PHISHING SOM IT-KRIMINALITET I DANMARK

Kandidatafhandling i Kriminologi
4. semester, 2019

Gruppe 2:
Lasse Fynbo Jensen
Lotte Cecilie Jensen
Michael Ankerstjerne

Vejleder:
Eva Magdalena Stambøl

Antal ord:
29.271

Abstract

Cybercrime is a phenomenon which has seen an expansive development over the last few years. As a result, phishing has become a crime in Denmark which demands more and more attention from both state and private actors. It is a complicated crime to both investigate and prevent, as phishers are sending thousands of phishing mails within a very short time span. This thesis examines phishing as a phenomenon and the practices around preventing and combating it in Denmark. Through interviews with several experts both from the police and the private sector we have collected extensive information, which is analyzed with Bruno Latour's actor-network theory in order to map the different actors which interact in the network, and through this process uncover the challenges that appear when combating phishing. This thesis uncovers several challenges.

1. Challenges related to police investigation and difficulties in the Danish legislation which is formulated based on the physical world and used on a digital phenomenon. Furthermore, international investigations are time consuming and cooperation with international actors can be difficult.
2. Challenges related to different procedures for reports regarding phishing. The police receive few phishing reports from citizens, and as a result the extent of phishing in Denmark is unknown due to the dark figure of phishing attacks.
3. Challenges related to the nature of cybercrime. Phishers are collaborating and trading information on the dark web. They mostly remain anonymous and use money mules to avoid detection. The difference in the spatial and temporal dimension of the internet compared to the physical world makes it difficult to investigate cybercrime and track down the offender's location.

This thesis also discusses challenges in criminological theory when analyzing cybercrimes like phishing. In applying Michel Callon's translation process on phishing it is uncovered that manipulation plays a significant part in a successful phishing attack. This thesis concludes that more extensive research on phishing in a Danish context is required, as knowledge on the subject is inadequate.

Indholdsfortegnelse

Tro- og loveerklæring

Det erklæres herved på tro og love, at samtlige gruppens medlemmer egenhændigt og selvstændigt har udformet nærværende projekt. Alle citater i teksten er markeret som sådanne, og projektet eller væsentlige dele af det har ikke tidligere været fremlagt i anden bedømmelsessammenhæng.

Vi er bekendt med reglerne for eksamenssnyd, herunder også plagiering og har læst Aalborg Universitets regler på:
https://www.aau.dk/uddannelser/studievejledning/regler/plagiat

Vi er bekendt med, at overtrædelse af reglerne vil blive indberettet for rektoratet og i sidste ende kan ende med bortvisning.
Endelig står vi inde for, at antal ord anført på forsiden stemmer overens med virkeligheden.

1. Indledning

Danmark er som samfund blevet mere digitaliseret, men denne udvikling har også en skyggeside. It-kriminalitet er blevet et fænomen, der fylder mere og mere i samfundet. I takt med teknologiens udvikling har kriminelle også fået flere muligheder for at udføre deres kriminelle handlinger på en ny platform, der ikke kræver, at de forlader deres hjem. Risikoen for at blive udsat for it-kriminalitet er derfor noget, der påvirker mange mennesker, når de dagligt færdes på internettet. Den konstante trussel og tabene forårsaget af it-kriminalitet har fyldt mediebilledet de seneste år. Nogle af overskrifterne i de danske nyheder lyder således:

- *Paraderne op: Her prøver it-kriminelle at snyde dig nu* (Berlingske, 2018)
- *DR: Tillidsfulde danskere snydes af it-kriminelle* (Nørgaard, 2018)
- *Plastvirksomhed udsat for it-kriminalitet: Snydt for tocifret millionbeløb* (Lindsø, 2019)
- *De kriminelle er blevet mere digitale* (Dansk Erhverv, 2018)

It-kriminalitet er derfor ikke længere blot et fænomen, der har stor nyhedsværdi i medierne, men det er også et emne, flere forskere er begyndt at beskæftige sig med. Kriminalitetsniveauet blandt unge er på det laveste nogensinde, og en af forklaringerne på dette bliver fremhævet som ændret livsstil, hvor unge bruger mindre tid på gaden og mere tid på cyberspace. Derfor har unges liv på cyberspace ifølge flere eksperter en stor betydning for den faldende ungdomskriminalitet. Det betyder dog ikke, at kriminaliteten er forsvundet, men at den stigende aktivitet på internettet betyder, at også den kriminelle aktivitet foregår et andet sted.

Samfundet og borgernes dagligdagsrutiner er i høj grad præget af teknologien, og det samme er de kriminelles handlemønstre. Det er derfor interessant yderligere at undersøge, hvordan teknologien og samfundet i samspil påvirker hinanden, og hvordan dette har betydning for kriminaliteten og hele det kriminologiske forskningsfelt. It-kriminalitet som fænomen kræver, at kriminologer tager stilling til, hvordan cyberspaces dynamiske tid-rum-konstellation påvirker kriminelles adfærd, motivation og muligheder.

2. Problemfelt

I følgende afsnit gennemgås nogle af de udfordringer, der er forbundet med efterforskning og analyse af it-kriminalitet som fænomen. Herunder hvordan det kan være svært at definere og lovgive på området. Derudover inddrages phishing som en it-kriminalitetsform, der kan illustrere nogle af de typiske udfordringer ved bekæmpelse af it-kriminalitet.

2.1 Problemer med at definere it-kriminalitet

It-kriminalitet er stadigvæk et relativt nyt fænomen, og derfor eksisterer der endnu ikke en fastlagt definition på, hvad it-kriminalitet er. Begrebet, og dermed også forståelsen af fænomenet, har ændret sig gennem tiden (Holt og Bossler, 2016, s. 6). I 1970'erne blev begrebet *computer crime* anvendt som udtryk for it-kriminalitet, og det var i samme årti, USA formulerede en af de første love mod computerkriminalitet. Terminologien omkring computerrelateret kriminalitet skiftede i 1990'erne, da det blev mere almindeligt at have adgang til en computer og internettet. Forskere begyndte nu at referere til kriminalitet begået online som *cybercrime*. Dette begreb blev i starten af årtusindskiftet udvidet til at referere til al teknologi-genereret kriminalitet (Holt og Bossler, 2016, s. 6). Thomas og Loader (2000, s. 2) pointerer dog vigtigheden i at skelne mellem it-kriminalitet og kriminalitet begået med teknologi, da kriminelle altid har brugt en form for teknologi. It-kriminalitet er ifølge dem en helt anden kaliber, og det indebærer derfor kun kriminalitet, som ikke ville have været mulig at begå uden internettet. Wall (2001, s. 2) forklarer derimod, at begrebet cybercrime ikke klarlægger meget andet end skadende adfærd, der på en måde er relateret til en computer. Som Holt og Bossler (2016, s. 6-7) fastslår, er efterhånden alle teknologiske enheder (såsom musikafspillere og mobiltelefoner) forbundet til internettet, og Walls (2001) fokus på computeren er derfor ikke længere fyldestgørende.

Den historiske udvikling af begrebet cybercrime eller it-kriminalitet viser tydeligt, at der er uenigheder om, hvad definitionen skal inkludere, og hvad den skal afgrænses fra. Yar (2005, s. 409) forklarer, hvordan fraværet af en klar definition af it-kriminalitet er en af de store problemer, når fænomenet skal analyseres. Grabosky (2016, s. 2) anvender i nyere tid

en bredt dækkende definition af it-kriminalitet, som inkluderer kriminelle handlinger, der enten kan være internet- eller computerbaserede:

"*(…) cybercrime refers to criminal activities involving the networked environment based on the Internet and/or World Wide Web. But we will use it to refer to offences involving stand-alone computers as well.*"

I en dansk kontekst præsenterer Det Kriminalpræventive Råd (2019a) også en bred definition af it-kriminalitet, som de inddeler i tre kategorier:

"Computer-integritetsforbrydelser
Disse forbrydelser går ud på at skade en persons eller virksomheds it-system. Det er forbrydelser, der angriber computeren. Fx hacking, distribuering af malware, fx vira, orme og trojanske heste eller såkaldte DDoS-angreb, der går ud på at overbelaste en internetside.

Computer-assisterede forbrydelser
Disse forbrydelser har ofte et økonomisk sigte. Det er kendte kriminalitetsformer som tyveri og bedrageri, der begås ved hjælp af internetteknologi. Det er fx Nigeriabreve, phising [sic] eller indbrud i en netbank.

Computer-indholdsforbrydelser
Forbrydelserne handler om at besidde eller dele kriminelt materiale. Det kan være ulovligt indhold i filer, beskeder eller andre informationer, der sendes ud på internettet. Det er fx børnepornografisk, racistisk eller voldeligt materiale."

Det Kriminalpræventive Råd (2019a) definerer it-kriminalitet som noget, der enten kan være angreb mod computere, angreb med computere eller besiddelse og deling af ulovligt indhold på computeren. Selvom de tre kategorier alle indeholder ordet *computer*, har de også fokus på skader forårsaget af ulovlig internetbrug. Definitionerne forekommer derfor mere betingede af brugerens anvendelse af internettet, og ikke hvorvidt den ulovlige aktivitet er foregået ved hjælp af en computer eller anden teknologi.

Clough (2010, s. 10) præsenterer også en tredeling af it-kriminalitet som begreb:

"1. Crimes in which the computer or computer network is the target of the criminal activity. For example, hacking, malware and DoS attacks.

2. Existing offences where the computer is a tool used to commit the crime. For example, child pornography, stalking, criminal copyright infringement and fraud.

3. Crimes in which the use of the computer is an incidental aspect of the commission of the crime but may afford evidence of the crime. For example, addresses found in the computer of a murder suspect, or phone records of conversations between offender and victim before a homicide. In such cases the computer is not significantly implicated in the commission of the offence, but is more a repository for evidence."

Det er også en opdeling af begrebet, som er internationalt anerkendt og anvendt i mange lande (Clough, 2010, s. 10). Generelt er der altså en skelnen mellem, om kriminaliteten er foregået som angreb mod en computer, eller om computeren fungerer som mellemled eller facilitator i en anden kriminel handling. Der er også uenighed om, hvorvidt it-kriminalitet kan defineres som noget, der blot involverer en computer, eller om brugen af internettet er afgørende for, at noget kan klassificeres som it-kriminalitet.

I dette speciale anvendes begreberne it-kriminalitet og cyberkriminalitet synonymt for alle typer af kriminalitet, der foregår ved brug af internettet, uanset om der er tale om angreb mod en computer, eller om computeren er facilitator for kriminaliteten. For specialet er det ikke væsentligt, om kriminaliteten er faciliteret af en computer, en mobiltelefon eller andre genstande med internetforbindelse, men det vigtige er, at internettet har spillet en afgørende rolle i udførelsen af kriminaliteten.

2.2 Gammel vin på nye flasker

It-kriminalitet er blevet et fænomen, der berører mange mennesker i dagligdagen. Det kommer blandt andet til udtryk ved, at der udgives håndbøger om, hvordan privatpersoner sikrer sig mod trusler på internettet. Waschke (2017) introducerer eksempelvis de mest almindelige it-trusler mod computerbrugere og forklarer, at almindelig antivirus ikke længere er nok for at sikre brugere mod at blive udsat for cyberangreb. It-kriminalitet er

stadig et forholdsvist nyt forskningsfelt inden for kriminologien, og derfor beskæftiger mange forskere sig med, hvilke teoretiske tilgange det er muligt at anvende i forhold til it-kriminalitet.

Grabosky (2001) er en af de forskere, som er tilhænger af at anvende traditionel kriminologisk teori på it-kriminalitet. Han mener, at it-kriminalitet har samme egenskaber som den mere traditionelle kriminalitet, men at mediet, hvorpå kriminalitet begås, er nyt, og at den bagvedliggende motivation for at begå kriminalitet hovedsageligt er den samme som i de traditionelle former for kriminalitet. Han kalder derfor it-kriminalitet for *gammel vin på nye flasker*. Grabosky (2001, s. 244, 2016, s. 57) medgiver, at der er opstået nye former for kriminalitet, herunder eksempelvis hacking som ikke fandtes før i tiden, men at størstedelen af it-kriminalitet er ældre former for kriminalitet, som er blevet transformeret af den teknologiske udvikling. Forfatteren mener dermed, at klassiske kriminologiske teorier har god forklaringskraft på it-kriminalitet. Grabosky (2016, s. 57) anvender eksempelvis *rutineaktivitetsteorien* direkte på it-kriminalitet, da han mener, at motivationen for at begå kriminalitet online er den samme som for den traditionelle kriminalitet. Det er derfor hans pointe, at de kriminalitetsformer (bedrageri, afpresning og trusler), som har eksisteret i mange år, nu udspiller sig på internettet. En anden forsker, som til dels tilslutter sig denne forklaring, er Jaishankar (2008a). Han argumenterer for, at mange klassiske kriminalitetstyper såsom tyveri og stalking kan udøves på cyberspace, hvor gerningsmanden har mulighed for større udbytte af sin kriminalitet, samtidig med at det ofte er nemmere ikke at blive opdaget og straffet for sin gerning.

Som reaktion på Graboskys (2001) *gammel vin på nye flasker* undersøger Yar (2005), om it-kriminalitet kan kategoriseres som en gammel kriminalitetstype på en ny platform, hvor traditionelle kriminologiske teorier kan anvendes som analyseredskab. Han gennemgår også it-kriminalitet med udgangspunkt i rutineaktivitetsteorien, men hans konklusion er, at teoriens fundament, der bygger på tre forudsætninger for kriminalitet (motiveret gerningsmand, egnet offer og mangel på beskyttere), som er tilstedeværende i samme fysiske rum, er svært at overføre til cyberspace. Ifølge Yar (2005, s. 414-415) har cyberspace en ustabil og dynamisk sammensætning, og derfor er det vanskeligt at overføre en teori baseret på en stabil tid-rum-sammensætning. Han mener derfor ikke, man bør tale om

gammel vin på nye flasker, men derimod *gammel vin på ingen flasker*, fordi der ikke er den rumlige dimension.

Der er altså uenighed om, hvilken forklaringskraft klassiske kriminologiske teorier har på cyberkriminalitet. Denne uenighed vidner om et komplekst felt, hvor der ikke findes et simpelt svar på problemstillingen. It-kriminalitet er desuden et bredt fænomen, som dækker over en række specifikke kriminalitetsformer heriblandt phishing. Phishing er en af de metoder, it-kriminelle ofte anvender til at snyde deres ofre. I år 2018 havde mere end 50 % af de danske borgere ifølge Digitaliseringsstyrelsen og DKCERT (2018, s. 35) oplevet forsøg på phishing. Det er en kriminalitetsform, der har eksisteret i mange år og som kommer i bølger, og det er derfor en trussel, der bør tages alvorligt (Digitaliseringsstyrelsen og DKCERT, 2018, s. 56). Phishing anvendes i dette speciale som den type it-kriminalitet, der er særligt i fokus.

2.3 Phishing som it-kriminalitet

Phishing anvendes af gerningsmænd med det formål at franarre brugere penge eller personfølsomme oplysninger. Det Kriminalpræventive Råd definerer begrebet:

"Phishing er en metode, hvor svindlere forsøger at narre internetbrugere til at oplyse brugernavn, adgangskode, kreditkort- eller netbanksoplysninger med videre. Brugeren får tilsendt en e-mail, hvor afsenderen tilsyneladende er en virksomhed, som man generelt har tillid til, eksempelvis ens bank, SKAT, en fragtvirksomhed eller lignende. I mailen opfordres modtageren til at indsende oplysningerne per e-mail eller logge ind på en falsk internetside, der til forveksling ligner bankens eller SKATs rigtige hjemmeside." (Kruize, 2018, s. 5).

Før phishingangrebet bliver succesfuldt, er gerningsmændene derfor nødt til at formulere en mail og eventuelt programmere en hjemmeside, der virker troværdig nok til, at brugeren indtaster de ønskede oplysninger. De it-kriminelle kan efterfølgende enten bruge oplysningerne til identitetstyveri, eller de kan misbruge offerets kreditkortoplysninger. Der anvendes primært to metoder til phishing: *malware* og *social engineering*. Ved et malware-angreb installeres skadelige filer på offerets computer, hvis vedkommende klikker på et

link eller åbner en vedhæftet fil. Hvis gerningsmanden gør brug af social engineering, er det manipulation og offerets manglende evne til at verificere en hjemmeside, der udnyttes. Social engineering er en samlet betegnelse over teknikker, som benyttes af kriminelle til at narre personer gennem social interaktion. De kriminelle kan altså både anvende teknologiske og psykologiske virkemidler i phishingangreb (Gupta, Tewari, Jain og Agrawal, 2017, s. 3629-3630). En phishingmail behøver ikke at indeholde et link til en hjemmeside, men kan også være et forsøg på at overtale offeret til at besvare mailen med personfølsomme oplysninger.

Med udgangspunkt i definitionen af it-kriminalitet illustrerer phishing som eksempel, hvordan internettet kan muliggøre forskellige former for bedrageri på en ny platform, der kan være attraktiv for potentielle gerningsmænd.

2.4 It-gerningsmænd

Cirka 80 % af alt internetkriminalitet er organiseret, hvor motivationen primært er økonomisk gevinst. For de resterende 20 % kan motivationen variere og være eksempelvis personlige eller teknologiske udfordringer. Organiseret phishing kan sammenlignes med almindelige virksomheder med klare mål for deres profit (Konradt, Schilling og Werners, 2016, s. 40). I rapporten *Kriminalitet i en digitaliseret verden* undersøger Peter Kruize (2013) gerningspersoner sigtet for forskellige it-kriminalitetstyper i Danmark. Der skal dog tages forbehold for, at offerundersøgelsen viste, at kun omkring 20 % af respondenterne anmeldte it-kriminalitet til politiet, og derfor indeholder statistikken om de sigtede også en vis usikkerhed, i forhold til hvor repræsentativ den er. Han nævner, at det typisk kan være de mindre professionelle og mindre organiserede, der ender med at blive sigtet. I årene 2010-2012 sigtedes 59 unikke personer i Danmark for misbrug af identitetsoplysninger. Disse kan blandt andet være indhentet ved hjælp af phishing (Kruize, 2013, s. 47). Langt størstedelen af it-kriminalitet begås ifølge statistikken af mænd i alderen 15 til 44 år. Derudover havde 36 af de sigtede tidligere domme, og derfor var der en recidivprocent på 61, hvoraf cirka halvdelen tidligere var dømt for ligeartet kriminalitet (Kruize, 2013, s. 48). Det viser, at størstedelen af dem tidligere har været straffet og derfor allerede er på en kriminel løbebane. Det er interessant ifølge Jaishankars (2008a, s. 5-6) *space transition theory*, som forklarer, at it-kriminelle kan have tendens til at flytte deres

kriminelle aktivitet til den fysiske verden - og de analoge kriminelle kan flytte noget af deres kriminelle aktivitet til cyberspace.

Antallet af sigtelser for denne type sager i Danmark er relativt lavt, og der er hverken på globalt eller nationalt plan meget viden om, hvem den typiske gerningsmand er. Det er derfor vanskeligt at danne sig et klart billede af, om disse personers kriminelle løbebane er opstået på grund af internettets muligheder, eller om mulighederne blot udnyttes i en i forvejen kriminel livsstil. Der er et overlap mellem analog kriminalitet og it-kriminalitet, da dele af den traditionelle kriminalitet kan gøres lettere på internettet - eksempelvis deling af børneporno eller udveksling af pengesummer gennem bitcoins. Jaishankars (2008a, s. 5-6) teori beskriver dog, at internettet kan virke attraktivt for personer med undertrykt kriminel adfærd, som ellers ikke nødvendigvis havde været kriminelle. Overordnet set arbejder it-kriminelle ofte organiseret og har økonomiske motiver, men ellers er det vanskeligt at vide, "hvem" man helt præcist taler om, når det handler om it-gerningsmænd. Det virker umiddelbart til, at det eneste, phishinggerningsmænd helt sikkert har tilfælles, er, at de har lavet phishing.

2.5 Kriminalitetsgenererende faktorer i cyberspace

Flere forskere har undersøgt, hvad der virker motiverende og tillokkende ved at begå kriminalitet online, og om der er forskel på motivationsfaktorerne i forhold til traditionel kriminalitet. Bedrageri har eksisteret som kriminalitetsform i mange år, men med opfindelsen af internettet er der en ny oplagt platform at bedrage på. Phishing som bedrageriform kan på flere måder minde om traditionelle bedragerisager, men forskellen er, at internettet nu faciliterer kontakten mellem gerningsmand og offer.

Ligesom phishing har mange andre it-kriminalitetsformer eksisteret, før internettet blev opfundet - herunder eksempelvis stalking, chikane og seksuelle krænkelser af børn. I takt med internettets fremgang er det dog blevet lettere og mere tilgængeligt for gerningsmænd at begå kriminelle handlinger (Aas, 2007, s. 159). Det er derfor relevant at problematisere internettets kriminalitetsgenererende faktorer.

