudbydere i det såkaldte "Netfilter"-samarbejde. Formålet med "Netfilter"-samarbejdet er på frivillig basis at blokere for adgangen til materiale på internettet, hvor børn bliver seksuelt udnyttet. I denne henseende underretter NC3 regelmæssigt internetudbyderne om websteder, som NC3 vurderer indeholder materiale, der er omfattet af straffelovens bestemmelser om børnepornografi. Det er efterfølgende internetudbyderne, der blokerer websteder i overensstemmelse med internetudbyderens betingelser. Dette samarbejde har vist sig at være nyttigt og effektivt i en række sager vedrørende seksuel udnyttelse af børn online, navnlig i sager med servere placeret i udlandet.

6.2.2 Foranstaltninger til imødegåelse af seksuel udnyttelse/misbrug online, sexting, cybermobning

Red Barnet, Danmark, og **Børns Vilkår**, som tilbyder **telefonisk rådgivning til børn**, laver regelmæssige kampagner målrettet mod børn, unge og forældre med henblik på at forebygge, at børn og unge bliver ofre for seksuel udnyttelse.

6.2.3 Forebyggende foranstaltninger mod sexturisme, børnepornografisk optræden o.a.

Red Barnet, Danmark, og den telefoniske rådgivningstjeneste Børns Vilkår har telefonlinjer, hvor børn, unge og forældre kan modtage rådgivning om, hvordan man skal reagere i tilfælde af seksuel udnyttelse af børn eller seksuel opførsel på internettet og rådgivning via chat samt f.eks., hvordan man melder det til politiet.

På Rigspolitiets websted har Nationalt Cyber Crime Center (NC3) offentliggjort informationsmateriale til henholdsvis børn og forældre/voksne med ansvar for børn om, hvordan man opfører sig på internettet, information om internetrelateret kriminel aktivitet, hvordan man melder det til politiet, og hvad man som borger selv kan gøre for at undgå at blive offer for seksuel udnyttelse online og stoppe yderligere spredning af sådant materiale.

6.2.4 Aktører og foranstaltninger til bekæmpelse af websteder, der indeholder eller formidler børnepornografi

I de sager, hvor ulovligt indhold opdages på en server i Danmark, kan det danske politi få en retskendelse, der giver dem tilladelse til at beslaglægge serveren og/eller det domæne, som serverens indhold er placeret på.

Som tidligere nævnt er formålet med det danske "Netfilter"-blokeringssystem at blokere adgang til websteder, der indeholder materiale med børnemisbrug. Deltagelse i ordningen er frivillig for internetudbyderne, og hver enkelt internetudbyder skal undertegne og overholde en kontrakt. NC3 står for administrationen af "Netfilter". NC3's medarbejdere vurderer og tilføjer websteder til filteret. Selve blokeringen håndteres af udbyderne af kommunikationstjenester, hvor filtreringen foregår. Blokeringen er en DNS-blokering, hvilket betyder, at det er selve URL-adressen, der blokeres. Webstedet fjernes ikke fra internettet og kan stadig konsulteres via IP-adressen.

Hver dag vurderer medarbejderne hos Nationalt Cyber Crime Center (NC3) mulige ulovlige websteder med henblik på at beslutte, hvorvidt webstedet bør blokeres eller ej. Hvis et websted skønnes ulovligt, tilføjes det "Netfilter"-databasen. En gang i timen genererer "Netfilter"-databasen automatisk en liste over websteder, der skal blokeres af internetudbyderne. En gang om dagen downloader internetudbyderne listen og bruger den til at blokere for adgangen til ulovlige websteder.

Der er fire måder, hvorpå NC3 indhenter viden om websteder til yderligere vurdering:

1. Når der gøres et forsøg på at få adgang til et blokeret websted, oprettes der hos internetudbyderen en logfil med oplysninger om, hvor brugeren kom fra, da vedkommende endte på det blokerede websted. Disse logfiler sendes til NC3 en gang om dagen. Logfilen er anonym og indeholder ingen oplysninger, der kan identificere brugeren, men kun oplysninger om, hvilket websted brugeren var på, inden vedkommende blev mødt af det blokerede websted. Disse websteder vurderes efterfølgende.
2. Anmeldelser fra borgere og *Red Barnet, Danmark*.
3. Websteder, der er blevet opdaget i løbet af efterforskningen af sager.
4. Internationale samarbejdsforbindelser, herunder Interpol og Europol.

Samarbejdet med de danske internetudbydere med henblik på at blokere for adgangen til ulovlige websteder har netop fejret sit 10 års jubilæum og forløber problemfrit. I de sager, hvor serveren er placeret i udlandet, efterlyser NC3 koordinering gennem Interpol og deres "worst of"-liste over de værste domæner.

Danmark benytter ofte Interpols database over seksuel udnyttelse af børn til identificering af ofre. Danmark har endvidere været involveret i udviklingen af Interpols ICSE-projekt helt fra begyndelsen. Rigspolitiet benytter ICSE gennem deres egen direkte VPN-forbindelse.

Nationalt Cyber Crime Center (NC3) deltager i Europols EU-strategiske gruppe af chefer for de nationale højteknologikriminalitetsenheder og så vidt muligt også i andre former for strategisk samt operationelt samarbejde.

6.3 Onlinesvindel med kort

Digitaliseringsstyrelsen tilbyder danske borgere og udlændinge bosiddende i Danmark "NemID", som er et sikkert login til internettet. Det består af et bruger-ID, et kodeord og et kodekort med engangskodeord. I dag kræver de fleste telekommunikationsudbydere, finansieringsselskaber og andre danske internetforhandlere NemID som identifikation.

Endvidere beskyttes betalinger online af virksomheder, der specialiserer sig i at formidle digital betaling. Disse virksomheder forbinder banker, virksomheder og forbrugere i et internationalt netværk og formidler digital betaling over hele Norden med en bred vifte af kortydelser, kontoydelser og betalingsløsninger for forretningsdrivende.

6.3.1 Indberetning af onlinesvindel med kort

De danske myndigheder har vurderet, at rigtig mange tilfælde af onlinesvindel anmeldes til de retshåndhævende myndigheder, eftersom dette er en betingelse hos de fleste forsikringsselskaber.

6.3.2 Den private sektors rolle

For så vidt angår banksvindel online organiserer Nationalt Cyber Crime Center (NC3) et mødeforum med deltagelse af den største udbyder af digitale betalingsløsninger, flere af de største banker og Finansrådet. I dette forum deles trends og tendenser – f.eks. nye værktøjer og måder at operere på – og modforanstaltninger drøftes.