Vendius (2015, s. 21) forklarer, at der er sket en stigning i antallet af sager om seksuelle krænkelser og misbrug af børn efter internettets fremkomst, da den traditionelle børnelokker er rykket væk fra gaden og ind bag en computerskærm. Internettet er en god platform til at sælge børnepornografi i store mængder, og det er svært for politiet at tackle denne udfordring, da de kriminelle sætter nye standarder og er innovative i deres kriminelle aktivitet. Phishing er i den forbindelse også en traditionel kriminalitetsform, der er mulig at udføre i meget større skala på internettet, da det er en mindre tidsinvestering at sende 1000 mails end at sende 1000 breve. Internettet gør det også sværere for politiet at finde frem til gerningsmanden, som kan udføre sin kriminelle handlinger fra et helt andet land.

En anden kriminalitetsgenererende faktor kan ifølge Grabosky (2016, s. 57) være, at den virtuelle verden indebærer et stort element af anonymitet og uvirkelighed, som kan distancere den kriminelle fra sine handlinger. Demetriou og Silke (2003) har i den forbindelse undersøgt, hvor mange af brugerne på en lovlig hjemmeside der ville tilgå ulovligt materiale på siden, hvis de fik mulighed for det. Størstedelen af de besøgende valgte at tilgå ulovligt piratkopieret materiale. Kombinationen af anonymitet på internettet og let tilgang til ulovligt materiale kan have en kriminalitetsgenererende effekt på mange, selvom det ikke var deres hensigt at opsøge ulovligt materiale. Jaishankar (2008a, s. 7) beskriver ligeledes, at anonymitet er en vigtig faktor for, at cyberspace er et oplagt sted at begå kriminalitet. Personer med en undertrykt tilbøjelighed til kriminalitet kan vælge at begå it-kriminalitet, da de ikke føler, det potentielt kan skade deres status og position i den fysiske verden. Ydermere er manglen på afskrækkende faktorer vigtig, da den opfattede risiko ved kriminalitet på internettet ofte er meget lav, mens fortjenesten opfattes som stor.

Anonymitetsfaktoren på internettet kan påvirke folk til at opføre sig mere ondskabsfuldt, end de ville ansigt til ansigt. Anonymiteten gør det lettere for folk at gå imod de gængse sociale normer, da de ikke er bekymrede for, at de bliver holdt ansvarlige for deres handlinger. De er mere tilbøjelige til at opføre sig destruktivt, fordi de ikke er bange for sanktioner, når de er anonyme. Når der ikke er sociale pejlemærker som eksempelvis ansigtsudtryk, kan folk også have tendens til destruktiv adfærd. Citron (2016, s. 57-59) erkender dog, at anonymiteten på internettet kan være en positiv ting, da det kan hjælpe

folk med at italesætte svære situationer i deres liv. Der skal derfor både overvejes fordele og ulemper angående anonymitet på internettet.

Der er altså forskellige faktorer, som kan virke kriminalitetsgenererende online. Forskningen berører især emner vedrørende anonymitet og det ikke at blive stillet til ansvar for sine kriminelle handlinger. Manglen på straf for it-kriminalitet viser også nogle af de udfordringer, som eksisterer i forhold til efterforskning og retsforfølgelse af it-kriminelle.

2.6 Lovgivning og efterforskning af it-kriminalitet

En af de store udfordringer ved bekæmpelse af it-kriminalitet er efterforskningen og lovgivningen på området. It-kriminalitet er svært og ressourcekrævende at efterforske, og lovgivningen er ofte mangelfuld eller tvetydig. Kriminalitetens transnationale natur gør det også problematisk at straffe forbrydere, da forbrydelsen ofte foregår på tværs af jurisdiktioner med forskellige love. Ifølge Grabosky (2016, s. 6) er en af udfordringerne, at teknologien altid udvikler sig hurtigere end lovgivningen. Derudover er der ofte tale om gråzoner, da lovgivningen skal være med til at stoppe den uhensigtsmæssige adfærd på nettet, men den skal ikke bremse den teknologiske udvikling.

Traditionel kriminalitet foregår som regel på en lokation, hvor både offer og gerningsmand er til stede, og derfor er jurisdiktionsspørgsmålet nemmere at afgøre. Ved et phishingangreb kan bare det at finde lokationen være udfordrende (Grabosky, 2016, s. 103-104). Yderligere kan det være svært at afgøre jurisdiktionen, hvis hackeren benytter servere i mange forskellige lande, mens vedkommende selv befinder sig i et andet land og offeret i et helt tredje. Det er en dyr og langsommelig proces at afgøre jurisdiktionsspørgsmålet, og det kan betyde, at mindre it-kriminalitetssager nedprioriteres. Det kan udnyttes af nogle kriminelle som en strategi for at undgå retsforfølgelse.

Brown (2015, s. 98-100) problematiserer, at der eksisterer en lang række barrierer, som begrænser efterforskning og retsforfølgelse af it-kriminelle. Han fremhæver eksempelvis:

- Udfordringer med at identificere gerningsmanden
- Udfordringer med at få adgang til og indhente bevismateriale

- Udfordringer med tid og ressourcer til uddannelse af efterforskere
- Udfordringer med det juridiske personales teknologiske indsigt eller ekspertise i it-kriminalitet
- Udfordringer med lovgivningen

Der mangler altså opkvalificering på disse punkter i forhold til it-kriminalitet, så retssystemet udvikler sig i takt med teknologien. Shipley og Bowker (2014, s. 379) pointerer i denne forbindelse, at det kan have konsekvenser, hvis mange it-kriminelle ikke retsforfølges. De anvender *broken windows*-teorien og forklarer, at mange småforseelser kan bane vejen for mere alvorlige former for it-kriminalitet. Et enkelt vellykket forsøg på phishing, som ikke har konsekvenser for gerningsmanden, kan betyde, at vedkommende fortsætter sin kriminalitet. Den manglende konsekvens kan yderligere sende et signal til samfundet om, at det ikke er en kriminalitetsform, der prioriteres og tages alvorligt af myndighederne. Foruden problemer med at retsforfølge den kriminelle er det ofte en udfordring at efterforske og opklare it-kriminalitet.

Den klassiske tilgang til kriminalitetsefterforskning med sikring af spor, afhøring af vidner og så videre er nærmest ikke-eksisterende, når der er tale om it-kriminalitet. Der er ikke fingeraftryk, DNA eller et reelt gerningssted. Derudover har it-kriminelle sjældent tidligere kriminalitet på deres straffeattest, og de har sjældent en kriminel omgangskreds. Dette går imod Kruizes (2013) undersøgelse, som viste, at it-kriminelle havde en recidivprocent på 61. Traditionel kriminalitet er ofte af personlig karakter mellem offer og gerningsmand. Ved it-kriminalitet kender de typisk ikke hinanden, og der kan gå lang tid fra hændelsen, til offeret opdager, at der er sket noget kriminelt. Som Waschke (2017, s. 162) udtrykker det: *"Cybercrimes are local, cybercriminals are global."*.

Desuden er der uddannet få it-efterforskere, og de er nødt til at koncentrere sig om de største sager. Samtidig er det en efterforskning, der er meget tidskrævende. Et af problemerne derfor, at det lokale politi ofte ikke har viden og ressourcer til at bekæmpe små it-kriminalitetssager, som kan vokse sig store med tiden (Waschke, 2017, s. 73). I de fleste lande er politiets statistik på området ligeledes mangelfuld. Det er ikke i alle lande,

der findes tal på it-kriminalitet, da sagerne blot registreres som eksempelvis "bedrageri", uden at der tages højde for gerningsmandens metode (Grabosky, 2016, s. 61).

2.7 It-kriminalitetens mørketal

Et af problemerne med bekæmpelse af it-kriminalitet er manglende ressourcer på området, hvilket kan være et resultat af den lave anmeldelsestilbøjelighed, som betyder, at der ikke allokeres passende ressourcer til at uddanne efterforskere. Den lave anmeldelsestilbøjelighed resulterer i et højt mørketal, og statistikkerne er derfor ikke retvisende, i forhold til hvor meget it-kriminalitet der reelt begås. En af udfordringerne er, at nogle kriminalitetsformer som eksempelvis piratkopiering og hæleri sjældent har et direkte offer, og derfor indfanges disse kriminalitetstyper hverken i offerundersøgelser eller anmeldelsestallene (Det Kriminalpræventive Råd, 2019b). Grabosky (2016, s. 61) pointerer, at det store mørketal gør det svært at overskue, hvilke it-kriminalitetsformer der har faldende og stigende tendenser. It-kriminalitet sker i de fleste tilfælde i høj volumen, men lav value. Det vil sige, at den enkeltes tab ofte ikke er omfattende, men i det store billede er it-kriminalitet dyrt for samfundet. Nogle af grundene til, at it-kriminalitet ikke anmeldes, kan ifølge Grabosky (2016, s. 61-62) og Waschke (2017, s. 169-171) være:

- At borgeren ikke opdager, at vedkommende har været udsat for kriminalitet
- At borgeren ikke tror, politiet tager det alvorligt
- At offeret er ligeglad
- At offeret er flovt over at være hoppet på et fupnummer
- At virksomheden ikke ønsker dårligt omdømme i forhold til deres sikkerhed

Mørketallet for it-kriminalitet kan således kun reduceres, hvis ofre i højere grad begynder at rapportere hændelserne, så der registreres et realistisk tal på, hvor mange der udsættes for det. Det er også en nødvendighed for, at der prioriteres flere ressourcer til området, så politiet får bedre forudsætninger for at bekæmpe kriminaliteten (Waschke, 2017, s. 169-171).

I Danmark spiller it-kriminalitet også en stor rolle, og Kruize (2009, 2013) har undersøgt fænomenet identitetstyveri i en dansk kontekst. Kruize (2009, 2013) nævner phishing som den mest anvendte metode til tilegnelse af personoplysninger på internettet.

Digitaliseringsstyrelsen og DKCERTs (2018) undersøgelse viser, at danskerne generelt er gode til at genkende og undgå phishing, men i 2017 registrerede Finans Danmark 792 forsøg på phishing rettet mod kundernes netbank, hvoraf 341 lykkedes og medførte økonomisk tab. Det samlede tab på grund af phishing blev i 2017 anført til 5.694.756 kroner (Digitaliseringsstyrelsen og DKCERT, 2018, s. 46; Finans Danmark, 2019). Der ses også en markant stigning af anmeldelser i Politiets statistik for databedrageri, som phishing kategoriseres under:

År	2014	2015	2016	2017	2018
Antal anmeldelser	5.628	15.399	19.321	21.939	20.517

Tabel 1: Anmeldelser af databedrageri (§279a) år 2014-2018 (Politi, 2019).

Tabellen viser en voldsom stigning i antallet af anmeldelser for databedrageri fra 2014 til 2018. En del af forklaringen på den store stigning fra 2014 til 2015 skyldes, at tyveri fra pengeautomater efter 2014 registreres som databedrageri. På trods af den relativt store forekomst af phishing i Danmark er emnet forholdsvist uudforsket i en dansk kontekst. Det er derfor interessant at undersøge, hvilke udfordringer der er ved at bekæmpe phishing i Danmark.

3. Problemformulering og formål

3.1 Specialets formål

Projektets formål er at undersøge, hvordan phishing bekæmpes i en dansk kontekst, og hvilke udfordringer der i den forbindelse opstår. Udfordringerne ved at bekæmpe phishing er ikke tidligere undersøgt i Danmark. Specialet tager udgangspunkt i danske eksperters indsigt i udfordringer relateret til bekæmpelse af phishing og suppleres med forskning fra andre lande. På den måde er det muligt at undersøge, om det er de samme udfordringer, som gør sig gældende i Danmark.

3.2 Problemformulering

Hvilke udfordringer er der ved at bekæmpe phishing som it-kriminalitet i et dansk efterforskningsnetværk?

4. Litteraturstudie

It-kriminalitet er et komplekst problem, som er blevet et større fokus i den globale verden. Det øgede fokus på informationsteknologier og digitalisering af samfundet betyder, at der er brug for en øget forståelse af it-kriminalitet og dens kompleksitet. Med udgangspunkt i den gældende problemstilling undersøger nedenstående litteraturstudie, hvilken forskning der findes på området, og hvilke problematikker der tidligere er afdækket om phishing.

4.1 Phishing som fænomen i litteraturen

Flere forskere har forsøgt at afdække phishing som fænomen. Phishing dækker over flere forskellige typer af angreb mod informationsteknologien, og udtrykket blev for første gang brugt i 1996. Gupta et al. (2017) kortlægger phishingfænomenets historiske udvikling fra 1996 til 2015. Selvom kriminaliteten har fundet sted i over 20 år, er det stadigvæk ikke lykkedes at finde en passende løsning, da gerningsmændene blot finder en ny svaghed og derefter fortsætter deres angreb. I artiklen diskuterer de en række tiltag mod phishing, og hvilke fordele og ulemper de hver især har. Foruden teknologiske tiltag mod phishing mener de, at det også er vigtigt at informere brugerne og give dem viden om phishing som trussel, før antallet af succesfulde angreb kan nedbringes. Flere forskere har prøvet at undersøge de økonomiske konsekvenser ved phishingangreb, som ifølge Konradt et al. (2016) er af særlig interesse på grund af de negative effekter, de har på verdensøkonomien. Konradt et al. (2016) giver et indblik i gerningsmændenes adfærd og økonomiske motiver og muliggør en beregning af indsatsernes effektivitet til at bekæmpe phishing. Samtidig argumenterer forfatterne for, at bedre kontrol af sorte markeder er en mere effektiv indsats til at forhindre kriminalitet end at øge straffen for at begå kriminaliteten. De belyser, hvordan it-kriminelle handler med hinanden på det sorte marked for at tjene penge på phishing. På disse sorte markeder bliver der blandt andet handlet med personfølsomme oplysninger, som er blevet fremskaffet ved identitetstyveri. Jaishankar (2008b) pointerer, at identitetsrelateret it-kriminalitet er i fremgang, og at phishing ofte anvendes til identitetstyveri. Han mener derfor, der er brug for en dybdegående analyse af typiske ofre for phishing. Flere forskere har sidenhen fulgt Jaishankars (2008b) opfordring til mere forskning på området.

4.2 Forskning i gerningsmænd og ofre for phishing

Leukfeldt (2014) undersøger med udgangspunkt i rutineaktivitetetsteorien, om der er bestemte faktorer, som øger eller mindsker risikoen for at blive offer for phishing. Han antager, at visse faktorer såsom øget synlighed på nettet, et stort økonomisk overskud, internetaktiviteter og brugen af populær software vil lede til øget phishingviktimisering. Han finder frem til, at økonomiske og personlige karakteristika ikke har nogen effekt på, om man bliver offer for phishing. Kun en ud af otte internetaktiviteter havde en effekt på risikoen for at blive et offer for phishing, og brugen af populær software leder heller ikke til øget viktimisering. Leukfeldt (2014) konkluderer som afslutning på sin kvantitative analyse, at it-kriminelle, som tjener penge på phishing, ikke går efter en bestemt målgruppe, men at de prøver at ramme alle. Leukfeldt og Jansen (2016) undersøger denne problematik yderligere med en kvalitativ tilgang for at klargøre, hvem der bliver offer for phishing. Det forsøges afdækket i 30 interviews, som også analyseres med udgangspunkt i rutineaktivitetsteorien. Forfatterne konkluderer, at rutineaktivitetsteorien ikke er tilstrækkelig til at identificere de karakteristikker og faktorer, som gerningsmænd benytter til at udvælge deres ofre. Konklusionen er derfor fortsat, at ofrene er udvalgt tilfældigt, men de anbefaler yderligere forskning på området.

Andre forskere har dog fundet frem til resultater, som viser, at både gerningsmandens og offerets karaktertræk faktisk har betydning for deres adfærd i forbindelse med phishing. Dion (2010) undersøger, hvordan gerningsmændene inkluderer machiavellistiske (manipulerende) og narcissistiske træk i phishingmails, og hvordan de benyttes til at manipulere ofre. Det gør de eksempelvis ved at udgive sig for at være en højerestående person såsom en direktør, en præsident eller en kongelig for derved at understrege deres suverænitet og manipulere offeret. Han sætter dog spørgsmålstegn ved, om gerningsmændene bevidst benytter narcissistiske træk i deres mails, eller om det er et udtryk for, at gerningsmanden selv besidder disse træk. De efterspørger derfor også yderligere forskning på området. Dion konkluderer, ligesom Gupta et al. (2017), at grundet udfordringerne med at opspore gerningsmændene, er den bedste indsats mod phishing oplysning, vidensdeling og opmærksomhed omkring truslen.

Curtis, Rajivan, Jones og Gonzalez (2018) har forsket yderligere i, hvordan karaktertrækkene machiavellisme, narcissisme og psykopati har betydning for både gerningsmænd og ofre for phishing. Undersøgelsen viste, at gerningsmænd med karaktertrækket machiavellisme bruger mere tid på at målrette angrebet mod det specifikke offer, mens personer med karaktertrækkene narcissisme og psykopati sender mindre individualiserede phishingmails. De finder ud af, at offerets personlighedstræk er af størst betydning for succesraten for angrebet, og at chancen for succes med et phishingangreb er højere, hvis offeret har narcissistiske træk, fordi de ofte er over-selvsikre og derfor har tendens til ukritisk at besvare en phishingmail. Konklusionen er, at både gerningsmandens og offerets karaktertræk har betydning for, hvordan phishingangrebet udføres, og om det bliver succesfuldt. Forfatterne mener, at denne viden er brugbar i forhold til, hvordan personer med forskellige karaktertræk udfører phishing, og hvilke personer der har størst risiko for at blive ofre for kriminaliteten. Andre forskere har undersøgt forskellige anti-phishingværktøjer med henblik for at kunne udvikle konkrete løsningsforslag til at bekæmpe phishing.

4.3 Forskning i bekæmpelse af phishing

Li og Schmitz (2009) undersøger de udfordringer, der kan være med eksisterende anti-phishingværktøjer. Herunder har de specifikt fokus på *honeypots*, som er et værktøj til at spore phishingmails og finde frem til deres afsender. I forbindelse med udviklingen af anti-phishingsystemer identificerer Li og Schmitz (2009) to kerneproblematikker. For det første er det umuligt at skabe et automatiseret opsporingsværktøj baseret på statistisk data, og for det andet er ethvert anti-phishingsystem, som afhænger af menneskelig dømmekraft, dømt til at fejle på et tidspunkt. Derfor kommer de med forslag til at forbedre brugen af honeypots. Som forslag til forbedringer anbefaler Li og Schmitz (2009) at benytte netbanker eller andre netbetalingsplatforme som honeypots for at kunne spore gerningsmændene. De konkluderer, at selvom deres forslag ikke er perfekt, vil det give en ny indgangsvinkel til bekæmpelse af phishingangreb.

Birk, Gajek, Grobert og Sadeghi (2007) kommer også med et løsningsforslag, som inkluderer brugen af honeypots. De undersøger organiseret it-kriminalitet og herunder specifikt organiseret phishing. De kortlægger i den forbindelse, hvordan phishing benyttes

til at indhente informationer og data, som videresælges på det sorte marked, og hvordan pengene efterfølgende hvidvaskes. I den forbindelse foreslår Birk et al. (2007), at man proaktivt sender falske informationer til phishernes hjemmesider, som øremærkes, så de kan spores tilbage til phisherne. På denne måde mener de, at det ved hjælp af honeypots er muligt at finde frem til nøglepersonerne i phishingangreb. Ligesom Li og Schmitz (2009) og Birk et al. (2007) undersøger Aleroud og Zhou (2017) tilgange til bekæmpelse af phishing. Forfatterne beskriver, at det er udfordrende at forebygge phishingangreb, da et succesfuldt phishingangreb afhænger mere af menneskelig interaktion og psykologi end teknologi. Dertil beskriver de, hvordan de modsvar, der findes inden for bekæmpelse af phishing, ofte reagerer for langsomt i forhold til angrebene. Som tidligere beskrevet af Gupta et al. (2017), kan det være svært at bekæmpe phishing, fordi hver gang en passende løsning bliver fundet, så finder it-kriminelle blot en ny fremgangsmåde. Aleroud og Zhou (2017) konkluderer derfor, at der er signifikante udfordringer på området. De eksisterende løsningsforslag kritiseres af Aleroud og Zhou (2017) for at ekskludere vigtige aspekter i bekæmpelsen af phishing, herunder relevante medieplatforme hvorpå angrebene foregår, samt at deres strategier for bekæmpelse af phishing er for uspecifikke.

4.4 Delkonklusion

Phishing er et stadigt stigende problem, og som det fremgår af litteraturen, er der forsket en del i kriminalitetsformen. Meget af forskningen har fokus på at belyse phishing som fænomen, men der er kun få forslag til, hvordan det bekæmpes. I Danmark er der lavet undersøgelser af den generelle it-sikkerhed, hvor phishing indgår (Kruize, 2009, 2013, 2018; Digitaliseringsstyrelsen og DKCERT, 2017; Sharp, 2010). Disse har dog været af kvantitativ karakter i form af især offerundersøgelser og har ikke haft fokus på phishing som isoleret fænomen, eller hvordan det bliver udført. Undersøgelserne i dansk kontekst har derimod fokus på it-sikkerhed generelt, og phishing som særlig it-kriminalitetstype har derfor ikke været fremhævet i dansk forskning.

5. Teori og metode

I dette kapitel præsenteres de teorier og metoder, der har dannet rammen for empiriindsamlingen og den efterfølgende analyse. Først præsenteres aktør-

netværksteorien, som er den centrale teori i specialet. Herunder inddrages overvejelser omkring undersøgelsens videnskabsteoretiske position. Efterfølgende gennemgås de metodiske valg, og hvordan disse relaterer sig til aktør-netværksteorien.

5.1 Teori

Dette afsnit præsenterer kort science-technology-society studies (STS) som forskningsfelt og herunder aktør-netværksteorien og dens væsentligste begreber. Efterfølgende præsenteres et litteraturstudie af, hvordan teorien tidligere er blevet anvendt til at analysere både traditionel kriminalitet og it-kriminalitet.

5.1.1 Aktør-netværksteori

STS er et bredt forskningsfelt, som i takt med den teknologiske udvikling er blevet mere og mere anerkendt (Jensen, Lauritsen og Olesen, 2007, s. 7). STS rummer mange forskellige analytiske termer og ideer, men fælles for dem er interessen for, hvordan samfundet og teknologien påvirker hinanden og herunder samspillet mellem menneskelige og ikke-menneskelige aktører (Jensen, 2010, s. 376). STS studerer derfor, hvordan aktørerne danner relationer - også kaldet netværk - på kryds og tværs. Årsagen til, at visse netværk er stabile, mens andre er ustabile, har været omdrejningspunktet for mange STS-analyser. Det er især interessant, hvordan teknologiers tilblivelse er afhængig af samfundet, og hvordan de igennem hele processen også selv påvirker samfundet (Jensen, 2010, s. 376-377).

Aktør-netværksteorien (ANT) er en teori inden for STS, som kan benyttes til at analysere, hvordan samfundet er opbygget af relationer. En af de mest prominente fortalere for ANT er den franske videnskabssociolog Bruno Latour. ANT tilhører den konstruktivistiske videnskabsposition og beskuer samfundet som et netværk af aktører, som både kan være menneskelige og ikke-menneskelige (Latour, 2008, s. 86). Til forskel fra andre sociologiske teorier inddrager ANT objekter i sociale sammenhænge på lige fod med mennesker for dermed at synliggøre, hvordan de indgår i og påvirker samfundet.

ANT kan bedst betegnes som en associationsteori, som analyserer og kortlægger, hvordan aktører er associeret med hinanden. ANT opstod som kritik af sociologien, der ifølge Latour (2008, s. 21-26) har en tendens til at behandle samfundet og det sociale som en

konstant variabel, der kan forklare individers handlen. Han kritiserer blandt andre Durkheim for at betragte det sociale som årsagen til stort set alt, mens alle andre aktører blot manipuleres af dets magt. Dermed ender det sociale med at blive mystificeret og kan ikke forklares. Latour (2008, s. 130-131) mener, at det sociale derimod ikke skal ses som forklaringen, men som det, der skal forklares. På den måde er samfundet en sammenvævning af aktører, hvorigennem det sociale opstår, og ved at følge disse aktørers omskiftelige forbindelser og relationer er det muligt at analysere, hvordan samfundet opbygges gennem associationer. Latour mener ikke, at sociologien skal være en videnskab om det sociale, men derimod en videnskab om associationer. Betegnelsen social er derfor ikke et ord, der beskriver et isoleret fænomen, men det er en betegnelse for forbindelser mellem fænomener, der ikke i sig selv er sociale. ANT søger altså at forklare det, andre sociologiske teorier ikke kan. ANT vil forklare det sociale; det er ikke det sociale, der skal stå for forklaringen (Latour, 2008, s. 26+132). Durkheim vil eksempelvis forklare kriminalitet i samfundet som et udtryk for det sociales dominerende magt over en individuel persons handlinger. Det sociale er således forklaringen på kriminaliteten (Brown, Esbensen og Geis, 2013, s. 268). Derimod vil ANT-forskeren søge forklaring på samfundets konstellationer ved at analysere aktørernes relationer, og disse forbindelser kan være med til at kortlægge det netværk, hvori kriminaliteten opstår. Det sociale er således ikke forklaringen, men det, der forklares i analysen af aktørernes forbindelser i netværket. I en ANT-analyse benyttes en række centrale begreber:

Aktør

Ifølge Latour (2008, s. 94) er en aktør en hvilken som helst ting, der gør en forskel i en tilstand. En aktør defineres af, hvad den gør, og den kan derfor både være menneskelig og ikke-menneskelig (Latour, 1999, s. 303). Eksempelvis så "sender" computeren en mail, og det at sende en mail uden en computer ville være en helt anderledes aktivitet. De ikke-menneskelige aktører indgår altså på lige fod med menneskelige aktører (Latour, 2008, s. 86). Sociologernes definition af aktører er ofte begrænset til mennesker, som foretager sig noget bevidst, men det har ifølge Latour (2008, s. 94+105) den konsekvens, at sociale forklaringer ofte ender med at skjule det, de burde afdække. Selvom ANT inkluderer objekter på lige fod med mennesker, skal teorien ikke blot ses som en sociologi, der også inkluderer ikke-mennesker (af mangel på bedre ord) (Latour, 2008, s. 133). Det er selve

denne skelnen mellem subjekt og objekt og samfund og natur, der skal opløses, da der ikke eksisterer nogen spaltning mellem det sociale og det materielle. Det ville derfor være misvisende at sige, at de påvirker hinanden, da selve skelnen mellem dem ikke giver mening. Spaltningen skal ignoreres, og derfor er det begrebet "aktører", der står tilbage (Latour, 2008, s. 99).

Computeren, der sender mailen, kan dog også anskues som et netværk bestående af forskellige aktører - herunder de materialer den er lavet af, fabrikken den er produceret på, personen der opfandt den og så videre. På den måde er en aktør en aktør i et netværk, men udgør også et netværk i sig selv. Det er aktørerne, der er nøglen til at forstå, hvordan det sociale imellem dem skabes, og det er ved at følge dem, at man kan lære, hvilke metoder de har udviklet for at hænge sammen (Latour, 2008, s. 33).

Netværk

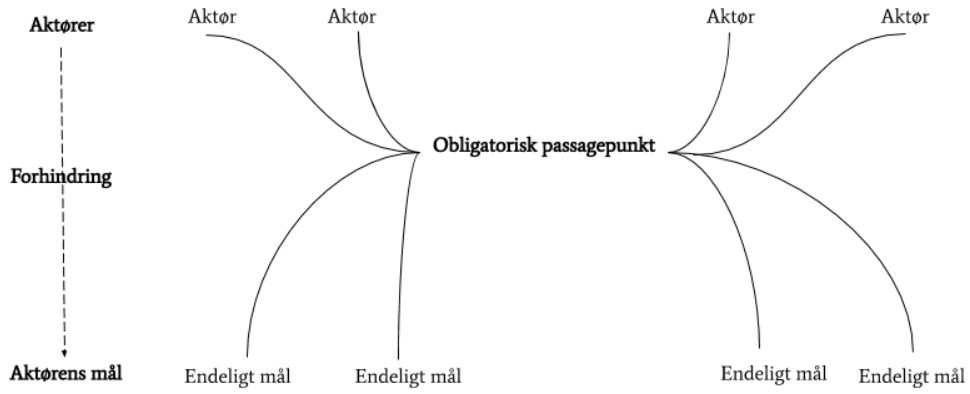
Netværk består af relationer mellem aktører, som er vævet sammen i knuder og forbindelser og tilsammen danner et netværk. Et netværk og dets aktører påvirker og konstituerer konstant hinanden, samtidig med at de enkelte aktører også påvirker hinanden indbyrdes (Latour, 2008, s. 155). Hvis en af disse aktører ændres eller fjernes, så påvirker det hele netværket, og der vil derfor ikke længere være tale om det samme netværk. Et netværk skal altså ikke ses som en konstant fastrammet entitet, men snarere som et spor efter aktører i bevægelse. Det er et redskab til at følge og beskrive aktørerne (Latour, 2008, s. 155+159). Latour (2008) ønskede egentlig, at ordet *network* blev erstattet med *worknet*, da det er aktørerne og deres ageren, der udgør netværket. Netværket er således blot et begreb eller et udtryk for den bevægelse, som aktørerne gør, for at få hverdagen til at hænge sammen. Det er disse bevægelser, som skal kortlægges og følges for at kunne beskue netværket (Latour, 2008, s. 160).

Translation

En translation opstår mellem aktører og er det, der genererer associationer (Latour, 2008, s. 133). Latour (1999, s. 311) beskriver translation som en proces, hvorigennem aktører erstatter og modificerer hinandens forskellige interesser i netværket. Translation handler altså om, hvordan aktørerne associeres med hinanden, tager form og skaber form i

netværket. ANT-forskeren Michel Callon (1984) har uddybet, hvordan en sådan proces foregår. En translationsproces kan ses som en proces, hvor forskellige aktører samarbejder om at nå et fælles mål og skabe en translation. Han inddeler translationsprocessen i fire stadier:

1. *Problematisering*: På det første stadie er der en aktør, der gør sig uundværlig i processen ved at definere et *obligatorisk passagepunkt*, som alle aktørerne skal igennem som led i at nå deres individuelle mål. Det obligatoriske passagepunkt er på den måde et element, der får aktørerne til at samarbejde om det fælles mål (Callon, 1984, s. 203-204). Figur 1 viser et eksempel på en translationsproces med fire aktører, som hver især har et endeligt mål, som kræver, at de gennemgår det obligatoriske passagepunkt:



Figur 1: Illustration af første trin i Callons translationsproces

2. *Interessement*: Aktørerne låses fast i deres tildelte roller i translationsprocessen, så de kan samarbejde. Hver aktør har det, Callon (1984, s. 206) omtaler som en *forhindring* (obstacle problem), der betyder, at de ikke kan nå deres individuelle mål alene - de er nødt til at indgå i processen med de andre aktører.

3. *Indrulning*: Hvis det andet trin i processen er succesfuldt, forbindes aktørernes roller til hinanden igennem forhandlinger på det tredje stadie. Gennem disse

forhandlinger hjælper de hinanden med at undgå deres forhindring og nå deres mål (Callon, 1984, s. 211-212).

4. *Mobilisering*: På det sidste trin udvælges aktører til at agere talsmænd for andre. I en efterforskning kan det eksempelvis være den enkelte efterforsker, der agerer talsmand for hele politiet og repræsenterer deres interesser. Det er vigtigt, at talsmændene er i stand til at repræsentere kollektivet, da de ellers kan blive forrådt, så processen ophører med at være succesfuld (Callon, 1984, s. 219-220).

Denne translation er en dynamisk proces, hvilket betyder, at netværket er i konstant bevægelse. Latour (1999, s. 49-51) beskriver en translationsproces af jordprøver fra regnskoven i Amazonas. Disse jordprøver er aktører, som bliver nummereret og farvekodet, og disse koder repræsenterer således jordprøverne. Jordprøverne bliver derved translateret til tal og farver, som vi som mennesker kan konceptualisere og undersøge i laboratorier.

Den sorte boks

En sort boks er et netværk af aktører, som er blevet så stabilt, at netværket ikke længere bliver anset som problematisk. Som resultat af netværkets succes bliver det usynliggjort og betragtes som en kendsgerning (Latour, 1987, s. 91-92, 1999, s. 304). Hvis denne stabilitet brydes, fordi der opstår problemer i netværket, så anses det ikke længere som en kendsgerning, og det er nødvendigt at åbne den sorte boks og beskue de enkelte aktører og deres relationer (Latour, 1999, s. 185). Computeren er et netværk af mange forskellige aktører, men den bliver oftest forstået som en samlet genstand. Så længe computeren virker uden problemer, vil denne opfattelse bestå, men hvis computeren stopper med at fungere, vil den ikke længere fremstå som et stabilt netværk. Kendsgerningen brydes, og det vil derfor være nødvendigt at åbne netværket (computeren), for at finde ud af hvilke aktører der skaber problemet. Dette er meget lig den fremgangsmåde, som en computertekniker anvender, når han eller hun udskifter dele (aktører) for at reparere en computer, som ikke længere virker.

5.1.2 ANT som analyseværktøj til kriminalitet

ANT er tidligere blevet anvendt i forskningen til at analysere kriminalitet som et netværk af både menneskelige og ikke-menneskelige aktører. Dette er også relevant i forhold til phishing, for som Aleroud og Zhou (2017) beskriver, afhænger et succesfuldt phishingangreb både af menneskelig interaktion og teknologi.

Der findes eksempler i litteraturen på, at flere forskere har anvendt ANT på it-kriminalitet. Hedström, Dhillon og Karlsson (2010) analyserer et hackerangreb mod et universitet ved at anvende ANT. Ligesom Aleroud og Zhou (2017) pointerer Hedström et al. (2010), at et succesfuldt hackerangreb ofte anses som et teknologisk brist, men at det er vigtigt at inddrage både menneskelige og ikke-menneskelige aktører, når netværkets usikkerhed skal belyses. Hackerangrebet mod Stellar University opstod som resultat af manglende forhandlinger mellem nøgleaktører i netværket, fordi de opfattede sig selv som isolerede enheder, der ikke havde betydning for hinanden. Netværket blev derfor ustabilt, og det var nødvendigt at åbne den sorte boks og gennemgå de forskellige delelementer, så netværket igen kunne sikres mod hackerangreb.

Ligeledes har Van der Wagen og Pieters (2015) med udgangspunkt i ANT undersøgt en sag om hacking fra Holland, hvor et botnet blev benyttet. Et botnet er et netværk af computere, som er inficeret, og som kan fjernstyres af gerningsmanden. Igennem ANT beskues skabelsen af dette botnet med hjælp af både menneskelige og ikke-menneskelige aktører, som interagerer med hinanden. Van der Wagen og Pieters (2015) konkluderer, at ANT kan give en unik indsigt i it-kriminalitet, som ikke kan opnås ved brug af andre teorier. Van der Wagen og Pieters (2018) bygger videre på deres tidligere undersøgelse og anvender ANT til at undersøge viktimisering inden for it-kriminalitet. Det er med henblik på at belyse begrænsningerne i de nuværende teorier om ofre og præsentere et nyt syn på ofre igennem ANT. Dette gøres ved at anse offeret som et netværk, som kontrolleres af en gerningsmand, som også udgør et aktør-netværk. I den forbindelse konkluderer Van der Wagen og Pieters (2018), at tre ANT-baserede koncepter kan benyttes til at beskue sårbare ofre, og at disse kan hjælpe til at forebygge it-kriminalitet. Eksempelvis offerets og gerningsmandens netværk som ikke kun indbefatter menneskelige aktører, men også ikke-menneskelige aktører som eksempelvis offerets antivirusprogram. Offeret kan også

translateres som aktør til nye netværk, i forbindelse med at vedkommendes computer eksempelvis bruges i et botnet.

Foruden it-kriminalitet er ANT også benyttet til at analysere traditionelle kriminalitetsformer, som udspiller sig i et netværk med mange associerede aktører.

Demant og Dilkes-Frayne (2015) benytter ANT til at analysere to cases om situationel kriminalitetsforebyggelse af stoffer i nattelivet. En vigtig pointe er, at situationel kriminalitetsforebyggelse har fokus på interaktionen mellem menneskelige og ikke-menneskelige aktører ligesom ANT. ANT kan dog supplere den situationelle kriminalitetsforebyggelse ved at give indsigt i, hvordan netværk konstrueres, og hvordan aktører påvirker hinanden. Derfor kan ANT anskueliggøre, hvordan de kriminalitetsforebyggende tiltag påvirker netværket og medvirker til enten mindre kriminalitet, eller at der blot sker en forskydning af kriminaliteten i tid og rum. Et andet eksempel på ANT brugt i forbindelse med kriminalitetsforebyggelse er Douillet og Dumoulin (2015), som viser, hvordan ANT kan anvendes til at forklare udviklingen og udbredelsen af overvågningskameraer i eksempelvis Frankrig, og hvorfor nogle byer oplever en stor udbredelse af overvågningskameraer, mens andre er mere forsigtige med at anvende dem. Forfatterne anvender samtidig ANT til at belyse, at det ofte hverken er kriminalitetsraten eller politiske trends, der gør, at der bliver opsat overvågningskameraer. Derimod hævder forfatterne, at nye overvågningsnetværk opstår som resultat af, at talsmænd mødes, og dermed kopieres eksisterende overvågningsnetværk til nye netværk.

ANT er også benyttet af forskere til at undersøge fænomener inden for kriminalitet, som eksisterende kriminologisk teori har svært ved at redegøre for. Moore og Singh (2015) argumenterer for, at ANT åbner op for nye muligheder for at studere vold mod kvinder. Forfatterne mener, at aktørerne og deres forbindelser skal synliggøres. Forfatterne illustrerer dette ved at anvende ANT på en billedserie, hvor en mand udøver vold mod sin partner. Billedserien indgår som en ny aktør i netværket. Et af billederne viser, at manden slår sin partner. Fordi denne aktør (billedet) eksisterer, så kan manden ikke benægte, at han har slået sin partner, og samtidig kan partneren heller ikke benægte, at hun er blevet slået. Billedet er derfor et bevis på mandens vold, og denne aktør gør, at hele netværket

ændrer sig. Moore og Singh (2015) illustrerer, hvordan ANT kan bidrage med en ny forståelsesramme af vold mod kvinder, hvor både menneskelige og ikke-menneskelige aktører har betydning for, hvordan hele netværket opfattes.

ANT er anvendt til at belyse både it-kriminalitet og traditionel kriminalitet som netværk af aktører, og hvordan disse netværk konstrueres og udvikler sig, men der findes ikke konkrete analyser af phishing fra et ANT-perspektiv. Det er derfor relevant med ny forskning, hvor ANT inddrages til at beskue phishing som et kriminologisk fænomen for at klarlægge, hvilke aktører og forbindelser der udgør netværket og derigennem den kriminalitet, der finder sted. I dette speciale bidrager ANT til en forståelse af, hvordan mange forskellige typer af aktører indgår i associationer med hinanden og skaber sociale konstellationer. Da fokus er it-kriminalitet og phishing, som er teknologisk betingede fænomener, er det relevant at anvende en teori, der inddrager både teknologiske og menneskelige aktører. Teknologien og mennesket er begge vigtige aktører for at forstå phishing og det netværk, hvori kriminaliteten opstår, og derfor bidrager ANT med en passende analyseramme til at kortlægge og beskrive de forbindelser, der er afgørende for, hvordan netværket er konstrueret. Vores valg af ANT understøttes af Luppicini (2014), som mener, der er mangel på forskning i interaktionen mellem teknologi og mennesker, og at ANT udgør et godt teoretisk udgangspunkt for forståelse af it-kriminalitet. ANT har en nøglerolle i analysen og forståelsen af it-kriminalitet som et samfundsproblem. Han mener derfor, at ANT i højere grad bør anvendes eksplicit i forskning om it-kriminalitet.

5.2 Videnskabsteoretisk position

Viden har forskellige positioner, alt efter hvilken videnskabsteoretisk tilgang der anvendes til at kvalificere den. ANT har som tidligere nævnt et konstruktivistisk syn på samfundet, og hvordan både viden og teknologi konstrueres i samspillet mellem aktører. Fra et konstruktivistisk synspunkt kan den viden, som er produceret i denne undersøgelse, anses for at være en konstruktion. De forskellige konstruktivistiske retninger er dog ikke enige om, om virkeligheden konstrueres af vores erkendelse, eller om det kun er selve erkendelsen, der modificeres, i takt med at vi opnår mere viden.

Den epistemologiske konstruktivisme ser erkendelsen og den fysiske virkelighed som to forskellige domæner (Collin, 2003, s. 25). Virkeligheden eksisterer altså uafhængigt af vores erkendelse af den, men vores viden om den er konstrueret af begreber og kategorier, som er bestemt af andre faktorer end genstandsfeltet. Ud fra dette synspunkt er resultaterne præsenteret i dette speciale blot én af mange konstruktioner af viden til forståelse og erkendelse af fænomenet phishing. Den ontologiske konstruktivisme foreskriver derimod, at den fysiske virkelighed er konstrueret af vores erkendelse af den, og derfor forsvinder distinktionen mellem ontologi og epistemologi (Collin, 2003, s. 29). Med udgangspunkt i den ontologiske konstruktivisme har vi undersøgt phishing og bidraget til erkendelsen og dermed fænomenets virkelighed. Denne videnskonstruktion er dog foranderlig og kan derfor modificeres ved nye undersøgelser. Ontologien er altså relativistisk, hvilket vil sige, at virkeligheden er afhængig af individet. Derfor eksisterer virkeligheden gennem vores forståelse af den. Latour (1996, s. 375) ønsker selv at fjerne distinktionen mellem repræsentationerne og tingen (epistemologien og ontologien). Han interesserer sig mere for, hvordan objekter repræsenteres, end for hvad de isoleret er. Han nævner dog, at alle entiteter både har en erkendelse og en eksistens, som er ekstern fra denne, uden at gå i dybden med hvor meget af en aktørs ontologi der konstrueres af vores erkendelse af og interaktion med den. Det betyder, at phishing og kriminalitet som objekter i sig selv er "noget", men at de også er påvirkelige af aktørernes interaktion. Selvom ANT beskæftiger sig mere med ontologi end med erkendelse, er det ikke helt entydigt, om teorien er ontologisk konstruktivistisk.