6.4 Andre fænomener inden for cyberkriminalitet

Det danske politi kæmper med at holde trit med cyberkriminelle, som konstant opfinder og udvikler nye strategier og værktøjer. For at afhjælpe dette problem indfører Nationalt Cyber Crime Center (NC3) løbende nyt software, herunder både kommercielle værktøjer og værktøjer, de selv har udviklet. Endvidere ansatte NC3 for nylig højt kvalificerede IT-ingeniører, der skal arbejde ude i de 12 politikredse.

6.5 Konklusioner

- **Det danske Center for Cybersikkerheds kapacitet til at fungere som clearinginstitut med hensyn til oplysninger mellem sig selv, politiet (NC3) og efterretningstjenesterne kan promoveres som en mekanisme, der fremmer god praksis.**

- **NC3 tager føringen med hensyn til efterforskning af onlinemateriale indeholdende seksuel udnyttelse af børn og vedligeholder endvidere det nationale HashSet for så vidt angår billeder med misbrug af børn.**

- **Efterforskerne i NC3 støttes i deres arbejde af en "innovationsafdeling" bestående af civile IT-eksperter, der yder teknisk bistand og konstant søger at forbedre NC3's effektivitet og kompetence.**

- **Alle adspurgte danske organisationer accepterer, at der er behov for en blanding af politifolk og civilt ansatte inden for dette område. De anerkender dog, at der er et problem med at fastholde medarbejdere og for at afhjælpe dette har de forsøgt at udvikle et førsteklasses arbejdsmiljø.**

- **NC3 udfører sine opgaver sammen med NGO'er og internetudbydere. En specifik og værdifuld mekanisme, der anvendes i samarbejde med sidstnævnte, er "Netfilter"-projektet, der registrerer brugere, der søger at få adgang til et websted, der er blevet blokeret på grund af ulovligt indhold. Det websted, der blev besøgt umiddelbart forinden, videregives til NC3. Viser dette websted sig at have et lignende indhold, blokeres det også. Logfilen anonymiseres dog og indeholder ingen data, der kan identificere brugeren.**

7 INTERNATIONALT SAMARBEJDE

7.1 Samarbejde med EU-agenturer

7.1.1 Formelle krav for samarbejdet med Europol/EC3, Eurojust, ENISA

Folkeafstemningen den 3. december 2015 endte med et "nej" til at afskaffe retsforbeholdet. Den danske regering søger nu at opnå en parallelaftale, så Danmark fortsat kan deltage i Europols/EC3's aktiviteter.

Samarbejdet med det nationale kontor i Eurojust er ikke underlagt nogen formelle krav eller specifikke procedurer. Med gennemførelsen af Eurojustafgørelsen opfordrede Danmark de lokale politikredse og anklagere til at udnytte Eurojusts bistand optimalt. Dette er blevet fremmet gennem uformelle kontakter og samarbejde.

7.1.2 Vurdering af samarbejdet med Europol/EC3, Eurojust og ENISA

Europol/EC3. I sager med internationale forbindelser sender Nationalt Cyber Crime Center (NC3) rapporter og f.eks. prøver på malware til Europol/EC3. I en række sager har EC3 været anvendt som knudepunkt til at koordinere distributionen af informationer blandt en lang række medlemsstater. NC3 deltager i EMPACT-samarbejdet og de deraf afledte operationer.

Det er NC3's vurdering, at EC3 har skabt en ramme og et grundlag for tillid og tæt samarbejde mellem medlemsstaterne, hvilket er afgørende for at bekæmpe international cyberkriminalitet. Ifølge de danske myndigheder har EC3's koordination, dataindsamling, analyser af malware osv. haft og vil fremover fortsat have en betydelig indvirkning på bekæmpelsen af international cyberkriminalitet.

Eurojust. Det lokale kontor i Eurojust har bistået de danske myndigheder i en række sager. Heraf kan nævnes følgende eksempler:
– En omfattende sag om cyberangreb, som blev begået af en svensk statsborger. Det nationale kontor hjalp med at indhente oplysninger om retspraksis fra andre EU-medlemsstater.

– En sag om børnepornografi. Det nationale kontor hjalp med at indhente oplysninger fra Rumænien om et forsøg på at købe et barn til seksuelle formål.
– En række sager om onlinesvindel og kreditkortsvindel. Det nationale kontor har hjulpet på flere forskellige måder, bl.a. ved at deltage i og arrangere koordinationsmøder.

I nogle tilfælde bistås anklagemyndigheden endvidere af den nationale enhed i Europol.

Det danske nationale medlem af Eurojust har bemærket, at oplysninger, som indsamles af Europol/EC3, i visse sager kunne anvendes mere systematisk for at sikre en koordineret efterforskning og retsforfølgning, da disse oplysninger kan give et bedre overblik, end hvad der er muligt ved at se på enkeltstående tilfælde.

7.1.3 Fælles efterforskningsholds og cyberpatruljers operationelle kapacitet

Fælles efterforskningshold. Nationalt Cyber Crime Center (NC3) har ikke deltaget i officielle fælles efterforskningshold, men NC3 har adskillige gange deltaget i fælles operationer og efterforskninger sammen med en række andre medlemsstater.

Det nationale kontor i Eurojust har meddelt, at Danmark har deltaget i et fælles efterforskningshold med Tyskland angående onlinesvindel begået i Tyskland og rettet mod kunder i Danmark. For øjeblikket deltager Danmark også i et fælles efterforskningshold angående menneskehandel, hvor forbrydelsen ligeledes er begået ved anvendelse af internettjenester, elektroniske identiteter og signaturer.
Danmark undersøger muligheden for finansiering fra Eurojust i alle sager, hvor der oprettes fælles efterforskningshold.

Cyberpatruljer. Nationalt Cyber Crime Center (NC3) deltager i forskellige tiltag, der koordineres af Europol, og som bl.a. er rettet mod slutbrugere af kriminalitet som en tjenesteydelse ("Crime As a Service"). Endvidere anvender NC3 virtuelle agenter til at infiltrere pædofile netværk på internettet.

Rigspolitiet finder, at de koordinerede tiltag i form af anholdelser, pressemeddelelser og oplysning har en indvirkning på rekrutteringsbasen, og at der dermed vil blive færre cyberkriminelle fremover. Deres erfaringer med at infiltrere pædofile netværk ved hjælp af virtuelle agenter er begrænsede, da det er vanskeligt for dem at agere som pædofile, eftersom de ikke må uploade pædofilt materiale.