Den præsenterede viden kan fra et ANT-synspunkt altså ses som et udtryk for, at vi i en vis grad medvirker til en konstruktion af phishingfænomenet i netværket. Den viden, som præsenteres i projektrapporten, kan dermed også medvirke til en ny konstruktion af begrebet phishing for læseren. Her er spørgsmålet dog, om selve fænomenet phishing er ændret af konstruktionen, eller om det blot er læserens erkendelse af det, der påvirkes.

5.3 ANT som metodologi

Vi vil i følgende afsnit reflektere over betydningen af at anvende ANT som metodologi, og hvordan denne ramme har påvirket valget af metoder til empiriindsamlingen, Yderligere

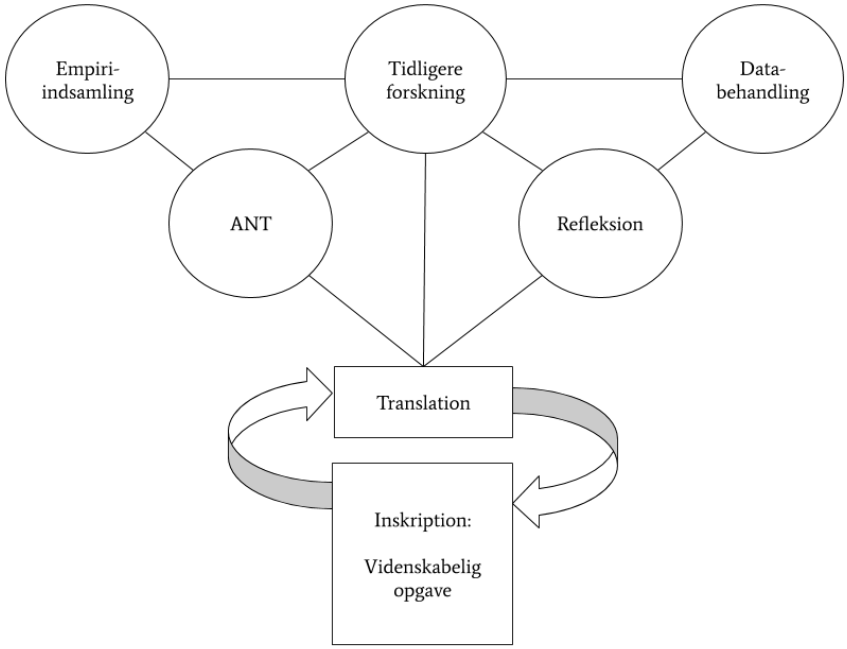
vil vi gennemgå de forskellige metodiske afgørelser, vi gennem arbejdsprocessen har truffet, og hvordan det har påvirket det endelige empiriske materiale.

Metodisk tilgang til phishing som aktør og netværk

Valget af ANT som analytisk og metodisk ramme har betydning for specialet, da phishing fra et ANT-perspektiv både kan beskues som en aktør og et netværk. Phishing er en aktør i større netværk af eksempelvis it-kriminalitet og er i sig selv også et netværk bestående af forskellige aktører. Ved at kortlægge aktørerne og deres relationer er det muligt at se, hvordan de konstruerer og forhandler med hinanden. Det giver et indblik i, hvordan disse aktører søger at stabilisere netværket, og hvilke translationsprocesser der finder sted. Samlet set giver dette en forståelse for, hvordan efterforskere, gerningsmænd, computere og phishingmails påvirker netværket, og hvorfor det ser ud, som det gør. Vores empiriindsamling har bestået af at afdække aktører og undersøge deres relationer til hinanden, hvilket giver en forståelse for netværket indefra. De forskellige aktører skal anses som ligeværdige, da det kun ved en empirisk undersøgelse er muligt at afdække, hvordan de er forbundet til hinanden. Det er med andre ord ikke en forudgående kategorisering og overbevisning, som skal styre, hvilke aktører der skal være fokus på. Vi skal fralægge allerede eksisterende antagelser om netværket og lade netværket vise sig, som det er. Vi skal derfor ikke antage, at nogle aktører er til stede i netværket eller tillægge nogle aktører mere værdi end andre, med mindre dette empirisk kan observeres. Den indsigt opnår vi ved at følge aktørerne og det netværk, de konstant skaber med deres translationer og associationer til hinanden (Latour, 2005, s. 12, 2008, s. 33).

Vores indgangsvinkel til at opnå viden om phishing var at lave et omfattende litteraturstudie. De videnskabelige artikler, der er udgivet om phishing, udgør alle aktører, der er en del af phishingnetværket, da de præsenterer resultatet af en række forskellige undersøgelser. Derved er hver artikel også et resultat af en translationsproces, hvor forfatterne har indsamlet empiri, lavet databehandling og holdt dette op mod den eksisterende litteratur om emnet. Sammenfatningen af dette er efterfølgende blevet translateret til en samlet artikel trykt på papir. Dette speciale er i sin helhed også resultatet af en translationsproces, hvor tidligere forskning kombineret med vores egen indsamlede empiri udgør denne rapport som en aktør, der nu også indgår i phishingnetværket. En

inskription er et begreb, som bruges af Latour (1987, s. 68) om en billedliggørelse af videnskabelig forskning. Det kan være en figur, en graf eller en citation, som giver visuelt bevis for forskningen. Den videnskabelige opgave kan derfor ses som en inskription af den indsamlede viden, som fremlægges i specialet, hvilket fremgår af følgende illustration:



Figur 2: Illustration af den videnskabelige opgaves inskriptionsproces

Som det ses, indgår empiriindsamlingen og databehandlingen i en translationsproces med ANT, tidligere forskning og vores refleksioner. Dette udmunder i den endelige videnskabelige opgave, som derfor fremstår som en inskription af den udførte undersøgelse.

Litteraturstudiet har endvidere ageret talsperson og været en måde, hvorpå vi kunne identificere nogle af de øvrige aktører i netværket (Latour, 1987, s. 70). Eksempelvis analyseres og diskuteres forskellige phishingmails i litteraturen, og selve mailen identificeres på den måde som en aktør i phishingnetværket, som derfor også er en vigtig aktør for os at inddrage i analysen af phishing i en dansk kontekst. Vi har derudover valgt at inddrage forskellige it-efterforskere hos Nordjyllands Politi og NC3 (Rigspolitiets Nationale Cyber Crime Center), en it-sikkerhedschef, en juridisk professor og en

kriminologiprofessor til at give os indblik i deres relationer og position i netværket. Derved opnår vi viden om mange forskellige aktører, da netværket ikke kan kategoriseres, førend praksis er blevet undersøgt, og aktørerne selv er kommet til orde i empiriindsamlingen (Latour, 2008, s. 33).

5.4 Metode

I dette afsnit præsenteres de metoder vi har benyttet til empiriindsamlingen. Først præsenteres den overordnede kvalitative metode, hvorefter semistrukturerede interviews, telefoninterviews og ekspertinterviews uddybes. Afslutningsvis beskrives databehandlingen og kvaliteten af den indhentede empiri.

5.4.1 Kvalitativ metode

I ANT eksisterer der et princip om symmetri, som omhandler, at der ikke skelnes mellem forskellige typer af aktører (Latour, 2008, s. 86). Symmetrien i ANT har haft betydning for, hvordan vi rent metodisk tilgik empiriindsamlingen, da vi var opmærksomme på ikke kun at observere menneskelige aktører i netværket. Til indhentning af empiri valgte vi den kvalitative metode, da den bedst lader os interagere med de forskellige aktører. I et kvalitativt studie undersøges det, hvordan noget gøres, opleves, fremtræder eller udvikles. Der er fokus på at beskrive, forstå, fortolke eller dekonstruere et emne med henblik på at få et så detaljeret indblik i det som muligt. Kvalitative studier giver derfor et mere nuanceret og detaljeret billede af et emne, end et kvantitativt studie ville gøre (Brinkmann og Tanggaard, 2010, s. 17-18). Med udgangspunkt i problemformuleringen hvor fokus er, hvordan phishing som it-kriminalitetsform bekæmpes i det danske efterforskningsnetværk, er den kvalitative metode ideel, da ønsket er at få et detaljeret indblik i udfordringerne ved bekæmpelse af phishing. Den kvalitative metodes studie af, hvordan noget gøres og fremtræder, danner også et godt udgangspunkt for en ANT-analyse, hvor fokus er på aktørerne og deres relationer til hinanden. Disse relationer undersøges bedst ved at observere og interagere med aktørerne for at få et indblik i, hvordan de danner forbindelser.

Vi har udført fem semistrukturerede interviews med seks informanter, som alle er aktører i phishingnetværket. De har givet indsigt i deres arbejdsopgaver, meninger og perspektiver

på forskellige problemstillinger. Slutteligt analyserede vi en dansk phishingmail for at få indsigt i den som aktør, der påvirker og har associationer til de resterende aktører.

5.4.2 Semistrukturerede interviews

Det semistrukturerede interview er en interviewform, som benyttes til indhentning af kvalitativ empiri. Før et interview påbegyndes, er en grundig gennemgang af litteraturen om emnet en nødvendighed, da det er vigtigt for at have den bedst mulige viden forud for interviewet for at kunne sætte sig ind i den teoretiske baggrund for genstandsfeltet og stille kvalificerede spørgsmål (Brinkmann og Tanggaard, 2010, s. 37). Den indhentede viden i forbindelse med udarbejdelsen af vores problemfelt og litteraturstudie har givet indsigt i både it-kriminalitet generelt og phishing mere specifikt. Denne indsigt gør, at vi bedre kan identificere og observere aktørerne. Den viden har også hjulpet os med at afgøre, hvilken retning vi ønsker at gå med de forskellige interviews og med at kvalificere interviewspørgsmålene. Vi er dog opmærksomme på, at vores forhåndsviden ikke må begrænse informanten i interviewsituationen, således at informanten kan bidrage med nye perspektiver på emnet.

Vi har valgt det semistrukturerede interview som metodisk tilgang til indhentning af empiri, da det er en interviewform, hvor intervieweren i en vis grad har styringen og tager udgangspunkt i en interviewguide, som er udformet på baggrund af den forudgående vidensindhentning. Dog giver det semistrukturerede interview også mulighed for, at de planlagte spørgsmål kan skubbes til side til fordel for at forfølge en informants fortælling, hvis det er relevant (Kvale og Brinkmann, 2009, s. 45). Fra et ANT-perspektiv anses interviewsituationen i sig selv som et netværk af aktører, som interagerer med hinanden. Dette værende eksempelvis intervieweren, informanten, diktafonen og interviewguiden. Alle disse aktører interagerer med og påvirker hinanden på kryds og tværs, hvorved interviewnetværket dannes. Det semistrukturerede interview er velegnet til vores empiriindsamling, da vi både kan få besvaret de forberedte spørgsmål og samtidig har mulighed for at kunne forfølge andre nye emner, som dukker op under interviewforløbet. Efterhånden som flere interviews gennemføres, udvikles vores forståelse af feltet, og datakvaliteten øges løbende, da intervieweren kan stille mere og mere kvalificerede spørgsmål (Ankersborg, 2011, s. 72). Vi ønsker ikke at lade os begrænse af vores

forudgående viden, og derfor er det kun en fordel, hvis informanten selv kan tage styringen og vurdere, hvad der er relevant.

Interviewguiden som værktøj og aktør

Semistrukturerede interviews udføres ud fra en interviewguide, som fungerer som rød tråd i interviewet. Den kan indeholde relevante emner og forslag til spørgsmål, som ønskes besvaret (Kvale og Brinkmann, 2009, s. 45). Vores interviewguide er opdelt i forskningstematikker og interviewspørgsmål. Forskningstematikkerne er udformet ud fra vores teoretiske baggrund og søger at afdække den konkrete viden til at besvare problemformuleringen. Dog udgør forskningstemaer sjældent gode interviewspørgsmål, og vi har derfor valgt at omformulere dem, så de passer bedre ind i en interviewkontekst. Interviewspørgsmålene er typisk indledende spørgsmål, som har til hensigt at få informanten til at fortælle sin historie. Disse efterfølges af opfølgende spørgsmål, hvis et relevant emne afdækkes under fortællingen (Brinkmann og Tanggaard, 2010, s. 41).
Vores interviewguides er udformet specifikt til de individuelle informanter. Det skyldes, at informanterne er eksperter inden for forskellige områder, og specialiserede spørgsmål er derfor en fordel. Vores interviewguides har dog det tilfælles, at de indledes med, at informanten skal præsentere sig selv, og hvilken viden eksperten repræsenterer. Vi har haft fokus på hovedsageligt at stille åbne spørgsmål, som ikke blot kan besvares med ja eller nej, fordi vi på den måde kvalificerer informantens svar, som bliver mere detaljerede (Deacon, Pickering, Golding og Murdock, 2007, s. 80).

Interviewguiden har stor betydning for, hvordan interviewet forløber, og hvilken viden der indsamles. Den indgår på den måde som en aktør i interviewnetværket, der påvirker de øvrige aktører. Da det ikke er meningen, at interviewguiden skal følges slavisk, giver den informanten mulighed for at afdække eventuelle aktører, som vi ikke har været opmærksomme på, og giver os muligheden for at forfølge disse.

5.4.3 Telefoninterviews

Da informanterne har arbejdspladser forskellige steder i Danmark, har vi valgt at udføre nogle af interviewene telefonisk. I telefoninterviews udelukkes nonverbal kommunikation, og det er kun muligt at kommunikere verbalt med informanten. Dog anses den nonverbale

kommunikation ikke som havende en afgørende karakter for vores interviews, da det er eksperternes viden og udsagn, som er relevante, og ikke deres kropssprog. Det relaterer sig også til, at vores interviews er i en professionel og ikke en personlig kontekst (Christmann, 2009, s. 160). Den nonverbale kommunikation kan dog være afgørende for en god samtaledynamik, selvom informantens kropssprog ikke inddrages i den efterfølgende analyse (Deacon et al., 2007, s. 67). Derudover er vi også opmærksomme på, om informanterne er påvirkede af vores tilstedeværelse i interviewsituationen, og om de eventuelt ikke vil give os deres egentlige mening, men snarere vil give os de svar på vores spørgsmål, som de tror, vi ønsker at høre. I den forbindelse har telefoninterviews den fordel, at den distance, som skabes imellem os og informanten, mindsker den form for bias markant (Bryman, 2012, s. 214).

I et ANT-perspektiv udgør selve interviewsituationen et netværk. Ved et telefoninterview er dette netværk udgjort af blandt andet vores telefon, diktafonen, interviewguiden, informanten og informantens telefon, som alle er aktører. Aktørerne har dynamiske associationer til hinanden, og det er gennem alle disse forbindelser, situationen konstrueres. Det er en interessant måde at anskue den metodiske tilgang på, da hver aktør påvirker netværket, hvor vores empiri og viden konstrueres. Den indsamlede empiri er derfor heller ikke en isoleret genstand, men er et resultat af relationerne mellem alle aktørerne i netværket. Interviewsituationen er således et netværk i sig selv, der samtidig har til formål at give et indblik i andre netværk. På den måde er det vigtigt at være opmærksom på, at netværket, hvori empiriindsamlingen foregår, er dynamisk og påvirkes af andre netværk og aktører.

5.4.4 Ekspertinterviews

De semistrukturerede interviews er udført med eksperter som informanter. Et ekspertinterview er især anvendeligt til at få konkret viden på et område fra en fagperson. Eksperten repræsenterer dermed mere end sig selv som person og repræsenterer også et helt felt og taler på vegne af sin viden på området (Kvale og Brinkmann, 2009, s. 167). Det er en klassisk ANT-tilgang at identificere og inddrage talspersoner, som taler på vegne af andre. På den måde får vi viden om et større felt, da informanten både kan tale ud fra sin egen erfaring, den eksisterende forskning og viden fra undersøgelser, der ikke i sig selv kan

tale. Latour (1987, s. 71) bruger udtrykket, at talspersonen er andre aktørers *mundstykke*. Vi har med andre ord adgang til en talsperson, der i kraft af sin ekspertrolle repræsenterer og taler for andre aktører. Ekspertinterviewet anses derfor også som en effektiv metode til at indhente en stor mængde viden på relativt kort tid inden for et specifikt område (Bogner, Littig og Menz, 2009, s. 2).

Vi har valgt at benytte denne type interviews, da viden om phishing i en dansk kontekst er relativt begrænset, og de forskellige aktører ikke nødvendigvis har del i hinandens viden. Det er derfor relevant at hente konkret viden om emnet fra forskellige danske eksperter, så denne viden kan samles. Dertil kan eksperterne anses som aktører i phishingnetværket, og ved at beskrive og interagere med disse aktører bliver vi klogere både på netværket og deres aktørrolle. Aktørerne er altså eksperterne, som ved, hvorfor de handler, som de gør (Gad og Jensen, 2007, s. 112).

I løbet af interviewene er vi opmærksomme på, at vi opnår subjektiv viden, da informanterne vil prioritere det, de mener, er vigtigt i forhold til emnet. Eksperter repræsenterer dog et felt og ikke sig selv som privatperson, hvilket gør, at de sandsynligvis ikke er betonede af den samme grad af subjektivitet. Dog skal ekspertens udsagn ikke tolkes som fuldkommen objektiv, og det er derfor vigtigt at være kritisk over for den viden og de udtalelser, som eksperten bidrager med (Bogner et al., 2009, s. 2). Det har vi i praksis grebet an ved at sammenligne eksperternes udtalelser på kryds og tværs, så ingen af udtalelserne fremstår unuancerede.

Refleksioner over interview med Nordjyllands Politi

Interviewet med Nordjyllands Politi forløb anderledes end forventet. Vi havde forventet, at der kun ville være en informant til stede, men informanten havde valgt at medbringe en kollega, som han mente havde stor viden om det emne, vi var interesserede i. På den ene side var det en fordel, da vi fik endnu en informant til undersøgelsen, som kunne bidrage med sin viden. Det viste sig også undervejs i interviewet, at de to informanter supplerede hinanden godt og ofte kunne uddybe hinandens svar. På den anden side kan der dog også være ulemper forbundet med at interviewe to informanter på samme tid. Deres svar kan påvirke hinanden, så de måske ikke kommer med udtalelser, der går imod det, den anden

har sagt. Vi vidste som sagt ikke, at der ville dukke to informanter op, og hvis vi havde vidst det på forhånd, havde vi haft mulighed for at planlægge interviewet anderledes, da dynamikken i interviewsituationen bliver påvirket af, at der er to informanter til stede. Vi følte derudover, at informanterne fra Nordjyllands Politi var en smule tilbageholdende i deres udtalelser og ikke var så kritiske. Den tendens så vi ikke i samme grad hos de øvrige informanter. Det kan eventuelt skyldes, at de sad to kolleger sammen og derfor tænkte over hinandens tilstedeværelse, når de svarede på vores spørgsmål. I den forbindelse kunne to særskilte interviews med informanterne have givet os andre resultater, som kunne sammenlignes. Interviewet foregik i et fællesareal hos Nordjyllands Politi, hvilket betød, at andre ansatte få gange var til stede i lokalet og snakkede. Det gjorde, at interviewet blev forstyrret, da opmærksomheden blev vendt over mod de andre ansatte, når de kom ind i lokalet. Det kan også have påvirket vores informanter, at andre af deres kolleger var til stede i lokalet, og de derfor holdt sig tilbage. Derudover blev lydoptagelsen forstyrret, da vores diktafon også optog alt baggrundsstøjen. Ud fra et ANT-perspektiv giver dette også mening, da det foreskriver, at aktører handler og påvirker hinanden forskelligt, afhængigt af hvilket netværk de indtræder i. Hvis vi havde haft et privat lokale eller kontor, hvor interviewene kunne afholdes, havde vi interageret med informanterne i et andet netværk, hvor de andre aktører ikke var til stede, hvilket potentielt kunne have resulteret i et andet interview.

5.4.5 Transskription af interviews

Vi har transskriberet alle lydoptagelserne af interviewene fra diktafonen. En transskription er en oversættelse af en mundtlig interviewsamtale til en skrevet tekst, som egner sig til analyse (Kvale og Brinkmann, 2009, s. 199). I forbindelse med transskriptionen af et mundtligt interview til tekstform er der forskellige udfordringer i forhold til at omsætte talesprog til skriftsprog, da det talte sprog adskiller sig fra det skrevne (Kvale og Brinkmann, 2009, s. 202-203). Eksempelvis kan sætningskonstruktionen i tale være væsentlig anderledes end på skrift. I den forbindelse har vi indført en række standarder for transskriptionerne, så disse er udført i samme stil, selvom forskellige personer har transskriberet interviewene. Det er ikke fundet relevant at inkludere en ordret transskription af interviewene, da det er meningsindholdet, der er relevant. Derfor er

pauser, opbrud og ord som "hmm" og "øh" ekskluderet fra transskriptionen, og derved tydeliggøres meningsindholdet. Derudover er visse sætningskonstruktioner fra interviewet gjort grammatisk korrekte for at gøre transskriptionen mere læsevenlig.

Transskriptionerne kan anses som en inskription og er på den måde et konkret produkt som resultat af informantens viden og erfaring gengivet i et interview. Der er således en stor mængde forudgående viden, som koncentreres i transskriptionen, der bliver det endelige produkt, som analysen tager udgangspunkt i.

5.4.6 Meningskondensering og -kategorisering

For at kunne afdække de mest relevante analyseemner fra vores empiri, har vi meningskondenseret og -kategoriseret vores interviews. Meningskondensering udføres ved at kondensere større dele af et interview ned til mindre bidder for derved at få den konkrete mening ud af dem (Tanggaard og Brinkmann, 2010, s. 47). Meningskategorisering er en kodning, hvor vi induktivt har kategoriseret nogle emner fra vores interviews i takt med meningskondenseringen med henblik på at kunne samle dem efterfølgende til overordnede analyseemner. I kategoriseringen har vi også nedfældet nogle analytiske spørgsmål og tanker med henblik på at anvende disse i analysen. Både meningskondenseringen og -kategoriseringen er udført i en tabel, hvor interviewsekvensen fra transskriptionen er indsat til venstre, meningskondenseringen i midten og kategoriseringen til højre. Et eksempel på vores meningskondensering og -kategorisering ses på følgende tabel:

Transskription	Meningskondensering	Meningskategorisering Fortolkning Analyse
Studerende 1: Ja. Så det havde været forskellen, for eksempel hvis det var, hvis du sad på NC3 i stedet for at være ude ved den her politikreds? *Larsen:* Ja, altså man kan sige, at NC3 er jo retsættende og -styrende for den indsats og de kompetencer, der skal bruges i forhold til it-kriminalitet, og der har vi … Der har været to primære issues omkring det, og den ene ting, det er, at det for kredsene har føltes nogle gange som meget langt til selve Rigspolitiet for at skulle få hjælp. Hvem skal man henvende sig til, hvor lang tid tager det og alle de der ting. Og hvad så, hvis der er noget akut, og så er der en kæde af kontaktpunkter, så det har man gerne	Specialiserede medarbejdere, som udsendes til de forskellige politikredse, for at bistå i efterforskninger. Samling af kompetencer Løsning på "afstanden" mellem kredsene og Rigspolitiet Hjælpe hvis efterforskerne sidder fast i it-problemer Undervisning i it-sikkerhed hos virksomheder Både simpel og kompleks it-efterforskning Holder foredrag for virksomheder, med hvad politiet oplever i øjeblikket inden for it-kriminalitet, for at hjælpe med at forebygge angreb hos dem.	**Forkortet afstand i efterforskning** Det kunne være en tidskrævende proces at afklare it-spørgsmål med Rigspolitiet, så NC3 er et forsøg på at forkorte processen og bringe kompetencer ud i de enkelte kredse Tidligere svært at gennemskue hvem man skulle kontakte, men nu it-kompetencerne mere tilgængelige, selv ved simple it-spørgsmål - Før droppede man måske it-vejen hvis den var for besværlig ift. at få hjælp **Forebyggelse ved oplysning** Undersøger gerningsmændenes metoder med henblik på forebyggelse af disse. Opbygge opmærksomhed hos flere aktører, så det ikke kun er politiet, der har viden om truslerne

Tabel 2: Kondensering og kategorisering af empiri

Igennem meningskondenseringen har vi kondenseret interviewpersonens udtalelser for efterfølgende i meningskategoriseringen at brede dem ud igen med henblik på analyse (Tanggaard og Brinkmann, 2010, s. 50-51). Meningskondenseringen og -kategoriseringen har fungeret som et værktøj til at udtrække relevante emner fra vores interviews og kategorisere dem for derved at målrette vores analyse. Det har også fungeret som et referenceredskab, som vi har kunnet vende tilbage til for hurtigt at kunne danne os et overblik over et interview.

5.4.7 Kvalitet i den kvalitative undersøgelse

Der er stor uenighed i metodelitteraturen om, hvorvidt validitet og reliabilitet kan anvendes på kvalitative studier, da disse begreber afspejler den kvantitative forskning mere end den kvalitative (Bryman, 2012, s. 389). Denne problematik kommer til udtryk i den eksterne reliabilitet, som handler om, i hvilken grad fundene i specialet kan genskabes. Det vil dog være svært at genskabe resultaterne, da det ikke kan garanteres, at

interviewomstændighederne kan genskabes, og informanten vil give de nøjagtigt samme svar. Derfor vil vi nu gennemgå nogle af de kvalitetskriterier, som Tanggaard og Brinkmann (2010) mener er vigtige i den kvalitative undersøgelse. Overordnet skal den kvalitative undersøgelse være transparent, og det skal være muligt for læseren at gennemskue, hvordan vi er kommet frem til vores resultater.

Derfor har vi gennem hele specialet været meget transparente omkring de forskellige metoder og teorier, som indtræder heri. Eksempelvis har vi reflekteret over vores metodevalg, samt de problematikker som vi oplevede gennem empiriindsamlingen. Et eksempel er interviewet med informanterne fra Nordjyllands Politi, hvor vi har været transparente omkring de omstændigheder, interviewet foregik under. Det gør, at læseren forstår, under hvilke forudsætninger empirien er indsamlet.

Ifølge Tanggaard og Brinkmann (2010, s. 493) er troværdighedstjek en vigtig del af den kvalitative undersøgelse. Igennem udarbejdelsen af specialet har vi konstant lavet troværdighedstjek på vores empiri og vores resultater. I interviewsituationerne har vi ofte stillet klargørende og opfølgende spørgsmål. Det gjorde vi for at være sikre på, at vi havde forstået informanten korrekt, men også for at prøve at eliminere nogle tvetydigheder i informanternes svar. Denne proces kan ses i følgende eksempel:

"Studerende 1: Ja. Så det, jeg hører jer sige, det er, at... Det bliver sværere i hvert fald.

Thy: Der er i hvert fald nogle store udfordringer omkring kryptering. (...) Det er i forhold til kryptering, og så kan man sige, at mulighederne er blevet uendeligt mange flere. Der er jo mange flere ting, man skal kunne finde ud af både kan finde ud af, men også magte at finde ud af, ikke også.

Studerende 2: Hvad betyder det, at der er problemer med krypteringen?

Thy: Jamen det betyder jo i sidste ende, at rigtig mange har faktisk mulighed for at sende oplysninger, besidde oplysninger, uden at vi nogensinde kan komme i nærheden af dem, og det er da en stor udfordring."

I ovenstående uddrag fra interviewet med Nordjyllands Politi bliver der spurgt ind til, om noget er forstået korrekt, hvilket informanten tilkendegiver, men samtidig bliver informanten også bedt om at uddybe et af sine svar, således en tvetydighed bliver elimineret. Samtidig viser eksemplet, hvordan vi har suppleret hinanden gennem interviewprocessen for at sikre, at den empiri, vi indhentede, var af en høj kvalitet.

Gennem databehandlingen har vi løbende italesat og diskuteret informanternes svar. Det gjorde vi især under meningskondenseringen og -kategoriseringen, hvor vi arbejdede sammen om hvert enkelt interview for at sikre os, at alle var enige i fortolkningen af informanternes svar. Da vi har haft fem ekspertinterviews, har det været muligt at sammenligne informanternes svar, hvilket øger kvaliteten, fordi det øger chancen for, at den viden, vi opnår, er korrekt. På samme måde har vi gennemarbejdet analysen for fejl, overdrivelser og diskrepanser. Ifølge Tanggaard og Brinkmann (2010, s. 493) styrker det troværdigheden at sammenligne resultaterne fra analysen med den videnskabelige litteratur, hvilket vi også har gjort flere steder.

Specialet kunne med fordel suppleres af en netnografisk undersøgelse, der er et etnografistudie på internettet eksempelvis på et forum på det mørke internet. Denne kunne supplere den nuværende analyse, hvilket havde haft flere fordele. For det første havde det betydet, at vi havde opnået en anden type af data end den, som vi fik gennem interviewene. Det ville have skabt muligheden for at belyse gerningsmændenes perspektiv og sammenligne dette med empirien fra interviewene. Vi ville derfor have opnået en triangulering gennem forskellige metoder til at indsamle empiri. Hvis empirien fra interviewene og netnografien understøttede hinanden, ville kvaliteten af specialet stige, fordi den indsamlede viden ville være mere sikker (Bryman, 2012, s. 392). En netnografisk undersøgelse ville også supplere aktør-netværksteorien som analyseredskab, fordi vi gennem den netnografiske undersøgelse ville have haft mulighed for at belyse en anden del af phishingnetværket. Denne type undersøgelse er dog meget tidskrævende, hvorfor det ikke var muligt at inddrage den i specialet sideløbende med de øvrige metoder.

6. Analyse

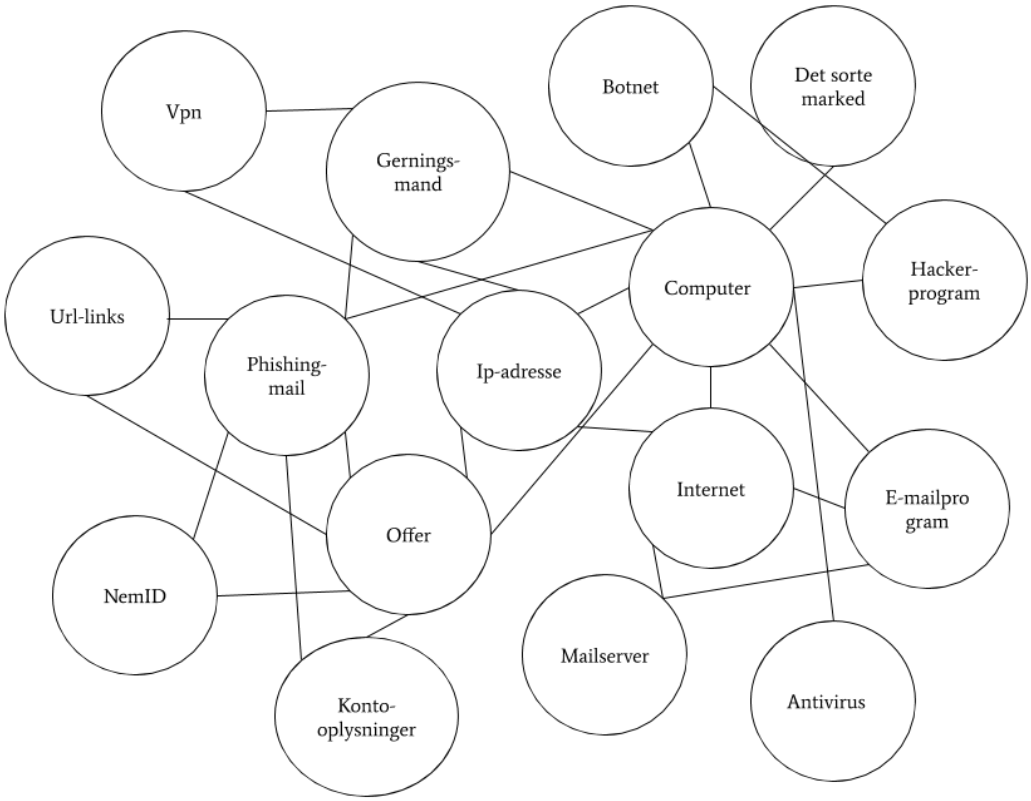
I dette afsnit analyseres empirien fra de fem afholdte interviews for at undersøge, hvilke udfordringer der er ved at bekæmpe phishing i Danmark. Analysen tager afsæt i ANT ved at identificere aktører og kortlægge de netværk, hvor phishingangrebet udføres, og hvor phishing efterforskes af politiet. Her anvendes Callons translationsproces som analyseredskab til at undersøge, hvordan aktørerne forhandler med hinanden. Løbende inddrages kriminologiske teorier og deres forklaringer på, at en kriminalitetsform som phishing opstår.

6.1 Phishingangreb som et netværk

For at få et indblik i udfordringerne ved bekæmpelse af phishing benyttes ANT til at afdække, hvilke aktører phishingangrebet som et netværk udgøres af. For at opnå en forståelse for hvilke udfordringer phishing som aktør skaber, når det indgår i andre netværk, er det relevant at beskue, hvilke aktører der indgår i en translationsproces, når et vellykket phishingangreb finder sted.

6.1.1 Aktører i phishingnetværket

I phishingnetværket interagerer flere forskellige aktører med hinanden, som illustreret på følgende figur:



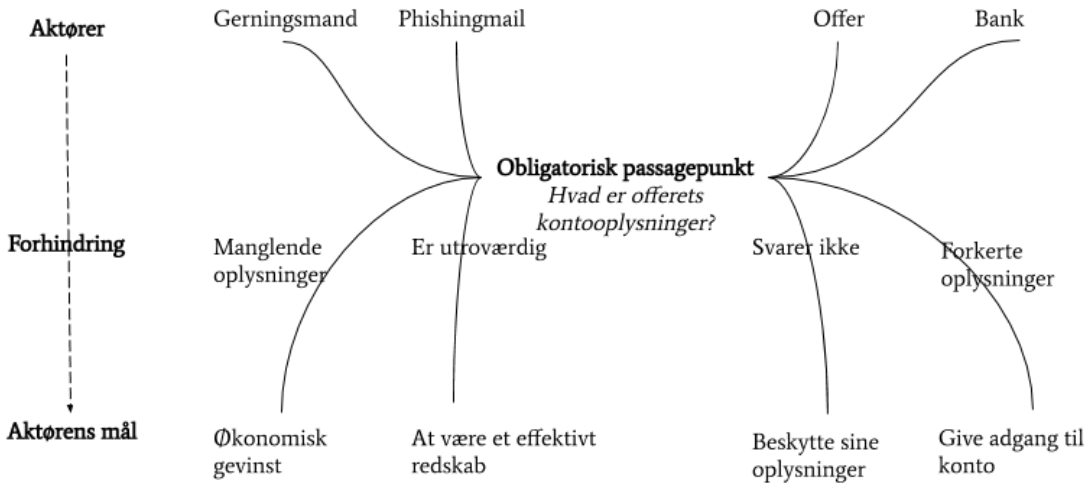
Figur 3: Phishing illustreret som et netværk

Figuren illustrerer et klassisk ANT-netværk, hvor aktørerne interagerer med hinanden på kryds og tværs. Der er ikke én aktør, der er centrum i netværket, men de er alle med til at opbygge og påvirke netværket som helhed. Phishingnetværkets kompleksitet afhænger af, hvilke aktører der indgår i det. Som kriminologiprofessor Peter Kruize nævner, kan en gerningsmand benytte sig af flere forskellige aktører: *"(...) man kan række så bredt, som eksempelvis at kunne sende en million phishingmails, eller man kan bruge et botnet til at lægge hjemmesider ned og afpresse dem på den måde."*. Phishingnetværket ændres altså afhængig af, om gerningsmanden sender én eller en million phishingmails, og om han benytter et botnet. Gerningsmanden bag et phishingangreb er som udgangspunkt altid økonomisk motiveret. Faglig koordinator og it-efterforsker hos Nordjyllands Politi, Søren Nielsen, påpeger: *"Altså formålet med meget kriminalitet er jo at få penge. Så i et eller andet... et eller andet form, som regel et eller andet økonomisk islæt"*. Som oftest er det derfor kontooplysninger eller personlige oplysninger, der kan videresælges, som gerningsmanden går efter, og disse indgår derfor også i netværket. Udover gerningsmanden

er computeren også en relevant aktør, når en phishingmail skal sendes. Det er gældende for både gerningsmandens og offerets computer, som interagerer med hinanden i netværket. Phishingmailen er endnu en relevant aktør, som har til formål at skabe tillid eller på anden vis manipulere offeret til at videregive sine oplysninger.

6.1.2 Et phishingangreb som translationsproces

Når et phishingangreb udføres, er dette en translationsproces, som involverer nogle af aktørerne i phishingnetværket. Gerningsmanden kan udgive sig for at være fra Nets eller offerets bank, hvor phishingmailen indeholder en advarsel om, at offerets konto vil blive lukket, hvis ikke vedkommende sender sine kontooplysninger retur. De relevante aktører i translationsprocessen er gerningsmanden, banken, phishingmailen og offeret. Det fælles mål kaldes *det obligatoriske passagepunkt,* og det er et punkt, alle aktørerne skal samarbejde om at komme igennem for hver især at nå deres endelige mål. Incitamentet til at indgå i translationsprocessen er derfor, at passagepunktet er obligatorisk for, at aktørerne undgår deres *forhindring* og opnår deres individuelle mål. Det obligatoriske passagepunkt er en del af det første trin i Callons (1984 s. 203) translationsproces, som hedder *problematisering*, og vil i denne translationsproces være: *Hvad er offerets kontooplysninger?* Gerningsmanden er den aktør, der gør sig uundværlig og definerer det obligatoriske passagepunkt, da han er interesseret i at få offerets kontooplysninger. Ved hjælp af virkemidler i phishingmailen forsøger han at overbevise offeret om, at det er til vedkommendes fordel, at mailens instruktioner følges.



Figur 4: Et eksempel på et phishingangreb som en translationsproces

På ovenstående figur illustreres det andet trin i Callons (1984, s. 206-207) translationsproces, *interessement*. Her identificeres de forskellige aktørers endelige mål og dermed deres interesse i at indgå i translationsprocessen. Offeret har som mål at beskytte sine oplysninger og kan derfor være villig til at indgå i translationsprocessen. Det er dog under forudsætning af, at offeret snydes af phishingmailen og tror, den er legitim. Offeret manipuleres på den måde til at indgå i en translationsproces, som vedkommende tror vil sikre kontoen[1]. Gerningsmandens endelige mål er at opnå økonomisk gevinst ved at sende phishingmailen, mens phishingmailens endelige mål er at være et effektivt redskab for gerningsmanden. Banken agerer facilitator og har derfor som mål at give adgang til deres kunders konti, hvis de korrekte informationer gives.

De forskellige aktører forhandler med hinanden på det tredje trin i Callons (1984, s. 211) translationsproces, *indrulning*. Eksempelvis forhandler phishingmailen med offeret ved at virke troværdig for at få adgang til kontooplysningerne, som it-sikkerhedschef Torbjørn Bonde-Jensen nævner, prøver phishingmailen at fremprovokere en følelsesmæssig respons: *"(…) der prøver [de] at få den her følelsesmæssige reaktion frem i modtageren, hvor de så*

[1] Callons translationsproces tager ikke højde for aktørernes bagvedliggende motivation, og derfor nævnes manipulation ikke i selve teorien

ligesom sænker paraderne lidt.". Hvis virkemidlerne i mailen er stærke nok, kan forhandlingen lykkes. Offeret tror på dette tidspunkt, at vedkommende har nået sit mål om at beskytte sine oplysninger, men er i virkeligheden blevet manipuleret i processen. Det sidste trin i Callons (1984, s. 214) translationsproces er *mobilisering*. Når offeret åbner phishingmailen, er denne talsmand for gerningsmanden og forsøger at snyde offeret ved hjælp af de metoder og virkemidler, gerningsmanden har inskriberet i den. Såfremt translationsprocessen gennemføres, uden at aktørerne forhindres, vil phishingangrebet være succesfuldt, og gerningsmanden vil være i besiddelse af offerets oplysninger.

Et eksempel på en phishingmail

Som nævnt er formålet med en phishingmail at virke tillidsvækkende for at få offeret til at udlevere sine personlige oplysninger. Informanterne har givet flere eksempler på, hvordan disse mails udformes, og hvad phisherne skriver for at få offeret til at opgive sine oplysninger.

Fra: NETS Kundeservice <Kundeservice@Netsdenmarkeu.onmicrosoft.com>
Dato: 29. jun. 2015 kl. 04.47.19 CEST
Til: "Kundeservicenets@outlook.com" <Kundeservicenets@outlook.com>
Emne: NETS: opdatering N1729203.

nets

Hello kunde

Din konto Nets er suspenderet, fordi vi opdager et problem på din konto.

Vi afgør, at nogen kan bruge din konto uden din tilladelse. Til din beskyttelse, har vi suspenderet din konto. For at løfte denne ophænget

Klik her
og følg proceduren for at angive at opdatere din konto

Bemærk: Hvis dette ikke er løst i de næste 48 timer vil vi blive tvunget til at indstille dit kort på ubestemt tid, fordi det kan bruges til svigagtige

Tak for dit samarbejde i forbindelse med denne sag.

Tak,

Billede 1: Eksempel på phishingmail (Nets A/S, 2019)

Nets fremhæver ovenstående eksempel på en phishingmail på deres hjemmeside med henblik på at oplyse borgerne om, hvordan phishingmails kan se ud. I phishingmailen står der, at offeret er suspenderet fra sin Nets-konto og har 48 timer til at give sine oplysninger, ellers vil kortet blive indstillet. Det er et eksempel på, hvordan phisherne bruger social engineering til at manipulere ofrene. It-sikkerhedschefen uddyber i den forbindelse:

"(…) i beskrivelsen af social engineering så handler det om ligesom at eje nogle psykologiske prespunkter, hvor man ved, at folk reagerer, så det enten er godt for dem eller skidt for dem. (…) Det er jo sådan noget, der får mennesker til at følelsesmæssigt at handle, før de ligesom forholder sig."