7.2 Samarbejdet mellem de danske myndigheder og Interpol

Nationalt Cyber Crime Center (NC3) har et godt samarbejde med Interpol, navnlig i sager angående seksuelt misbrug af børn. NC3 er tilsyneladende meget aktivt i forbindelse med udviklingen af Interpols ICSE-database.

7.3 Samarbejdet med tredjelande

Nationalt Cyber Crime Center (NC3) samarbejder med tredjelande i forbindelse med efterforskningen af cyberkriminalitet. Der er særlige regler i den danske lov om behandling af personoplysninger, som fastsætter regler for overførslen af personoplysninger til tredjelande.

Det er Nationalt Cyber Crime Centers (NC3) erfaring, at Europol er en meget effektiv oplysningskanal på grund af organisationens evne til hurtigt at distribuere relevante oplysninger mellem medlemsstaterne om igangværende efterforskninger. Muligheden for at krydstjekke oplysninger i Europols databaser af at høj værdi for efterforskningerne – også inden for cyberkriminalitet.

Alle ovennævnte punkter blev anvendt i den sag om seksuelt misbrug af børn, som i Danmark er kendt som "Randerssagen", og som omfattede gerningsmænd i Danmark, Sverige og Nederlandene (og uden for EU også Australien).

USA har imidlertid udstationeret en anklager inden for cyberkriminalitet i Eurojust, som uden tvivl vil muliggøre en tæt kontakt til USA, hvis behovet opstår. Det er også muligt at samarbejde med Schweiz og Norge takket være deres samarbejdsaftaler med Eurojust.

7.4 Samarbejdet med den private sektor

– De danske regler om lagring af data forpligter danske udbydere af kommunikationstjenester til at lagre data vedrørende telefonopkald og SMS'er samt abonnentoplysninger i 12 måneder. Endvidere er danske udbydere af kommunikationstjenester i henhold til retsplejeloven forpligtet til at bistå politiet med at foretage lovlige aflytninger og efterkomme retskendelser vedrørende videregivelse af f.eks. abonnentoplysninger.

– Danske hostingfirmaer har pligt til at efterkomme retskendelser vedrørende beslaglæggelse af internetdomæner, og DK Hostmaster, som er ansvarlig for alle .dk-domæner, er forpligtet til at efterkomme retskendelser vedrørende videregivelse af .dk-domæner. Dette giver dansk politi mulighed for at overtage kontrollen over domæner, som anvendes til kriminalitet.

– Hvis en international virksomhed har en lokal filial i Danmark, er denne lokale filial underlagt de danske regler om retlige foranstaltninger såsom ransagninger, beslaglæggelser, aflytninger og videregivelse. Der har været sager, hvor en lokal filial af en international virksomhed har været genstand for sådanne retlige foranstaltninger. Som hovedregel vil alle anmodninger om bistand fra offentlige myndigheder eller private virksomheder i en udenlandsk jurisdiktion blive foretaget inden for rammerne af gensidig retshjælp.

For så vidt angår nogle private tjenesteudbydere som f.eks. Facebook og Google henvises imidlertid til svaret under punkt 7.A.5.

Med hensyn til blokering af adgang bør der også henvises til beskrivelsen af "Netfilter"-aftalen mellem Nationalt Cyber Crime Center (NC3), Red Barnet og de fleste udbydere af kommunikationstjenester. Denne aftale omfatter i øjeblikket kun ulovligt materiale i form af seksuel udnyttelse af børn. NC3 agter dog i samarbejde med Statsanklageren for Særlig Økonomisk og International Kriminalitet at forhandle med udbyderne af kommunikationstjenester om at udvide aftalen til andre former for ulovligt materiale.

Det påhviler internetudbydere at bistå det danske politi med aflytning af kommunikation, herunder aflytning af telefonsamtaler mv. (retsplejelovens § 786). Det påhviler desuden internetudbydere at bistå dansk politi med hastesikring af elektroniske data, herunder trafikdata (retsplejelovens § 786 a).

Nationalt Cyber Crime Center (NC3) deltager i det Europol-ledede samarbejde om efterforskning og forebyggelse af svindel med betalingskort. Finansrådet samarbejder med lignende institutioner i hele Europa, ligesom de fleste større danske banker er tilknyttet en international finansiel institution. Via disse netværk modtager og sender den danske finansielle sektor oplysninger om grænseoverskridende onlinesvindel med betalingskort.

7.5 Internationalt samarbejde – redskaber

7.5.1 Gensidig retshjælp

Det danske politi og den danske anklagemyndighed har generelt et udmærket kendskab til mulighederne for at modtage bistand fra lande uden for EU via gensidig retshjælp.

Det danske politi anfører, at det gør brug af gensidig retshjælp i relevante tilfælde. Når denne procedure anvendes, kræver det, at politiet tillige inddrager den danske anklagemyndighed.

I en sag om et phishingangreb mod de danske banker i 2015 blev det konstateret, at angrebene blev foretaget fra en computer i en anden medlemsstat. Efterforskningen viste dog, at den pågældende computer blev fjernstyret fra en anden computer, som befandt sig i en tredje medlemsstat. Den danske anklagemyndighed indbragte efterfølgende sagen for retten og opnåede de relevante dommerkendelser vedrørende computeren i sidstnævnte land. Der blev sendt en anmodning om gensidig retshjælp til dette land, foreløbig uden resultat.

Danmark modtager også anmodninger om bistand fra tredjelande. Som eksempel kan nævnes en sag fra Midt- og Vestjyllands Politi og Anklagemyndighed. Sagen vedrørte et DOS-angreb på Sea World i Florida, hvor den formodede gerningsmand var en dansk statsborger. FBI anmodede om gensidig retshjælp, og anmodningen blev efterkommet.

7.5.2 Gensidig anerkendelse – instrumenter

Danmark har ikke givet oplysninger om anvendelsen af EU-instrumenter til gensidig anerkendelse i forbindelse med forebyggelse, efterforskning og retsforfølgning af cyberkriminalitet.

Den offentlige anklagemyndighed opstiller ikke tal herfor. Anklagemyndigheden har dog det indtryk, at instrumenterne kun sjældent anvendes, om overhovedet.

Danmark deltager ikke i den europæiske beskyttelsesordre.

7.5.3 Overgivelse/udlevering

Kategorien "internetkriminalitet", som er omhandlet i rammeafgørelsen om den europæiske arrestordre, er ikke defineret i dansk ret. Det er derfor op til de retshåndhævende myndigheder at vurdere, om den pågældende overtrædelse falder ind under denne kategori.

Spørgsmålet om udlevering er fastsat efter lov om udlevering af lovovertrædere, konsolideret lov nr. 833 af 25. august 2005 med senere ændringer (udleveringsloven). Udlevering er ikke betinget af, at der foreligger en aftale. Udlevering er således også mulig, hvis der ikke er indgået nogen udleveringsaftale mellem Danmark og det pågældende land.

Udlevering efter udleveringsloven af ikkedanske statsborgere til lande uden for EU kan ske, hvis lovovertrædelsen efter dansk ret kan straffes med fængsel i mindst et år (udleveringslovens § 2 a). Denne betingelse er opfyldt i sager om cyberkriminalitet, dvs. de handlinger, der er nævnt i tabel 2 i spørgeskemaet fra GENVAL. Hvis udleveringen sker til fuldbyrdelse af en dom, skal personen være blevet idømt fængsel i mindst fire måneder i det land, der anmoder om udlevering, eller vedkommende skal anbringes i anstalt i mindst fire måneder (udleveringslovens § 3, stk. 2).

En dansk statsborger kan udleveres til lande uden for EU, hvis den pågældende i de sidste to år forud for den strafbare handling har haft bopæl i det land, hvortil udlevering ønskes, og en handling, der svarer til den lovovertrædelse, for hvilken der søges udlevering, efter dansk ret kan straffes med fængsel i mindst et år, eller hvis handlingen efter dansk ret kan medføre højere straf end fængsel i fire år (udleveringslovens § 2). Udlevering skal normalt ske på grundlag af en overenskomst med det andet land, men gælder der ikke en sådan overenskomst, kan Rigsadvokaten alligevel træffe beslutning om udlevering af en dansk statsborger på grundlag af de samme betingelser.

Der gælder særlige bestemmelser i EU, for at Danmark kan overholde Rådets rammeafgørelse om den europæiske arrestordre. Bestemmelserne i udleveringsloven vedrørende udlevering fra Danmark til en anden EU-medlemsstat på grundlag af en europæisk arrestordre afviger på flere måder, bl.a.:

- Der stilles ikke krav om dobbelt strafbarhed ved udlevering til strafforfølgning for en lang række lovovertrædelser, der er opført på den såkaldte positivliste, herunder børnepornografi og internetkriminalitet (udleveringsloven § 10 a, nr. 4 og 11).
- Danske statsborgere kan i bund og grund udleveres på samme måde som udlændinge.
- Udlevering kan ikke nægtes på det grundlag, at de pågældende lovovertrædelser har politisk karakter, eller at der ikke er tilstrækkelige beviser til støtte for tiltalen eller dommen for en handling, i forbindelse med hvilken der søges udlevering.
- Udstedelsen af en europæisk arrestordre er i sig selv grundlag for anholdelse og udlevering til strafforfølgning eller afsoning af en dom.
- En europæisk arrestordre skal behandles inden for korte frister, og loven fastsætter frister for behandling af en beslutning om udlevering og for eventuel domstolsprøvelse af denne beslutning.

Endelig gælder der særlige bestemmelser for udlevering til nordiske lande. Udlevering fra Danmark til Finland, Island, Norge og Sverige til strafforfølgning eller afsoning af en dom kan ske på grundlag af den nordiske arrestordre, som trådte i kraft i oktober 2012. De myndigheder, der har kompetence til at udstede og fuldbyrde en nordisk arrestordre, er de lokale anklagemyndigheder. Der findes ikke statistiske oplysninger om brugen af den nordiske arrestordre. Ingen lokal anklagemyndighed har oplyst at have anvendt den nordiske arrestordre i sager om cyberkriminalitet.

Rigsadvokaten træffer beslutning om og fremsætter anmodninger om udlevering i forbindelse med udlevering til og fra EU-medlemsstater og tredjelande (udleveringslovens § 15 og 18 b). Det er dog de retshåndhævende myndigheder, der tager initiativ til at anmode om udlevering eller til at udstede en europæisk arrestordre.

Beslutninger og anmodninger om udlevering til de nordiske lande, dvs. Finland, Island, Norge og Sverige, på grundlag af en nordisk arrestordre træffes af politidirektøren og behandles af den pågældende politikreds (udleveringslovens § 18 h). Hvis en udleveringsanmodning baseret på en nordisk arrestordre og en udleveringsanmodning fra et ikkenordisk land fremsættes samtidig, er det dog Rigsadvokaten, der beslutter, om udleveringen kan finde sted.

Europæiske arrestordrer udstedt af Rigsadvokaten sendes til den relevante politikreds og videresendes direkte til de kompetente myndigheder inden for EU via INTERPOL og – til tredjelande – ligeledes ad diplomatisk vej.

Udleveringssager registreres ikke særskilt efter lovovertrædelsens art. Rigsadvokaten er derfor ikke i stand til at fremlægge statistikker over antallet af sendte/modtagne anmodninger mv. i forbindelse med cyberkriminalitet.

Når Justitsministeriet modtager en udleveringsanmodning, foretager det en foreløbig vurdering af den. Medmindre anmodningen kan afvises uden videre efterforskning, videresender Rigsadvokaten anmodningen til den kompetente politikreds med henblik på yderligere efterforskning, hvilket omfatter afhøring af den eftersøgte person. Når efterforskningen er afsluttet, sender politikredsen resultaterne til Justitsministeriet. På grundlag af udleveringsanmodningen og resultatet af politiets efterforskning beslutter Justitsministeriet, om anmodningen kan efterkommes eller ej.

Udleveringsanmodninger på grundlag af en nordisk arrestordre behandles alene af den relevante politikreds.

Overgivelsen skal som hovedregel finde sted hurtigst muligt. Den person, som er genstand for en udleveringsbeslutning, har ret til at indbringe beslutningen for retten inden for en frist på tre dage (udleveringslovens § 17, 18 e og 18 i). Overgivelsen kan således ikke finde sted inden udløbet af denne frist på tre dage, medmindre den pågældende person har givet afkald på sin ret.

Rigsadvokaten har udsendt retningslinjer for behandling af udleveringsanmodninger. Udleveringsanmodninger skal indeholde oplysninger om tid og sted for den begåede handling, dens beskaffenhed og de anvendelige straffebestemmelser samt oplysninger om, hvorvidt der foreligger en beslutning om anholdelse eller fængsling eller er faldet dom i sagen (udleveringslovens § 11, 18 a og 18 g).