Dog kan det ses, at mailen ikke er skrevet på korrekt dansk, når de eksempelvis skriver "For at løfte denne ophænget". Kriminologiprofessoren forklarer, at det er et typisk kendetegn på en phishingmail: *"I Danmark og Holland kunne man sagtens se, at det var en som ikke magtede sproget og bare havde brugt Google Oversæt, og så var det ret nemt at gennemskue."* Eksemplet indeholder også andre typiske kendetegn ved en phishingmail. It-ingeniøren Nicolai Larsen fra NC3 forklarer, at mailen ofte opfordrer modtageren til at klikke på et link, som fører hen til en falsk hjemmeside, hvor vedkommende skal indtaste sine oplysninger. På ovenstående eksempel fremgår det, at afsenderen prøver at få offeret til at klikke på et link, som sandsynligvis fører hen til en hjemmeside, phisherne har oprettet. De kan oprette en hjemmeside, som minder om den organisation, de udgiver sig for at komme fra for at virke tillidsvækkende.

It-sikkerhedschefen fortæller, at phisherne sender mails fra en mailadresse, som også skal virke troværdig: *"(…) de registrerer et domæne, som minder om. Så er der en ekstra bindestreg eller et ekstra tal eller et L er udskiftet med et et-tal."*. Det kan også ses på Billede 1, hvor phisherne har forsøgt at efterligne Nets' Kundeservices mailadresse. Det mest iøjnefaldende ved phishingmailen er dog, at den kommer fra Nets, mens ordlyden i mailen tyder på, at den kommer fra en bank. Det kunne være et tegn på, at phisheren ikke har sat sig ind i, hvilken type organisation Nets er.

6.1.3 Udfordring med phishing som organiseret kriminalitet

Phishing er en lukrativ måde at opnå økonomisk gevinst på, og som tidligere nævnt forekommer opdagelsesrisikoen ved it-kriminalitet ofte meget lav. Kriminologiprofessor Peter Kruize forklarer i den forbindelse, at flere kriminelle overgår fra konventionelle kriminalitetsformer til it-kriminalitet: *"(…) vi kan også se via undersøgelser, at der er overlap mellem dem, der begår traditionel kriminalitet og internetkriminalitet og mere organiseret form for kriminalitet, at de også bruger internet mere og mere (…)"*. Flere kriminelle begynder altså at begå it-kriminalitet frem for traditionel kriminalitet.

Det sorte marked

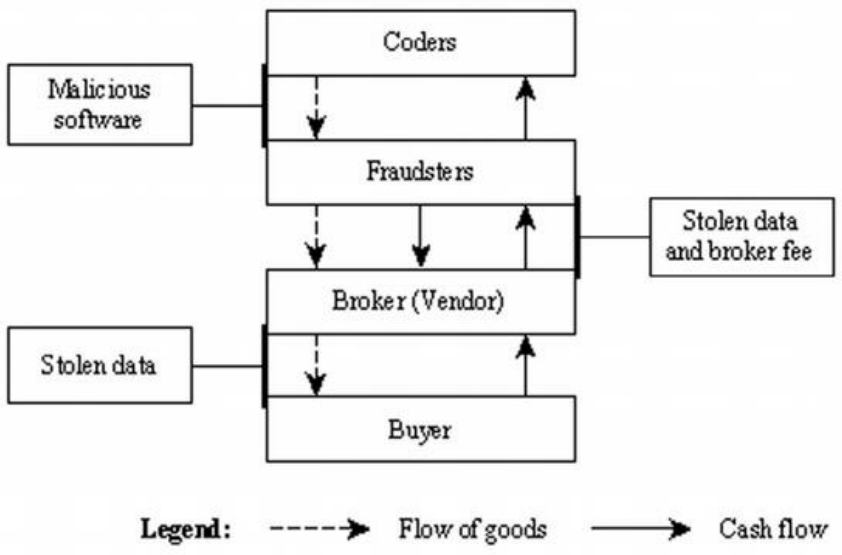
Det sorte marked anvendes af gerningsmænd til at købe og videresælge ofrenes oplysninger. Nye teknologiske aktører er på den måde blevet introduceret og giver flere muligheder for kriminel aktivitet, mens gerningsmændene har en lavere risiko for at blive opdaget og straffet for deres handlinger, da det foregår på det mørke internet, hvor det er svært at finde frem til dem. It-ingeniøren Nicolai Larsen fra NC3 fortæller, at it-kriminalitet og handel med oplysninger foregår meget organiseret:

"(…) dem der laver phishing ved at samle data ind er jo et arbejdsområde for sig selv (…) en, der har haft specialiseret sig i at phishe folk for at samle informationer, men så bruger han ikke de her oplysninger til andet end at sælge dem til andre kriminelle, der så bruger dem til direkte kriminelle aktiviteter."

Phisherne indsamler altså værdifulde informationer, som de videresælger på det sorte marked. Køberne af disse informationer kan så benytte dem til at opnå økonomisk gevinst. I phishingnetværket eksisterer det sorte marked som en aktør, men det sorte marked er også selv et netværk, hvor forskellige kriminelle aktører indgår og forhandler med hinanden.

Det sorte marked er knudepunktet for de kriminelle forhandlinger mellem forskellige aktører og er derfor en vigtig del af phishingnetværket, hvor kriminelle kan handle anonymt med hinanden gennem krypterede forbindelser på det mørke internet. Det gør det til en udfordring at efterforske og optrævle de kriminelle netværk. At informationer

bliver phishet, solgt og først senere bliver brugt til handlinger, der medfører et økonomisk tab hos offeret, er én af årsagerne til, at phishing er en udfordring at efterforske, da der kan gå flere måneder mellem, at offeret er blevet phishet, til de opdager, at de har mistet deres informationer. En anden årsag er, at de egentlige gerningsmænd bag phishing er svære at finde frem til, da det ikke altid er dem, der benytter den stjålne information, men blot videresælger den til andre. Konradt et al. (2016) har undersøgt phishingnetværket, og hvordan handlen med stjålne data fungerer. I den forbindelse har de identificeret fire aktører, som er til stede på det sorte marked som netværk og som handler med hinanden:



Figur 5: Illustration af organiseret phishing (Konradt et al., 2016, s. 41)

Som det fremgår af figuren, er disse aktører *koderen*, *svindleren*, *mægleren* og *køberen*. Fra et ANT-perspektiv er dataet også en aktør, som skal være til stede, før forhandlingerne i netværket kan foregå. Som vist på figuren foregår der nedad i systemet en overførsel af software fra koderen til svindleren samt salg af data i form af eksempelvis person- eller kontooplysninger mellem svindleren, mægleren og køberen. Salget medfører en pengestrøm tilbage i systemet. Det viser, hvordan data er værdifuldt på det sorte marked og kan medføre stor økonomisk gevinst for gerningsmændene, som it-ingeniøren fra NC3 også pointerer: *"(...) når data er helt nye, så er det jo de ypperste kriminelle, der har adgang til data her, fordi der er prisen jo høj for nye data."*. I en rapport fra it-sikkerhedsfirmaet

Armor (2018, s. 7+9) oplyser de, at prislejet på kreditoplysninger ligger på 300-400 kroner, mens personlige oplysninger ligger på 3000-5000 kroner. Koderen er en person med teknologiske kompetencer, som eksempelvis programmerer en falsk hjemmeside eller skadelige filer, som skal snyde brugeren. Koderen kan således hyres af flere forskellige bagmænd og indgå i forskellige netværk. Svindleren er det næste led i kæden, som udformer phishingmailen med linket til den falske hjemmeside og sender den til ofrene. Svindlerne forhandler også med en mægler, som køber og videresælger data. I et ANT-perspektiv kan mægleren dog også være en ikke-menneskelig aktør som eksempelvis det sorte marked, som blot fungerer som en platform, hvorpå køber og sælger kan mødes. It-ingeniøren fortæller, at nogle bagmænd driver organiseret phishing som en ganske almindelig virksomhed, som han har set eksempler på i Nigeria og Israel:

"De hyrer simpelthen folk til at komme ind. De har sådan nogle lister. Lidt ligesom telemarketing (...) Så møder de ind om morgenen, de får en liste over de der oplysninger, de nu har, så kontakter de folk, og hvis de får bid, så sender de dem op til nogle, der er teknisk lidt mere kyndige, der så kan guide eller vejlede folk lidt bedre. Så det er virkelig organiseret som en helt almindelig virksomhed."

De organiserede kriminelle har været nødt til at introducere nye teknologisk kyndige aktører i det kriminelle netværk. Det viser også udfordringen med at finde frem til de egentlige bagmænd, da efterforskerne ofte kun finder frem til stråmændene, som udfører angrebene, ifølge it-efterforsker Jesper Thy fra Nordjyllands Politi: *"(...) hvis vi eventuelt får ham identificeret, så er det ikke nødvendigvis ham, der har lavet det her. Så er han et muldyr, der skal tage imod pengene og udlevere dem til nogle andre (...)".* For efterforskerne kan det altså være en udfordring at bekæmpe phishing, da det er organiseret således, at det er svært at finde frem til de egentlige bagmænd, som derfor ikke bliver retsforfulgt. Birk et al. (2007) argumenterer for, at der kan arbejdes proaktivt mod de sorte markeder ved at sende falske informationer til phisherne, som kan spores for at kunne finde frem til de egentlige bagmænd. Konradt et al. (2016) påpeger, at en mere effektiv metode til bekæmpelse af phishing er bedre kontrol af de sorte markeder og ikke nødvendigvis strengere straffe. I forlængelse af Cesare Beccarias klassiske kriminologi findes *afskrækkelsesteorien*, som handler om, at der findes to måder at afholde folk for at begå

kriminalitet: *specifik afskrækkelse* og *generel afskrækkelse*. Den specifikke afskrækkelse omhandler, om gerningsmanden selv oplever at blive straffet for sin kriminalitet. Den generelle afskrækkelse handler om, om gerningsmænd i samfundet generelt straffes for den type kriminalitet. Med udgangspunkt i teorien betyder det, at det skal være mere *sikkert*, at kriminelle straffes, hvilket ifølge teorien har en mere afskrækkende effekt end straffens *strenghed* (Stafford og Warr, 2014, s. 434).

6.2 Forskydning i tid og rum

Forskydningen i tid og rum er et element ved it-kriminalitet, der gør kriminalitetsformen særligt svær at bekæmpe - ikke kun i Danmark, men i hele verden. Når en gerningsmand sender en phishingmail, kan det foregå ét sted i verden, mens offeret modtager denne mail et helt andet sted i verden, og der kan være en stor forskydning i tiden, da der kan gå lang tid fra påbegyndelsen af angrebet, til der opstår et økonomisk tab. Det, forklarer it-ingeniøren fra NC3, kan give problemer i forhold til opklaringen, da det kan være svært for offeret at kæde de to hændelser sammen og give en kvalitativ anmeldelse:

"Når man skal finde ud af, hvad der egentlig er sket (…) det har folk slet ikke overblik over, så derfor så kan de godt stå i sådan en situation, at de bare ikke kan give en kvalitativ anmeldelse, fordi de ikke selv er klar over det."

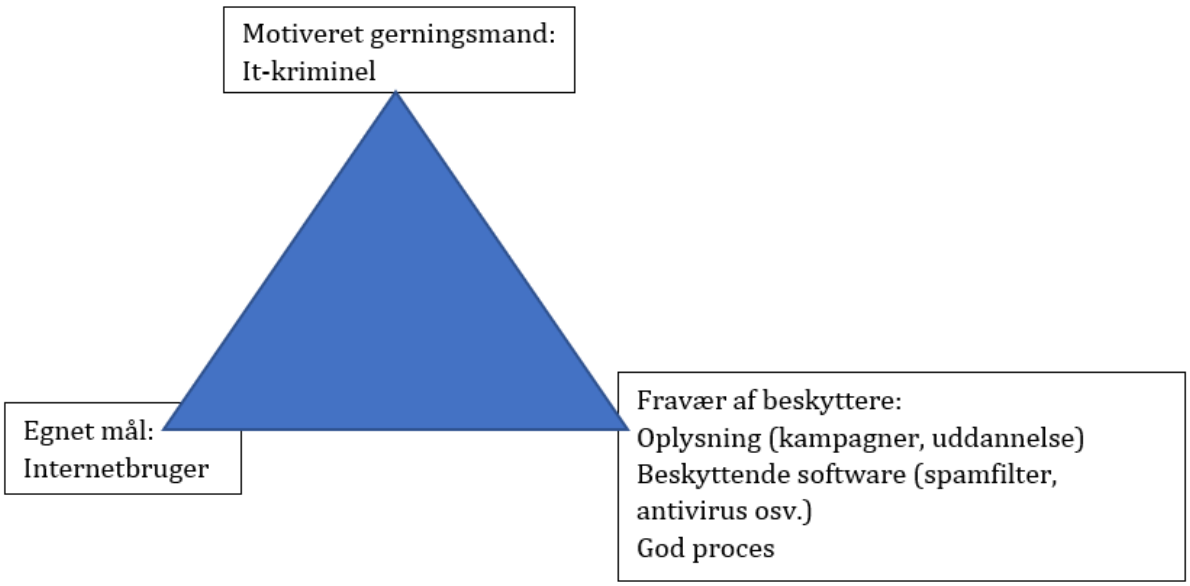
For politiet betyder det, at anmeldelserne kan være mangelfulde, fordi ofrene ikke har overblik over, hvad der er sket. Det besværliggør bekæmpelsen af it-kriminalitet for politiet, da en anmeldelse med kun meget få detaljer er svær at efterforske og opklare, og gerningsmanden kan derfor fortsætte sine angreb.

Forskydningen i tid og rum er et perspektiv, der er centralt i meget forskning om it-kriminalitet. Det er et af de elementer, der skaber uenighed blandt forskerne om, hvorvidt klassiske kriminologiske teorier har forklaringskraft, når det kommer til it-kriminalitet. Rutineaktivitetsteorien er en teori om situationel kriminalitetsforebyggelse, som beskriver, at der findes tre forudsætninger for, at kriminalitet opstår: En motiveret gerningsmand, et egnet mål og fravær af beskyttere. Disse forudsætninger skal findes på samme tid og sted, og derfor er det muligt at forebygge kriminalitet ved at forhindre, at situationen opstår

(Cohen og Felson, 2014, s. 470). Rutineaktivitetsteorien er anvendt af blandt andre Grabosky (2016) og Reyns og Henson (2015) til at forklare kriminalitet på internettet, hvor motiverede gerningsmænd, egnede ofre og fravær af beskyttere eksisterer samtidig. Den tilgang til begrænsningen af it-kriminalitet kan relateres til it-sikkerhedschefens udtalelse om, at der er tre faktorer, der skal prioriteres, når it-kriminalitet skal forebygges: *"der er ligesom tre områder, man skal have prioriteret. Det er det menneskelige, proces og teknologi, og der, kan man sige, at hvis man ligesom ikke får adresseret alle tre, jamen så vil der være et hul i kæden (...)"*.

De menneskelige, proceslige og teknologiske parametre er altså tre måder at forebygge kriminalitet på. Det menneskelige kan være personers dømmekraft, når de modtager en phishingmail: *"de skal have nogle ressourcer for det første, og så skal de have visse kompetencer."*. De menneskelige kompetencer kan derfor forbedres ved uddannelse eller oplysningskampagner, så det bliver sværere at snyde personerne. Den proceslige faktor kan indebære en god proces for, hvad man stiller op, når man modtager en phishingmail, som it-sikkerhedschefen forklarer: "*(...) en styring af, hvordan man samarbejder, og hvad skal man gøre, hvis der sker noget*" - altså med andre ord hvordan man forholder sig, hvis man oplever forsøg på phishing. Den teknologiske forebyggelse kan være i form af software og teknologiske hjælpemidler, der advarer brugeren om mulige it-trusler.

Med udgangspunkt i rutineaktivitetsteorien kan it-sikkerhedschefens fokus på menneskelige, proceslige og teknologiske foranstaltninger ses som et udtryk for at sikre tilstedeværelsen af beskyttere, så alle tre forudsætninger for kriminalitet ikke opstår. Derved deler han teoriens opfattelse af, at kriminalitet kan forebygges situationelt. I rutineaktivitetsteorien er den motiverede gerningsmand ikke i fokus, og det er derfor de to andre forudsætninger for kriminaliteten, der må forhindres. Et fravær af beskyttere vil i forbindelse med it-kriminalitet betyde, at borgerne ikke er veloplyste, eller at de ikke har teknologisk beskyttelse mod phishingmails.



Figur 6: Kriminalitetstrekanten illustreret med it-kriminalitet

Ovenstående figur viser kriminalitetstrekanten med de tre forudsætninger for, at en kriminel handling finder sted. Ud fra dette perspektiv er det muligt at forhindre it-kriminalitet, hvis der er beskyttere til stede i form af oplysning, beskyttende software og en god proces, som it-sikkerhedschefen udtaler. Fra et ANT-synspunkt relaterer det sig til forståelsen af it-kriminalitet som et netværk udgjort af en række aktører. De tilstedeværende aktører har betydning for netværket, hvilket vil sige, at beskytternes tilstedeværelse har den konsekvens, at phishingangrebet ikke lykkes. Rutineaktivitetsteorien har derfor flere ligheder med ANTs netværksorienterede tilgang til kriminalitet som en dynamik mellem aktører. ANT har dog ikke en fast dimension af tid til at definere aktørernes tilstedeværelse eller fravær af hinanden. Latour (1996) forklarer, at en af fordelene ved at tænke i netværk er opsplittelsen af begrebet distance, da geografiske barrierer ikke er definerende for aktørernes evne til at påvirke hinanden, fordi deres associationer er ikke bundne af tid og sted. Rutineaktivitetsteorien og ANT deler på den måde opfattelse af netværk, men har forskellige opfattelser af tid og rum.

Reyns og Henson (2015) har også undersøgt it-kriminalitet med udgangspunkt i rutineaktivitetsteorien, men de er af en anden opfattelse end it-sikkerhedschefen. De mener ikke, beskyttere såsom antivirus er af afgørende betydning for, om man i sidste ende bliver offer for it-kriminalitet. Offerets aktivitet på internettet, såsom at handle på nettet eller

oplyse personlig information online, har dog stor betydning for, hvor egnet et mål vedkommende udgør. Reyns og Henson har i deres undersøgelse fokus på risikoen for at blive udsat for identitetstyveri og undersøger derfor ikke risikoen for at blive phishet. Dette undersøger Leukfeldt (2014), som dog mener, at offerets internetaktivitet kun har en minimal indvirkning på risikoen for at blive phishet, og at alle er potentielle mål for phishing, uanset hvordan de agerer på internettet. Han argumenterer for, at resultaterne ikke er overraskende, da phishing ofte sendes ud til en meget bred målgruppe af mennesker i form af spam.

Som tidligere belyst er der en igangværende diskussion om klassiske kriminologiske teoriers forklaringskraft på it-kriminalitet. Herunder er der uenighed om rutineaktivitetsteoriens anvendelse i forbindelse med it-kriminalitet. Yar (2005) er en af de forskere, der ikke mener, den kan anvendes på it-kriminalitet. Hans kritik går på, at teoriens forklaring af kriminalitet især beror på en stabil tid-rum-sammensætning, hvor de tre forudsætninger for kriminalitet skal være til stede i samme tid og rum. It-ingeniøren fra NC3 nævner, at en af udfordringerne ved it-kriminalitet er, at lande- og kredsgrænser ikke kan overføres til en effektiv bekæmpelse af it-kriminalitet: *"den går jo på tværs af alle landegrænser, og den er jo også fuldstændig ligeglad med kredsgrænser, så kredsgrænserne er jo effektive i forhold til lokalt og fysisk kriminalitet, men ikke forhold til it-kriminalitet (...)".* Det relaterer sig til Yars (2005) kritik af rutineaktivitetsteorien, som er, at den kun kan bruges på it-kriminalitet, hvis cyberspace har en rumlig opbygning lignende den fysiske verden, hvor tid, sted og distance kan identificeres. Han mener, cyberspace er anti-rumligt, og det er et sted, hvor der er nul distance mellem de forskellige punkter, da alt bare er et klik væk. Derfor er de geografiske barrierer, som kan forhindre interaktion i den fysiske verden, brudt. Her bliver teoriens forklaringer tvivlsomme, fordi den er afhængig af aktørers tilstedeværelse eller fravær af hinanden. Hvis alle objekter og personer er til stede samtidig, hvordan er det så meningsfuldt, at tilstedeværelsen af en gerningsmand er kriteriet for kriminalitet?

Kriminologiprofessoren Peter Kruize mener, it-kriminalitet i en vis udstrækning skal betragtes som et nyt fænomen: *"(...) det er et nyt fænomen, da der er opstået nye former for kriminalitet, som ikke fandtes før internettet. Men jeg vil sige, at langt den overvejende*

del er klassisk kriminalitet, som har fået ny jakke på." Han læner sig dog op ad Yars (2005) opfattelse af, at den flydende tid- og rumdimension er en udfordring for de klassiske teorier:

"(…) Til en vis udstrækning vil man kunne bruge klassisk teori, men som du også selv var inde på, så er der noget særligt ved internetkriminalitet (…) du kan udføre it-kriminalitet fra et sted i Asien, mens målet er i Danmark. Så geografi og tid og den mængde, man kan nå, gør det helt specielt. Jeg vil heller ikke sige, at det ikke har en indflydelse på den teori, man nu anvender (…) Jeg tror i hvert fald, vi har brug for en fornyelse af kriminologiske teorier, som muligvis godt kan tage afsæt i de klassiske kriminologiske teorier."