Foreløbig anholdelse i udleveringssager kan finde sted på de samme betingelser som i en dansk straffesag.

7.6 Konklusioner

- **Der er tvivl om Danmarks medlemskab af Europol, og en afklaring haster. Selv om Danmark for nuværende ikke er medlem af J-CAT, bidrager Danmark væsentligt til EC3 og samarbejder med EC3's forskellige arbejdsgrupper (EUCTF, ECTEG & EMPACT m.fl.).**

- **Samarbejdet med NC3 og EC3 er stort set upåklageligt. Alle EC3's operationelle indsatscentre (seksuel udnyttelse af børn, cyberangreb og svindel med betalingskort) meldte om et særdeles godt samarbejde med NC3, og det samme gjorde NC3 selv.**

- **Med hensyn til alle former for grov kriminalitet sætter de lokale myndigheder stor pris på bistanden fra de lokale kontorer og fra Eurojust som sådan, og bistanden betragtes som en væsentlig merværdi.**

- **Danmark anvender MLAT-processen og har oplevet vanskeligheder svarende til dem, som andre lande har oplevet, når de anvender processen til efterforsknings- og bevisformål. Fagfolk på området anvender umiddelbart ikke instrumenterne til gensidig anerkendelse.**

- **Nordsjællands Politi deltager i øjeblikket i et fælles efterforskningshold (JIT) med de spanske myndigheder, hvilket viser, at Danmark er villig til at engagere sig i JIT-processen og samarbejde med sine internationale partnere på retshåndhævelsesområdet i kampen mod cyberkriminalitet.**

8 UDDANNELSE, OPLYSNING OG FOREBYGGELSE

8.1 Specifik uddannelse

Retshåndhævende myndigheder

Der udbydes uddannelse inden for cyberkriminalitet til forskellige målgrupper.

Politiskolen har det overordnede ansvar for udbuddet af uddannelse til det danske politi, mens Rigsadvokaten har ansvaret for kompetenceudvikling hos anklagemyndigheden. Nationalt Cyber Crime Center (NC3) har dog en central rolle, når det gælder udbud af uddannelse inden for cyberkriminalitet til både politiet og anklagemyndigheden. Et tæt samarbejde mellem Rigsadvokaten, Politiskolen, repræsentanter fra politikredsene og NC3 har ført til udviklingen af uddannelsesprogrammet Cybercrime – niveau 1 og 2.

I december 2015 blev **Cybercrime – niveau 1** lanceret. Det er et blandet uddannelsesprogram bestående af syv timers **e-læring** og halvanden dags casebaseret uddannelse. Formålet med programmet er at give medarbejderne en grundlæggende teknisk forståelse af og viden om cyberkriminalitet og sætte dem i stand til at vurdere, hvilke oplysninger der er relevante med henblik på korrekt registrering og håndtering af henvendelser om cyberkriminalitet.

Programmets formål er desuden at sætte medarbejderne i stand til at foretage en indledende vurdering af, hvorvidt et anmeldt tilfælde af cyberkriminalitet udgør en strafbar handling, og om der skal træffes indledende og hastende efterforskningsmæssige foranstaltninger for at sikre digitale beviser.

De emner, der berøres, er:

- cyberkriminalitet og lovgivningen
- digitale genstande og beviser
- netværk og beviser – grundlæggende
- sociale medier og kommunikation
- forebyggelse af cyberkriminalitet
- registrering og håndtering af sager.

Det fulde program er målrettet front-end-medarbejdere i politikredsene, og alle front-end-medarbejdere forventes at gennemføre programmet i løbet af 2016.

Programmets fire e-lærings-moduler giver en grundlæggende indføring i cyberkriminalitet og bliver en obligatorisk del af Politiskolens grundforløb og vil desuden blive udbudt til efterforskere og anklagere generelt i 2016.

Cybercrime – niveau 2, som er målrettet efterforskere og anklagemyndigheden, er under udvikling og vil blive lanceret i oktober 2016. Kurset **Cybercrime 2**, som er målrettet specialister og varer en uge, blev allerede i 2015 udbudt til anklagemyndighedens specialister inden for cyberkriminalitet.

Politiskolen har siden 2007 udbudt et **uddannelsesprogram for IT-efterforskere**, som er målrettet politikredsenes efterforskere med speciale i cyberkriminalitet. Programmet udbydes en til to gange om året afhængig af efterspørgslen. Programmet består af et e-lærings-modul (5 ECTS) og to uddannelsesophold af hver en uges varighed.

NC3 tilbyder ca. en gang om året interne efteruddannelseskurser i IT-kriminaltekniske værktøjer (X-Ways, ENCASE, XRY, Cellbright) for medarbejdere i NC3. NC3 har løbende fokus på kvalitetssikring af IT-kriminaltekniske metoder, rapportering, bevishåndtering osv.

Siden 2010 har Politiskolen og Nationalt Cyber Crime Center (NC3) samarbejdet med norsk og svensk politi om **Nordic Computer Forensic Programme** (30 ECTS), som udbydes af Politihøgskolen i Oslo. Programmet er en blanding af e-læring og uddannelsesophold. Det er et krav, at NC3's nationale IT-kriminaltekniske specialister gennemfører programmet, og programmet har siden 2014 også været udbudt til specialister i politikredsene.
Programmet udbydes to gange om året.

Desuden udbydes specifikke uddannelsesprogrammer inden for seksuel udnyttelse af børn både til efterforskere i politikredsene og til anklagemyndigheden ca. en gang om året.

ECTEG-moduler betragtes generelt som uddannelsesmoduler for specialister og er målrettet nationale specialister, som allerede har gennemført Politihøgskolens NCFI-uddannelse. EGTEC-modulerne udbydes til specialister i NC3, og nogle få har gennemført en fuld masteruddannelse på University College Dublin, som delvist er baseret på ECTEG-moduler. NC3 har også været med til at gennemgå og udvikle ECTEG-modulerne.

Cepol-kurser udbydes via Politiskolen, og kurser, der er relevante i forbindelse med cyberkriminalitet, annonceres over for NC3-medarbejdere og betragtes som suppleringskurser.

Medarbejderne kan på årsbasis deltage i eksterne kurser, seminarer og konferencer i overensstemmelse med deres individuelle kompetenceudviklingsplaner.

Ekspertisecenter. Nationalt Cyber Crime Center (NC3) har en central rolle, både med hensyn til læseplaner, konceptudvikling og uddannelsesudbud inden for cyberkriminalitet og kan sammenlignes med en ekstern afdeling under Politiskolen.

NC3 har i tæt samarbejde med Politiskolen og Rigsadvokaten
udviklet Cybercrime-uddannelsen, som oprindeligt var målrettet politikredsene. NC3 sørger for undervisere til flere andre uddannelsesprogrammer, som udbydes af Politiskolen eller Rigsadvokaten, såsom: IT-efterforskeruddannelsen, uddannelsesprogrammer inden for seksuel udnyttelse af børn, Cybercrime 2 for specialister inden for retsvæsenet og introduktionskurser, som indgår i grundforløbet på uddannelsen til politibetjent.

Dommere og domstole

Det kan bemærkes, at Domstolsstyrelsen siden 2010 har udbudt kurser om forskellige emner til dommere på frivillig basis, herunder kurser i cyberkriminalitet.

Anklagemyndigheden og Nationalt Cyber Crime Center (NC3) overvejer desuden, hvilke af e-læringsmodulerne i "Cyber Crime I" der er relevante for domstolene, og hvorvidt det er teknisk muligt at udbyde disse moduler til dommere. Anklagemyndigheden vil indbyde dommere til kurset "Cyber Crime II", forudsat at dommerne har adgang til og allerede har afsluttet de relevante e-læringsmoduler i "Cyber Crime I", hvilket er det gængse krav for at kunne deltage i "Cyber Crime II".

8.2 Oplysning

Rigspolitiet udsender advarsler om aktuelle trusler om cyberkriminalitet og oplysninger om udviklingen på området på Rigspolitiets officielle Facebook- og Twitter-sider.

Nationalt Cyber Crime Center (NC3) tilbyder forelæsninger om forskellige aspekter af cyberkriminalitet, lovgivning og kriminalitetsforebyggelse på Danmarks Tekniske Universitet.
NC3 gør også hyppigt opmærksom på aktuelle trusler via Facebook og Twitter.

NC3 deltager desuden i relevante TV-programmer for at gøre opmærksom på visse typer cyberkriminalitet såsom sextortion (afpresning ved hjælp af seksuelt materiale) og internetsvindel.

Rigspolitiet har i samarbejde med Københavns Politikreds lanceret et samskabelsesprojekt med talrige private partnere, bl.a. for at skabe opmærksomhed om IT-relateret økonomisk kriminalitet.

8.3 Forebyggelse

8.3.1 Dansk lovgivning/politik og andre foranstaltninger

NC3 lancerede for nylig et initiativ, der skal styrke samarbejdet mellem dansk politi og dansk erhvervsliv. Initiativet er løst baseret på FBI's program Infragard.

Det danske politi arbejder også tæt sammen med NGO'en Red Barnet om forebyggelse af seksuelt misbrug af børn og spredning af materiale, der indeholder denne form for misbrug.

Det danske "Netfilter"-projekt er et eksempel på en forebyggende aktivitet, der involverer såvel det danske politi som de danske serviceudbydere.

8.3.2 Offentlig-private partnerskaber (OPP)

De danske myndigheder understreger, at Nationalt Cyber Crime Center (NC3) har deltaget i offentlig-private partnerskaber, inden begrebet overhovedet fandtes.

Samarbejdet med Red Barnet og internetudbyderne om DNS-blokering af materiale på internettet, hvor børn bliver seksuelt udnyttet, er det ældste eksempel herpå.

NC3 arbejder tæt sammen med Finansrådet og et privat IT-sikkerhedsfirma for at bekæmpe banksvindel mv. NC3 undersøgte for nylig mulighederne for at indgå et samarbejde med et privat kreditoplysningsbureau for at afbøde virkningerne af identitetstyveri ved at udsende "advarsler om svindel" på internettet og således oplyse eventuelle kreditorer og andre om, at en person har været udsat for identitetstyveri. Dette har imidlertid – på grund af de givne forudsætninger – vist sig ikke at være muligt, eftersom samarbejdet ligeledes skulle være åbent for andre private konkurrenter på markedet.

NC3 har endvidere indledt et offentlig-privat partnerskab kaldet "NC3Skyt" med private virksomheder for at ruste samfundet til at forebygge og reagere på udnyttelsen af sikkerhedsmæssige svagheder ved hjælp af fortrolig udveksling af oplysninger mellem deltagerne samt uddannelse af infrastrukturinteressenter. **Initiativet er inspireret af FBI's program Infragard**.

8.4 Konklusioner

- **Den overordnede struktur i de danske oplysnings- og uddannelsesaktiviteter om cyberkriminalitet for fagfolk ved de retshåndhævende myndigheder må betragtes som en særdeles god praksis.**

- **Navnlig er de e-læringsmoduler, som de danske myndigheder har udviklet til politiet og fagfolk ved anklagemyndigheden, en glimrende ramme, som kan være til inspiration for andre medlemsstater. Også på nationalt plan kunne dette materiale udbydes til det danske retsvæsen med henblik på oplysning og uddannelse.**

- **De kompetente danske myndigheder generelt, Center for Cybersikkerhed og navnlig NC3 er godt engageret i offentlig-private partnerskaber.**

- **Andre oplysnings- og forebyggelsesinitiativer synes også at være værdifulde.**

- **Dommere blev i modsætning til andre parter tilbudt uddannelse inden for cyberkriminalitet på frivillig basis. Uddannelse bør kraftigt tilrådes, selv om den ikke er obligatorisk for dommere, som den er for politibetjente og anklagere.**

9 AFSLUTTENDE BEMÆRKNINGER OG ANBEFALINGER

9.1. Forslag fra Danmark

Med hensyn til situationen på nationalt plan har de danske myndigheder konstateret, at der er et større behov for uddannelse af personale i politikredsene, for innovation, både med hensyn til nye teknologier og efterforskningsmæssige foranstaltninger, og for lovgivning. Der er dog fastsat en plan for den videre udvikling, og dele af den er allerede blevet gennemført.

Med hensyn til situationen i Den Europæiske Union finder Rigspolitiet i lyset af de teknologiske fremskridt, navnlig inden for transmission og opbevaring af data samt sikker videregivelse, at den nuværende EU-lovgivning ikke er tilstrækkelig, hvad angår efterforskning og retsforfølgning af cyberkriminalitet. Nogle af de større sager bliver mere og mere komplicerede og kræver derfor højt specialiserede tekniske efterforskningsfærdigheder samt et effektivt og velfungerende internationalt retssamarbejde.