Det flydende tid- og rumperspektiv er dog uanset hvad en udfordring for politiets arbejde i praksis, og netop fraværet af et stabilt tid og rum for den kriminelle handling er et af de elementer, gerningsmændene kan udnytte, når internettet anvendes som platform for kriminelle aktiviteter.

6.3 Internettet er kriminalitetsfremkaldende

Som beskrevet i problemfeltet er internettet en attraktiv platform til kriminel adfærd, hvilket skyldes flere forskellige faktorer, herunder internettets struktur, og de muligheder fraværet af stabilt tid og rum skaber.

It-ingeniøren fra NC3 udtaler om internettet, at: "(…) *det er jo meget anarkistisk, internettet, fordi du kan jo gøre, hvad du vil."*, hvilket betyder, at der på internettet er et fravær af styring, kontrol og orden (Ordnet, 2019). Udover at internettet er anarkistisk af natur, så udtaler it-sikkerhedschefen, at: "(…) *på den tekniske side, der har vi jo internettet, som aldrig har været designet i sin oprindelige tanke til hverken at være privat eller sikkert, fordi det var ligesom ikke det, der var designtankerne*.".

Internettets iboende anarki, samt at det ikke er designet til at være sikkert og privat, betyder, at det er en attraktiv platform at begå kriminalitet på. Jaishankar (2008a) fremlægger i space transition theory syv påstande om, hvilke faktorer der kan have betydning for, at kriminalitet opstår på cyberspace. Ifølge teorien er individer med en undertrykt kriminel adfærd tilbøjelige til at begå kriminalitet på internettet. Denne

kriminelle adfærd ville individerne ikke udleve i den fysiske verden af frygt for at miste deres status eller position i samfundet. Det synspunkt kan sammenlignes med Travis Hirschis (2014, s. 231) kriminologiske teori om *social bonds*, hvor sociale bånd afholder individet fra at begå kriminalitet. Ifølge space transition theory skyldes tilbøjeligheden til at begå kriminalitet på internettet blandt andet det faktum, at det er muligt at være anonym (Jaishankar, 2008a, s. 7). It-ingeniøren udtaler vedrørende anonymiteten på internettet:

"*(…) du skal jo ikke vise pas eller anden id for at oprette en e-mail. Og du har heller ikke sådan et, altså ligesom vi har cpr-numre i Danmark til at identificere os selv, hvis vi bliver stoppet eller et eller andet, det er der jo heller ikke på internettet.*"

Ifølge space transition theorys anden påstand betyder internettets anonyme og anarkistiske natur, at det for de kriminelle er attraktivt at begå kriminalitet på internettet. Jaishankar (2008a, s. 7) mener, at en af de faktorer i samfundet, der gør, at folk generelt ikke er kriminelle, er skrækken for afstraffelse. Denne faktor er stort set fraværende på cyberspace, fordi internettet tillader gerningsmænd at angribe deres ofre med lav opdagelsesrisiko. It-ingeniøren udtaler også at:

"*(…) de kriminelle [vil] i stigende grad være digitale, og den digitale kriminalitet vil også stige i høj grad. Og man kan sige det (…) som alle i branchen, de ser nu, det er, altså de kriminelle er jo dovne ligesom alle andre. De vil gerne have mest muligt ud af mindst, eller mest ud af mindst muligt arbejde.*"

De kriminelle vil altså have en stigende tendens til at begå it-kriminalitet, fordi de på internettet kan få mest muligt udbytte ud af mindst muligt arbejde. Den adfærd kan belyses ud fra den kriminologiske teori *rational choice*, som beskriver, at gerningsmænd prøver at maksimere glæde og minimere smerte. Ud fra dette synspunkt vælger personer at begå kriminalitet, fordi de tror, at det er til deres fordel (Cornish og Clarke, 2014, s. 437). Kriminelle vælger altså at begå it-kriminalitet frem for analog kriminalitet, fordi det opfattes som mindre risikabelt at begå kriminalitet på internettet grundet dets anarkistiske og anonyme struktur, og derfor er opdagelsesrisikoen mindre. Incitamentet for at begå it-

kriminalitet er også større, fordi internettet har en stor pulje af potentielle ofre, som kan udnyttes til økonomisk gevinst for gerningsmanden.

Udover rational choice kan afskrækkelsesteorien anvendes til at forklare, hvorfor internettet er et ideelt sted at begå kriminalitet. It-ingeniøren fra NC3 udtaler: *"Men vi efterforsker alle sager, men nogle sager har jo bare et naturligt stop, for eksempel hvis det er en vpn-tjeneste i Rusland eller i Kina (…)"*.

Han beskriver, hvordan en vpn kan besværliggøre efterforskningen ved at skjule brugerens ip-adresse og dermed minimere chancen for retsforfølgelse. En ip-adresse er et unikt nummer, som computere har og bruger til at kommunikere med hinanden. Den kan sammenlignes med et vejnavn og -nummer og kan bruges til at identificere computeren. Ip-adressen bliver logget, når man færdes online, men ved at bruge en vpn kan brugeren maskere sin aktivitet. Brugerens egen ip-adresse forbliver skjult og erstattes af ip-adressen på den vpn-server, vedkommende tilkobler sig. Vpn er derfor en teknik, der ofte anvendes af kriminelle, så deres ip-adresse ikke kan anvendes som identifikationsmetode. Hvis det danske politi ikke straffer it-kriminelle, så afskrækker det ikke gerningsmændene. Der sker hverken en specifik afskrækkelse, fordi den specifikke gerningsmand ikke bliver straffet, eller en generel afskrækkelse, fordi andre it-kriminelle i samfundet heller ikke bliver straffet.

6.3.1 Regulering af internettet

Som belyst i det ovenstående er der en række faktorer, som gør internettet attraktivt til kriminel adfærd. En af disse er, at internettet er anarkistisk og derfor ikke reguleret. Ved at øge reguleringen af internettet og gøre det mindre konsekvensfrit at lave it-kriminalitet, ville det være mindre attraktivt. Der er dog et problem med at gøre dette, hvilket it-ingeniøren fra NC3 forklarer: *"(…) hele infrastrukturen gør jo, at vi er med suveræne grænser, landegrænser og opdeling af suverænitet og alt muligt, den eksisterer slet ikke på internettet."*.

Udover at internettet besidder en anarkistisk natur, så er det også struktureret anderledes end den fysiske verden, da der ikke findes fysiske grænser på internettet. Juraprofessoren

Birgit Feldtmann kommer med et eksempel på denne forskel ved at beskrive forskellen på lovgivningen i Tyskland og Danmark: *"(…) i Tyskland er det forbudt at sige, at holocaust ikke har fundet sted, og det har jo historiske grunde. I Danmark er det ikke kriminaliseret. Og her har der været nogle højreorienterede tyskere, som driver deres hjemmesider fra Danmark."*.

At der ikke eksisterer grænser på internettet på samme måde, som der gør i den fysiske verden, betyder, at det er kompliceret at regulere. Hvis internettet blev reguleret på samme måde som den fysiske verden, ville det sandsynligvis gøre det mindre attraktivt. It-ingeniøren beskriver en mulig regulering af internettet:

"*(…) Det kan godt være, at man siger, at jamen for at oprette en Gmail der skal du sende et gyldigt pas, men der findes jo lige så mange forskellige pas, som der findes lande, og hvem skal så tjekke, om passet er ægte og alle de her ting (…)*"

En mulighed ville være at kræve identifikation, hver gang brugeren benytter internettet, men det er en udfordring at afgøre, hvem der skulle have til opgave at håndhæve denne regulering. Denne form for identitetskontrol ville potentielt kunne øge mængden af phishingangreb, da værdien af personfølsomme oplysninger vil stige på det sorte marked og dermed gøre handlen med disse mere lukrativ.

6.3.2 Sikkerhed på bekostning af brugervenlighed

Som beskrevet tidligere var sikkerhed ikke en del af internettets oprindelige design, hvilket it-kriminelle kan udnytte. En udfordring er derfor, at internettet i sin natur er usikkert. Øget sikkerhed har dog en slagside for brugerne ifølge it-ingeniøren:

"(…) det, der er problematisk ved internettet i dag. Det er jo faktisk brugervenligheden, fordi virksomheder og tjenesteudbydere de vil jo gerne gøre det brugervenligt for at få brugere. Og det er jo også en god tanke, men brugervenlighed er jo også sårbart over for misbrug, fordi hvis det skal være brugervenligt, så kan det ikke være 100 % sikkert."

Øget sikkerhed kommer altså på bekostning af brugervenligheden af de forskellige tjenester og hjemmesider. En måde at øge sikkerheden ville ifølge it-sikkerhedschefen være at indføre brugerbetaling:

"*Der blev på et tidspunkt snakket om, at der skulle være sådan nogle mikrobetalinger på e-mail, så at ligesom, når man skal putte et frimærke på et postkort eller et eller andet, jamen så, så skulle [man] betale et eller andet hver gang man sendte en e-mail. Men rent praktisk, så har det jo ikke været til at indføre sådan et system, og der var nok heller ikke rigtig mange, der havde lyst til at have det i virkeligheden at betale for noget, som dybest set var gratis (...)*"

Indførelsen af mikrobetalinger ville gøre det dyrt og mindre attraktivt for phisherne at sende et stort antal e-mails, men den øgede sikkerhed ville være på bekostning af brugervenligheden. Som it-sikkerhedschefen beskriver, var det ikke praktisk muligt at indføre dette, og det kunne gøre legitime brugere utilfredse at blive straffet for, at kriminelle sender phishingmails. Det viser, at sikkerhed og regulering af internettet ikke i alle tilfælde er at foretrække frem for eksempelvis brugervenlighed.

6.4 Dansk it-efterforskning som et netværk

For at få et indblik i udfordringerne ved bekæmpelse af phishing benyttes ANT til at afdække det netværk, som phishing efterforskes i. Et phishingangreb efterforskes indledningsvis i Danmark, og derfor er det relevant først at kortlægge det danske it-efterforskningsnetværk.

6.4.1 Kortlægning af aktører

Fra et ANT-perspektiv anses den danske it-efterforskning som et netværk udgjort af en lang række aktører, som konstruerer og påvirker hinanden. I en it-efterforskning af en phishingsag indgår aktører såsom: offeret, gerningsmanden, phishingmailen, efterforskeren, computere og ip-adresser. Det er aktørerne, der skaber det netværk, som efterforskningen foregår i. En efterforskning uden it vil ikke være en it-efterforskning, fordi den aktør ikke eksisterer i netværket. Det er derfor aktørerne, der skaber de forskellige forbindelser, som gør, at noget kan kaldes en "it-efterforskning". I empirien fremgår det,

hvordan it-efterforskningen er et komplekst netværk udgjort af forskellige aktører. It-ingeniøren fra NC3 forklarer, at afstanden mellem aktørerne i efterforskningsnetværket i Danmark var stor:

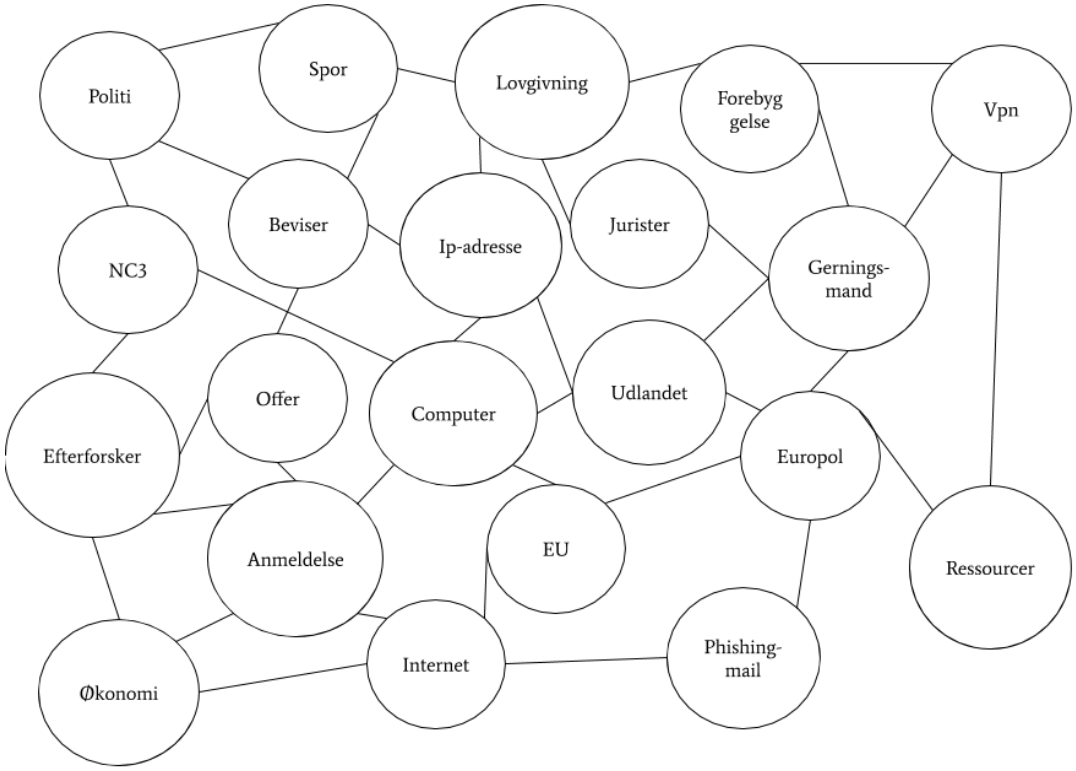
"det [har] for kredsene føltes [som] (…) meget langt til selve Rigspolitiet for at [kunne] få hjælp. Hvem skal man henvende sig til, hvor lang tid tager det og alle de der ting. Og hvad så, hvis der er noget akut, og så er der en kæde af kontaktpunkter, så det har man gerne ville skære væk, så det bliver mere direkte."

Fra Rigspolitiets side har man altså introduceret en ny aktør i det danske it-efterforskningsnetværk i form af NC3. NC3 er et samlet center for it-kriminalitetsefterforskning i Danmark og blev etableret for at gøre kommunikationen lettere og for at kunne arbejde mere effektivt ved at fjerne nogle af kontaktpunkterne. It-ingeniøren fortæller, at hans opgave er at hjælpe efterforskerne med både komplekse og simple it-opgaver. Både NC3 og de enkelte politikredse indgår derfor som aktører i it-efterforskningsnetværket. It-efterforsker Søren Nielsen fortæller, at Nordjyllands Politi samarbejder med NC3, hvis der opstår problemer:

"(…) hvis der er noget, vi sidder heroppe og ikke kan finde ud af, så er vores storebror jo NC3, som vi ligesom skal rådføre os med, som ligesom lægger retningslinjer, og alle kredsene har fået ansat en it-ingeniør, altså en eller anden ingeniør med it-baggrund, som er ansat sådan set under NC3, men er placeret ude i alle politikredsene (…)"

En anden aktør inden for it-efterforskningsnetværket er lovgivningen. Som it-ingeniøren fra NC3 forklarer: *"(…) vi har jo en retsplejelov og nogle retssikkerhedsprincipper, som vi skal overholde (…)"*, og loven som aktør har på den måde indflydelse på, hvilket grundlag politiet har at arbejde ud fra.

It-efterforskningen består altså af flere forskellige aktører, som interagerer med hinanden i netværket.



Figur 7: It-efterforskning som et netværk

Som det ses på figur 7, er it-efterforskningsnetværket et netværk udgjort af aktørerne, som på forskellige måder indgår i en dansk it-efterforskning.

6.4.2 Computeren som aktør i efterforskningsnetværket

Både gerningsmandens og politiets computere indgår i netværket som et redskab for efterforskerne til at opklare kriminalitet. It-efterforskeren hos Nordjyllands Politi nævner i forbindelse med deres tilgang til efterforskningen: *"(...) [vi undersøger], hvad kan vi få ud af deres computere og deres mobiltelefoner i forhold til beviser."*. Det vil sige, at gerningsmandens computer indgår i netværket som bevismateriale, når efterforskerne undersøger, om der er kriminelt indhold på den. Hvis de skal opspore en gerningsmand, som har lavet et phishingangreb, er politiet også nødt til at bruge deres egne computere til at finde ud af, hvor angrebet kommer fra, så de kan finde gerningsmandens fysiske lokation. På den måde stiller gerningsmanden som aktør krav til både efterforskeren og it-efterforskningsnetværket. Efterforskeren er nødt til at efterforske kriminaliteten i det netværk, hvor kriminaliteten er opstået, og den kriminelle befinder sig. Når en kriminel begår kriminalitet online, så er it-efterforskningen og efterforskeren også nødt til at befinde

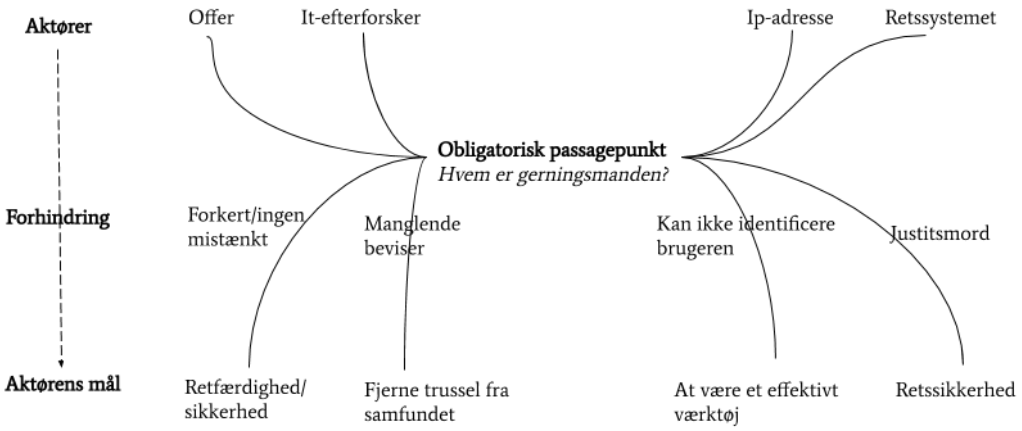
sig i dette netværk. Det er dog ikke altid lige nemt, fordi gerningsmændene er gode til at skjule deres digitale spor. Som it-ingeniøren fra NC3 nævner, undersøger de gerningsmandens ip-adresse for derigennem at finde en fysisk lokation:

"(...) hvad er det for nogle ip-adresser, der har været logget ind og så typisk så, hvis de er dygtige, så peger det selvfølgelig på nogle vpn-udbydere, så skal vi selvfølgelig have gang i nogle kendelser. Og nogle vpn-udbydere de vil gerne samarbejde med myndigheder, hvis vi har kendelser, og andre de gemmer så ikke logs."

Gerningsmandens ip-adresse, vpn og vpn-udbyderen indgår derfor også som aktører i it-efterforskningsnetværket. Som det fremgår, er netværket efterhånden meget omfattende og komplekst, og det er en af de helt store udfordringer ved at bekæmpe it-kriminalitet.

6.4.3 It-efterforskning som en translationsproces

Som tidligere belyst eksisterer der en række forskellige aktører i it-efterforskningsnetværket, og enhver it-efterforskning kan anses for at være en translationsproces, hvor forbrydelsen translateres fra spor til gerningsmanden. I processen gør en aktør gør sig uundværlig og definerer problemet, som de relevante aktører skal samarbejde om at løse. I en it-efterforskning vil dette være at finde frem til gerningsmanden. It-efterforskeren fra Nordjyllands Politi nævner formålet med en it-efterforskning: *"(...) om man kan finde gerningsmanden, der står bag det (...)"*. Det obligatoriske passagepunkt er altså *hvem er gerningsmanden?* Og i en it-efterforskning er dette punktet, som aktørerne skal samarbejde for at passere. It-efterforskeren er den aktør, der gør sig uundværlig i translationsprocessen og definerer det obligatoriske passagepunkt. For at finde ud af hvem gerningsmanden er, skal it-efterforskeren finde og inddrage relevante aktører i translationsprocessen, som it-ingeniøren fra NC3 nævner: *"(...) så kan vi samarbejde med den danske virksomhed og efterforske, jamen hvad har der været sket på deres server, hvornår blev de hacket, og hvad er det for nogle ip-adresser, der har været logget ind (...)"*. Det viser, hvordan efterforskerne inddrager den danske virksomhed, som er offeret, og ip-adressen i translationsprocessen for at samarbejde og finde frem til gerningsmanden.



Figur 8: Andet trin i translationsprocessen illustreret med det obligatoriske passagepunkt, forhindringer og eksempler på aktørernes individuelle mål

Som nævnt er det obligatoriske passagepunkt *hvem er gerningsmanden?*, men de forskellige aktører har forskellige motivationer for at skulle igennem passagepunktet, fordi deres endelige mål varierer. Som vist på figur 8 har offeret et andet mål end it-efterforskeren. I dette eksempel er målet for offeret at opnå retfærdighed og afklaring, hvorimod målet for it-efterforskeren kan være at fjerne kriminelle fra samfundet. For at disse mål kan opnås, er de nødt til at undgå deres forhindringer. Forhindringen for offeret kan være, at den skyldige aldrig findes, og offeret kan derfor ikke opnå retfærdighed. Ved at gennemgå det obligatoriske passagepunkt undgår aktørerne deres forhindring, og de har derfor incitament til at indgå i translationsprocessen.