Rigspolitiet støtter således **en strømlining af EU-lovgivningen på følgende områder**:
i) **harmonisering af reguleringen af efterforskningsmæssige foranstaltninger**
ii) **harmonisering af lovgivningen om cyberkriminalitet for at indføre strafferetlige sanktioner på samme niveau** og således sikre håndhævelsen af den gensidige retshjælp, så medlemsstaterne kan efterkomme de fleste anmodninger om gensidig retshjælp på dette område.

De kompetente danske myndigheder anfører, at en forudsætning for at kunne anmode om en bestemt efterforskningsmæssig foranstaltning via gensidig retshjælp meget ofte er **adgang til oplysninger om opbevaring af data** (hvilken IP-adresse var forbundet med hvilken IP-adresse, hvornår, i hvor lang tid, og hvor blev IP-adressen lokaliseret). Hvis disse oplysninger ikke er tilgængelige, ender de fleste efterforskninger her, og de retshåndhævende myndigheder har mere end nogensinde behov for at kunne få adgang til disse oplysninger, **ikke kun nationalt, men også i andre medlemsstater.**

Rigspolitiet mener desuden, at **EU er nødt til at gentænke efterforskningskompetencen, når det gælder søgninger på internettet**. Servernes fysiske placering er irrelevant for brugerne, og vi er nødt til at acceptere cyberspace som et sted for sig, men samtidig som en del af én medlemsstats jurisdiktion i efterforskningsøjemed, men ikke nødvendigvis to eller flere medlemsstaters jurisdiktion.

Gensidig anerkendelse af resultater af søgninger (undersøgelse af servere eller cloud-konti uden at være afhængig af serviceudbyderen) i sager om cyberkriminalitet, som kan foretages fra den stat, der står for efterforskningen, uden teknisk bistand fra den stat, hvor serveren er placeret, vil også give de retshåndhævende myndigheder et meget effektivt redskab og forhindre, at flygtige beviser går tabt.

9.2 Anbefalinger

Med hensyn til den konkrete gennemførelse og anvendelse af rammeafgørelsen og direktiverne var det eksperthold, der deltog i evalueringen af Danmark, tilfredse med det danske system.

Danmark bør følge op på anbefalingerne i denne rapport senest 18 måneder efter evalueringen og rapportere om fremskridtene til Gruppen vedrørende Generelle Anliggender, herunder Evaluering (GENVAL).

Evalueringsholdet fandt det relevant at fremsætte en række forslag for de danske myndigheder. På grundlag af forskellig god praksis fremsættes desuden relaterede anbefalinger til EU og EU's institutioner og agenturer, navnlig Europol.

9.2.1 Anbefalinger til Danmark

1. **Danmark bør overveje at tilpasse sin nuværende statistiske fremgangsmåde på passende vis, så statistikkerne bedre afspejler den aktuelle og fremtidige situation med hensyn til cyberkriminalitet (se også anbefaling nr. 12).**

2. **Danmark bør overveje at forbedre effektiviteten og sammenhængen i sit sagsbehandlingssystem, som ikke blot bør indeholde mistænktes og ofres navne, men også nogle operationelle oplysninger og efterforskningsmæssige spor (f.eks. telefonnumre, IP-adresser, IBAN-numre, DNA-profiler, særlige måder at operere på) og bør på et tidligt tidspunkt gøre det muligt automatisk at finde parallelle sager.**

3. **Danmark bør overveje at indføre realtidsdeling af oplysninger og dele efterretninger med Finansrådet.**

4. **De danske myndigheder opfordres til at tage de nødvendige skridt til at sikre Danmarks fortsatte deltagelse i Europol/EC3-aktiviteter – herunder at overveje at udstationere en fuldtidsmedarbejder hos J-CAT.**

5. **Det undervisningsmateriale, der er udviklet til anklagemyndigheden og NC3, bør gøres tilgængeligt for retsvæsenets administration til uddannelsesformål under fuld hensyntagen til retternes og dommerne uafhængighed.**

6. **Danmark bør blive ved med at fremme en forvaltningspraksis af første klasse for fortsat at tiltrække og fastholde relevante velkvalificerede medarbejdere i de forskellige kompetente tjenester.**

7. De danske myndigheder bør videreføre og udvide udvekslingen af viden, erfaring og værktøjer med Europol/EC3 (f.eks. via SPACE) og andre relevante enheder.

8. Den nuværende situation i Danmark med hensyn til opbevaring af trafikdata kræver, at der findes en hurtig løsning på visse fagfolks manglende retssikkerhed. Danmark bør hurtigt vedtage og gennemføre den nye lovgivning, som er under udarbejdelse.

9.2.2 Anbefalinger til Den Europæiske Union, dens institutioner og andre medlemsstater

9. Den Europæiske Union og dens institutioner bør mere aktivt fremme fastlæggelsen og udbredelsen af medlemsstaternes bedste praksis, herunder redskaber til bekæmpelse af cyberkriminalitet.

10. Med inspiration fra det danske sagsbehandlingssystem (som er fælles for politi og anklagemyndighed) rådes EU og dens institutioner til at overveje, om det ville gavne medlemsstaterne, hvis Eurojust og Europol udvikler et sagsbehandlingssystem, der kan omfatte fælles områder.

11. EU og dens institutioner bør proaktivt fremme brugen af open source-værktøjer og materiale fra medlemsstaternes kompetente myndigheder for at lette videndelingen.

12. Medlemsstaterne bør udvikle hensigtsmæssige statistikker, der korrekt afspejler, hvordan det reelt forholder sig med cyberkriminaliteten. Dette er vigtigt for at kunne kontrollere, hvor virkningsfulde de gældende retlige og efterforskningsmæssige foranstaltninger er, og for at kunne reagere på en hurtigere og mere effektiv måde.

13. **Medlemsstaterne bør undersøge flere områder med god praksis i Danmark, som potentielt kunne blive en inspirationskilde, bl.a.:**
    - **den danske forvaltningstilgang (en langsigtet tilgang, som forsøger at sikre små, gradvise ændringer i processerne for at forbedre effektiviteten og kvaliteten og for regelmæssigt at revidere processen) – hvilket synes at være til stor gavn for de retshåndhævende myndigheder.**
    - **NC3's såkaldte innovationsteam anvender softwareeksperter til at udnytte open source-software og udvikle skræddersyede værktøjer.**
    - **NC3's overordnede ansættelsesmodel omfatter lige mange politiefterforskere og civile IT-ingeniører, hvilket sikrer en optimal blanding af tekniske og efterforskningsmæssige færdigheder til at tackle cyberkriminalitet.**
    - **Et godt eksempel på det aktive løbende samarbejde mellem de forskellige kompetente enheder er, at Center for Cybersikkerhed efter anmodning yder specifik teknisk bistand til NC3-efterforskninger.**
    - **Efterforskningsproceduren "flow", som anvendes i Nordsjællands Politikreds, består af et front-end-kontor (der står for indsamling, dokumentering og sortering af henvendelser fra alle kilder) og et visitationscenter (der gennemgår alle henvendelser og udvælger dem, som skal efterforskes på de lokale politistationer).**

9.2.3 Anbefalinger til Eurojust/Europol/ENISA og andre agenturer/organer

14. **Europol bør overveje mulighederne for at lette udvekslingen af NC3's kriminaltekniske viden og værktøjer med EC3 og de andre medlemsstaters kriminaltekniske enheder.**

15. **Europol bør fremme og lette oprettelsen af en ramme, inden for hvilken medlemsstaternes kompetente myndigheder kan dele eller anvende værktøjer i fællesskab.**

16. Både Cepol og EJTN bør undersøge den e-lærings-strategi, som de danske myndigheder har udviklet, så grundlæggende bevidsthed om og kendskab til cyberkriminalitet kan udbredes til kompetente fagfolk i alle medlemsstaterne.

17. Eurojust bør med støtte fra EC3 på den ene side og JIT-netværket på den anden proaktivt finde frem til egnede sager, hvor et fælles efterforskningshold vil være til gavn på cyberkriminalitetsområdet. Eurojust bør navnlig tilskynde de medlemsstater, som hidtil ikke har anvendt JIT, til at gøre brug af denne proces.

18. ENISA bør overveje, hvordan den CERT-model, som anvendes i Danmark, kan udbredes/udvides.

ANNEX A: PROGRAMME FOR THE ON-SITE VISIT AND PERSONS INTERVIEWED/MET

The Danish Authorities are invited to check and complete the following:

Tuesday 15 March 2016

10.00-11.00 Ministry of Justice – "Welcome and introductory meeting" - *Slotsholmsgade 10, Copenhagen*

13.00-16.00 Director of Public Prosecutions - *Rigsadvokaten, Frederiksholms Kanal 16, Copenhagen*

Wednesday 16 March 2016

9.30-16.00 The Danish National Police, National Cyber Crime Center (NC3)*, Ejby Industrivej 125-135, Glostrup*

Thursday 17 March 2016

9.30-12.00 North Zealand Police - *Prøvestensvej 1, Elsinore*

14.00-16.00 Danish Defence Intelligence Service, Centre for Cyber Security - *Kastellet 30, Copenhagen*

Friday 18 March 2016

9.30-11.00 Ministry of Justice – "Debriefing meeting"

ANNEX B: PERSONS INTERVIEWED/MET

(The Danish Authorities are invited to check and complete the following list of attendees)

Ministry of Justice

Deputy Permanent Secretary Pernille Breinholdt Mikkelsen
Deputy Head of Division Michael de Thurah
Deputy Head of Division Nicolai Winther
Head of Section Michael Schaumburg-Müller
Head of Section Mark Orberg

The Director of Public Prosecutions

Assistant Deputy Director Alessandra Giraldi
Assistant Deputy Director Pernille Langermann

Deputy Chief Prosecutor Karina Nørgaard

Chief of Training and Development Holger Smith
Prosecutor Henriette Reinholdt

The Danish National Police, National Cyber Crime Center

Head of National Cyber Crime Center Kim Aarenstrup
Head of Innovation and Technology Karsten Brinkmann Pedersen

General Counsel Kate Jacquerot

Legal Adviser Jesper Hagen

Superintendent Flemming Kjærside
Superintendent Sonny Olesen

Senior Consultant Susan Varmer

North Zealand Police

Senior Chief Prosecutor Ida Sørensen

Centre for Cyber Security

Head of Policy Department Thomas Kristmar

Chief Legal Advisor Jørgen Breddam
Training and Exercise Peter Knøster

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ACRONYM IN DANISH OR OTHER ORIGINAL LANGUAGE	FULL NAME IN DANISH OR ORIGINAL LANGUAGE	ENGLISH
CEPOL			European Police College
CERT			Computer Emergency Response Team
CFCS			Centre for Cyber Security under the Danish Ministry of Defence
CMS			Case Management System
CoE			Council of Europe
CSA			Child Sexual Exploitation
DDIS			Danish Defence Intelligence Service
DPP		*Rigsadvokaten*	Director of Public Prosecution
ECJ			European Union's Court of Justice
EC3			European Cybercrime Centre
EGTEC			European Cybercrime Training and Education Group
EJN			European Judicial Network
EJTN			European Judicial Training Network
EMPACT			European Multidisciplinary Platform Against Criminal Threats
ENISA			European Union Agency for Network and Information Security
EUCTF			European Union Cybercrime Task Force
EUROJUST			European Unit Judicial Cooperation Unit

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ACRONYM IN DANISH OR OTHER ORIGINAL LANGUAGE	FULL NAME IN DANISH OR ORIGINAL LANGUAGE	ENGLISH
EUROPOL			European Police Office
FBI			United States Federal Bureau of Investigations
GENVAL			Working Party on General Matters including Evaluations
ICSE			Interpol's International Child Sexual Exploitation Database
ICT			Information and Communications Technology
INTERPOL			International Criminal Police Organization
IOCTA			Internet Organised Crime Threat Assessment
IOT			Internet of Things
IP			Internet Protocol
IPR			Intellectual Property Rights
IT			Information Technology
J-CAT			Joint Cybercrime Action Task Force
JIT			Joint Investigation Team
JHA			Justice and Home Affairs
LEA			Law Enforcement Authorities
MLA			Mutual Legal Assistance
MLAT			Mutual Legal Assistance Treaty
MoJ		*Justitsministeriet*	Ministry of Justice
NAW			Nordic Arrest Warrant
NC3		*Nationalt Cyber Crime Center*	Danish National Cybercrime Center
NGO			Non-Governmental Organisation

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ACRONYM IN DANISH OR OTHER ORIGINAL LANGUAGE	FULL NAME IN DANISH OR ORIGINAL LANGUAGE	ENGLISH
PET	PET		Danish Security and Intelligence Service
NOST			National Operating Staff - Danish coordinated multidisciplinary mechanism for serious cyberattacks
PPP			Public Private Partnership
SCADA			Supervisory Control and Data Acquisition
SPACE			EC3's restricted virtual platform
SPOC			Single Point of Contact
TOR			The Onion Router
VPN			Virtual Private Network
VPS			Virtual Private Server