På næste trin i processen forbindes aktørerne med hinanden gennem forhandlinger. I en it-efterforskning forhandler efterforskerne med beviserne. It-ingeniøren fra NC3 kommer med et eksempel på, hvordan en ip-adresse kan lede hen til en formodet gerningsmand: *"(…) netbutikken kan så se den pågældende persons ip-adresse som den, der køber, men når vi så kommer hjem til personen, så viser det sig, at det så har været hacket (…)"*. Det viser, hvordan politiets efterforskere har forhandlet med ip-adressen for dermed at kunne udlede, hvor den mulige gerningsmand befinder sig. I dette tilfælde leder den dog ikke hen til selve gerningsmanden, men til en uskyldig persons computer som er et mellemled. It-ingeniøren nævner, at det kan være udfordrende at finde frem til den rigtige lokation, fordi

de ofte er maskeret gennem en vpn-forbindelse, som skjuler gerningsmandens ip-adresse og lokation. Det viser, hvordan gerningsmanden kan bruge de teknologiske aktører til sin fordel til at udføre kriminelle handlinger, mens it-efterforskeren prøver at bruge teknologien til sin fordel til at bekæmpe kriminalitet. Forhandlingen er dermed en essentiel del af translationsprocessen, fordi den er afgørende for, at målet opnås.

Fjerde og sidste trin i translationsprocessen er *mobilisering*. I denne del af translationen agerer nogle aktører talsmænd for andre. It-efterforskeren efterforsker eksempelvis sagen på vegne af politiet som organisation og agerer derfor talsmand for denne aktør.

Hvis it-efterforskningen finder frem til en mistænkt, sker der en ny translationsproces, og et nyt obligatorisk passagepunkt defineres og reflekterer denne ændring i sagen. Et eksempel kunne være i en phishingsag, hvor man i starten af efterforskningen ikke har en mistænkt. Efterhånden som efterforskningen skrider frem, fører beviserne måske til en mistænkt, hvilket gør, at det obligatoriske passagepunkt ændres til at reflektere, at der nu er en mistænkt. Et nyt obligatorisk passagepunkt kunne derfor være *er den mistænkte gerningsmanden?*

6.5 Lovgivning som en sort boks

Lovgivning er en aktør i efterforskningsnetværket og udgør som et stabilt netværk en sort boks. Lovgivningsnetværket er så stabilt, at det anses som en kendsgerning, men de traditionelle lovgivningsmæssige kendsgerninger udfordres af teknologiaktørens tilstedeværelse i it-efterforskningsnetværket. Juraprofessor Birgit Feldtmann nævner, at lovgivningen i flere tilfælde ikke er fyldestgørende til afsigelse af domme og retsproceslige afgørelser vedrørende it-efterforskning. It-kriminaliteten har med andre ord udfordret kendsgerningerne i lovgivningen, og den sorte boks er derfor blevet ustabil. Juraprofessoren nævner, at det ofte er nødvendigt for domstolen at strække fortolkningen af loven, når der skal gives kendelser til it-efterforskning, da både retsplejeloven og straffeloven hovedsageligt er tiltænkt den fysiske verden:

"(...) altså hele den måde efterforskning og regulering af efterforskning, det er i retsplejeloven (...) Den er knyttet til den fysiske verden. (...) Og der har der blandt andet

været nogle spørgsmål om, at hvis du har en mobiltelefon og får koden til den, hvad er det så egentlig? Er det en ransagning? Hvad er reglerne? Det har man ikke decideret taget stilling til fra lovgiverens side, og det betyder, at domstolen i sidste ende skal se på, hvis forsvaret rejser sagen, hvad er rammen så for det her, og hvad er det her? (…) man bruger de gamle koncepter, procesretlige koncepter som ransagning og så videre til det her, men det giver nogle problemer (…)"

Juristerne er på grund af disse problemer i netværket nødt til at åbne den sorte boks og vurdere, om der er passende paragraffer, der kan dække de nye kriminalitetsformer, eller om det er nødvendigt med nye love. Med Latours (1999, s. 185) ord er det nødvendigt at åbne den sorte boks ved at kigge ned i maskinrummet og beskue de enkelte aktører og deres relationer. Juraprofessoren mener, at lovgivningen i Danmark skal gennemtænkes med fokus på it-kriminalitet. Hvis teknologi i højere grad inddrages i den danske lovgivning, ændres dette netværk som et resultat af den nye aktør, der introduceres. Når netværket på et tidspunkt igen er blevet stabilt, er det igen en sort boks, som kan anvendes som en kendsgerning i it-efterforskningsnetværket. Lovgivningen som en sort boks betyder, at der ikke er problemer i netværket, hvilket vil sige, at lovgivningen heller ikke skaber problemer i efterforskningsnetværket. Med dette udgangspunkt vil det være en fordel at åbne den sorte boks og undersøge aktørerne i netværket, så det igen kan blive stabilt. Det kan være en udfordring at bekæmpe phishing i Danmark, hvis ikke flere aktører indgår som sorte bokse i efterforskningsnetværket.

6.5.1 Juristernes manglende it-kompetencer

Et af problemerne ved at lovgive mere specifikt om it-kriminalitet og teknologi er ifølge Brown (2015, s. 56) juristernes manglende it-kompetencer, hvilket juraprofessor Birgit Feldtmann også ser som en udfordring:

"[Udfordringen] er, at jurister ikke altid forstår, hvad det er, der sker på internettet. Jeg har jo brugt det her lille eksempel med en cloud. For at kunne lovgive om det, eksempelvis om det kunne give nogen jurisdiktionsproblemer, så skal man jo teknisk forstå, hvad det er. (…) men jeg tror, at hvis man lavede, det kunne være en kommission, som skulle kigge på strafferetsrådet, straffelovsrådet eller noget i den stil, at man så også tilknytter nogle it-

kyndige, som kan i letforståelige termer forklare juristerne, hvad det egentlig er. Altså jeg tror, at for at lave en god lovgivning på området vil det hjælpe at have noget sparring med nogle folk, som har forståelse for det tekniske."

Hun mener altså ikke, at juristerne altid selv har de teknologiske kompetencer til at formulere en fyldestgørende lovgivning på området, og det kan betyde, at det vil være nødvendigt at samle en kommission med it-kyndige personer. Loven kan fra et ANT-perspektiv ses som en inskription af viden om kriminalitetsformer og kriminalitetsudvikling. Denne viden kondenseres til en lovtekst, som fremad agerer på vegne af den tidligere viden og danner rammen for fremtidige straffe. Viden om it er ikke i høj grad inskriberet i den danske lovgivning, hvilket netop kan hænge sammen med de manglende it-kompetencer, som juraprofessoren nævner. Hvis teknologiske kompetencer introduceres i lovgivningsnetværket i form af en kommission, vil denne viden også kunne inskriberes i lovteksterne og eventuelt løse nogle af problemerne, der skaber ustabilitet i netværket.

6.5.2 Konsekvenser ved manglende retsforfølgelse

Fra nogle kriminologiske synspunkter er det væsentligt, at kriminelle straffes for deres handlinger, da det sender et signal til samfundet. Direktøren for World Economic Forums Center for Cybersikkerhed forklarer, at it-kriminalitet er den mest risikofri kriminalitetsform, og at der ikke er tale om opklaringsprocenter, men opklaringspromiller (Pedersen, 2019). Det vil sige, at der ikke sendes et stærkt signal til de kriminelle om, at det er et strafbart forhold, der tages alvorligt, hvilket kan være med til at forklare den store mængde af it-kriminalitet. Ifølge Beccaria (2014, s. 28-29) er straffen samfundets måde at forhindre kriminalitet på, da mennesker agerer rationelt og derfor kan afskrækkes med straf fra at begå kriminelle handlinger. På den måde spiller lovgivningen en vigtig rolle i at kriminalisere et forhold, og politiet har et vigtigt arbejde i at efterforske eksempelvis phishing. Ifølge afskrækkelsesteorien vil en phishinggerningsmand være mindre tilbøjelig til at lave et phishingangreb, hvis han har oplevet at blive straffet for sine tidligere angreb. Ligeledes vil det være mindre sandsynligt, at en person laver et phishingangreb, hvis det er alment kendt, at it-kriminelle generelt straffes for phishingangreb. På den måde kan lovgivningen have en stor betydning for kriminalitetsudviklingen. Lovgivningen og

dommene spiller derfor også en rolle i phishingnetværket. Hvis antallet af domme for phishing og it-kriminaliteten generelt øges, vil det betyde, at det af befolkningen ikke opfattes som risikofrit og acceptabelt at begå den type af kriminalitet.

6.6 Manglende anmeldelser og manglende ressourcer?

Anmeldelser og ressourcer er en nødvendighed for, at dansk politi kan efterforske et kriminelt forhold. I et ANT-perspektiv indgår anmeldelsen fra offeret som en inskription af en hændelse for at få politiet, som agerer ud fra lovgivningen, til at efterforske sagen. I den forbindelse foregår der en translationsproces hvor offeret, anmeldelsen, politiet og loven alle indgår som aktører. It-ingeniøren fra NC3 fremhæver eksempler på, at borgere ikke ønsker at anmelde phishingangreb: *"Vi har jo oplevet, at der er nogle, der siger, at de gider ikke at anmelde det og det og det til politiet, fordi det kan ikke betale sig. Politiet kan ikke gøre noget ved det alligevel (…)"*. Det medfører, at translationsprocessen aldrig bliver påbegyndt, fordi offeret ikke indgiver anmeldelsen. Som vist på tabel 1 er der sket en stigning i antallet af anmeldelser af databedrageri, men i politiets statistik er det ikke muligt at få yderligere detaljer om, hvilke forskellige databedragerityper der er tale om, og tallet dækker derfor over mange forskellige typer. Det understøttes af Grabosky (2016, s. 61), som forklarer, at it-kriminalitet ofte bliver registreret under andre kriminalitetsformer, og det er derfor uklart, hvor udbredt det er. It-efterforskeren fra Nordjyllands Politi forklarede, at de ikke som sådan forholder sig til begrebet phishing, når der kommer en anmeldelse. Det kan betyde, at det er svært at overskue, hvilke metoder gerningsmændene bruger og se mønsteret i et større perspektiv, og derfor kan det være udfordrende at bekæmpe kriminaliteten. Det betyder også, at det ikke er muligt at få et klart tal på, hvor mange der reelt anmelder phishing.

Der kan der være flere forklaringer på, at offeret ikke ønsker at anmelde phishing. Grabosky (2016, s. 61-62) og Waschke (2017, s. 169-171) nævner nogle af forklaringerne som:

- At borgeren ikke opdager, at vedkommende har været udsat for kriminalitet
- At borgeren ikke tror, politiet tager det alvorligt
- At offeret er ligeglad
- At offeret er flovt over at være hoppet på et fupnummer

Især Grabosky og Waschkes pointe om at borgeren tror, at politiet ikke tager det alvorligt, bekræftes af it-ingeniøren fra NC3. It-efterforskeren fra Nordjyllands Politi udtaler også:

"Der tror jeg, at man kommer i politiet langt med bare at råde og vejlede i, at de bare skal ignorere det og slette det, fordi det er så masseforekomst. Så det er først i det øjeblik, hvor det ligesom er kommet skridtet videre, hvor der er nogle, der har brugt oplysningerne, at det ligesom bliver til en politisag."

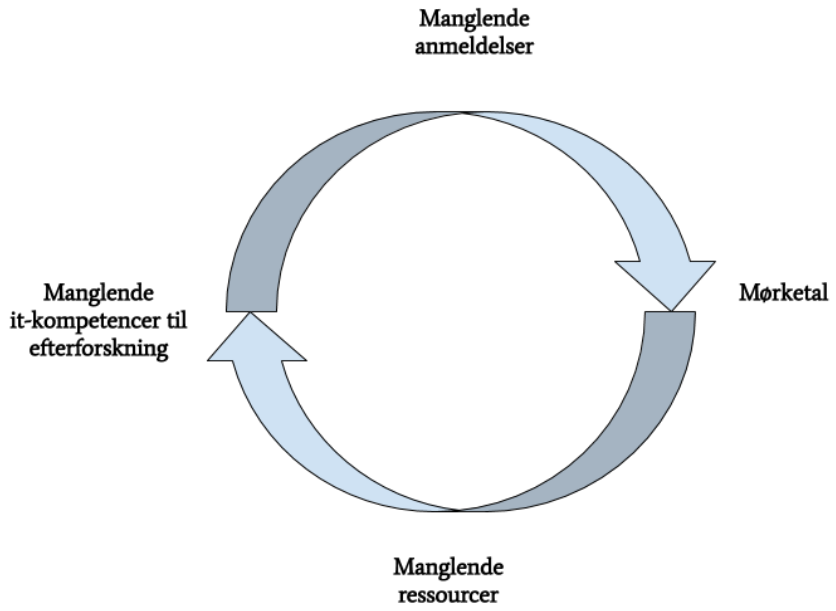
It-efterforskeren giver udtryk for, at Nordjyllands Politi opfordrer folk til bare at slette phishingmailen, hvilket for borgeren kan give et indtryk af, at politiet ikke tager det alvorligt. It-ingeniøren fra NC3 forklarer derimod, at det kan være en udfordring at bekæmpe phishing, hvis ikke politiet modtager anmeldelser, fordi de ikke får et realistisk billede af, hvor stort omfanget af kriminaliteten er. NC3 vil derfor gerne have anmeldelser, selvom der kun er tale om et forsøg:

"Vi vil gerne have anmeldelsen, også selvom det kun er et forsøg, men så bruger vi det mere som sådan en form for efterretninger, hvor vi samler informationerne, kigger det igennem og tænker, okay, ligner det noget, vi kender, eller ligner det ikke."

NC3 har altså ressourcer til at modtage anmeldelser og translatere dem til efterretninger, som benyttes til at skabe forbindelser mellem forskellige sager. It-ingeniøren mener, at det går ud over politiets ressourcer til bekæmpelse af it-kriminalitet, hvis ikke de får nok anmeldelser:

"Så når politikerne de ringer til politiet og siger, hvor mange sager omkring den slags snyd, får politiet anmeldt om året? Så kan vi sige ingen. Fordi folk de ikke gider anmelde det. Og så siger politikerne, jamen så er der jo ikke noget problem med i Danmark, men det er der jo."

Politiet og politikerne bliver ikke opmærksomme på omfanget af phishingangreb i Danmark, hvis det ikke anmeldes.



Figur 9: Illustration af hvordan manglende anmeldelser påvirker politiets ressourcer

Som figur 9 viser, skabes der en negativ cirkel, hvor manglende anmeldelser hænger uløseligt sammen med mørketallet og derfor de politiske beslutninger på området. Dette påvirker politiets ressourcer og dermed deres efterforskningskapacitet, som igen påvirker anmeldelsesraten, fordi borgerne kan få den opfattelse, at det ikke kan betale sig at anmelde det. Der er altså en forskel på, hvordan Nordjyllands Politi og NC3 prioriterer phishinganmeldelser, og hvordan de mener, borgerne skal forholde sig til phishingangrebene. NC3 opfordrer til, at borgerne anmelder både vellykkede og mislykkede phishingangreb, mens Nordjyllands Politi mener, at borgeren i langt de fleste tilfælde skal slette mailen og ikke lade det blive en politisag. NC3 viser en proaktiv tilgang til kriminalitetsbekæmpelse ved at anvende anmeldelser som efterretninger for at kunne forudsige mønstre i kriminaliteten. Nordjyllands Politi har derimod en anden tilgang til bekæmpelsen, da de opfordrer folk til at slette phishingmailen, hvis ikke den har medført et økonomisk tab.

Professor i kriminologi Peter Kruize forklarer, at der foreligger et stort mørketal inden for phishing, og at offerundersøgelser derfor kan give et mere retvisende billede af omfanget: *"(...) offerundersøgelser giver selvfølgelig et bedre indblik i mørketal, men ikke 100 %"*. Han har gennemført offerundersøgelser med henblik på at afdække omfanget af blandt andet

phishing, og de har vist, at det er en stigende udfordring. Offerundersøgelserne er en god metode til at afdække omfanget af phishing, da der foreligger et stort mørketal i anmeldelsesstatistikkerne, fordi mange ikke anmelder forsøg på it-kriminalitet, og fordi politiets praksis på området kan variere.

6.6.1 Manglende ressourcer?

Antallet af anmeldelser har konsekvenser for mængden af ressourcer, der allokeres til bekæmpelse af phishingsager. Ifølge kriminologiprofessoren er politiets ressourcer afgørende for bekæmpelse af phishing. *"Jeg tror (...) det handler om kapacitet og kendskab hos politiet, som er den afgørende faktor."*. NC3 er en afdeling, som udelukkende har fokus på it-kriminalitet og derfor har en større samling af kompetencer på it-området, hvorimod de forskellige politikredse skal håndtere mange forskellige kriminalitetstyper. It-ingeniøren fra NC3 mener dog stadig, at der mangler ressourcer hos politiet: *"(...) der er jo helt grundlæggende (...) for få ressourcer. Fordi det er jo ... Altså it-kriminalitet er jo i eksplosiv vækst."*. At NC3 også prioriterer mindre phishingsager og laver efterretninger kan have den betydning, at de mangler ressourcer til at efterforske. It-efterforskeren fra Nordjyllands Politi er dog uenig i, at der mangler ressourcer til it-efterforskning: *"(...) rent ressourcemæssigt har vi nok at trække på, hvis der er noget, der giver problemer. Jeg tænker ikke, det er der... Kompetencerne er i hvert fald til stede er mit umiddelbare indtryk."*. I Nordjyllands Politi er opfattelsen altså, at der både er tilstrækkelige ressourcer og kompetencer til at bekæmpe phishing.

Den manglende anmeldelsestilbøjelighed viser en udfordring i forhold til bekæmpelse af phishing i Danmark, da der internt i politiet er uenighed både om proceduren for håndtering af phishinganmeldelser og mængden af ressourcer på området. Det kan resultere i, at borgerne ikke ønsker at anmelde det, hvilket starter en negativ udvikling, som i sidste ende betyder, at politiet ikke får tildelt de fornødne ressourcer til bekæmpelse af phishing.

En anden grund, til at it-kriminalitet er ressourcekrævende at efterforske, er, at gerningsmænd kan sende en stor mængde data over lange distancer på meget kort tid. Kriminologiprofessor Peter Kruize udtaler:

"*At man kan række så bredt, som eksempelvis at kunne sende en million phishingmails, eller man kan bruge et botnet til at lægge hjemmesider ned og afpresse dem på den måde. Og du kan udføre it-kriminalitet fra et sted i Asien, mens målet er i Danmark.*"

Denne pointe bliver yderligere uddybet af Aas (2007), som beskriver, at internettet har gjort kriminalitet mere tilgængeligt og nemmere at udføre, og at skadevirkningerne derfor er blevet mangedoblet. Phishingmails kan altså sendes ud meget hurtigt og til mange personer på én gang. For politiet er phishingsager utroligt ressourcekrævende, da de er nødt til at efterforske hver enkelt phishingmail. Samtidig er politiet også nødt til at involvere transnationale aktører, hvilket kan være en langsommelig proces.

Politiet er altså nødt til at bruge en stor mængde af ressourcer til at opklare en sag med phishing, hvorimod det kun kræver få ressourcer for gerningsmændene at sende en million phishingmails ud.

6.6.2 Efterforskernes manglende it-kompetencer

Ligesom lovgivningen kan efterforskningen anses som en sort boks. En traditionel efterforskningsproces kan beskues som et netværk, der er blevet så stabilt, at det betragtes som en kendsgerning, fordi der er nogle faste procedurer, der følges i en standardefterforskning. Efterforskningsnetværket er derfor en sort boks. It som aktør i efterforskningsnetværket skaber dog problemer, hvilket gør det nødvendigt at åbne den sorte boks. It-kriminalitet sætter krav til efterforskernes kompetencer til at efterforske ved hjælp af it, og derfor er netværket blevet ustabilt. Som it-ingeniøren fra NC3 fortæller, gjorde den stigende forekomst af sager om it-kriminalitet det tydeligt, at mange efterforskere ikke har de nødvendige it-kompetencer:

"(…) det var omkring der 2014-2015, at der faktisk skete den her tænkning i, at man måtte simpelthen erkende, at det var ikke muligt internt i politiet at finde de nødvendige kompetencer til at følge med de kriminelle på it-området. Og det gjorde man både, fordi man fik noget erfaring med det med nogle af de her hacker-sager, hvor man var oppe mod nogle konkrete problemer, men også fordi de kan jo se, altså vi kigger jo også til resten af

verden, og de kan jo se, hvordan at de kriminelle de i retssager begynder at stille spørgsmål til efterforskernes kompetence- og uddannelsesniveau."

Denne situation viser, at netværket var ustabilt, og derfor måtte politiet åbne den sorte boks og finde ud af, hvilke kompetencer der manglede. It-efterforskningsnetværket blev efterfølgende søgt stabiliseret ved at inddrage civile kompetencer, som havde den nødvendige viden til at påtage sig efterforskningsopgaverne. Denne proces skete både inden for it-kriminalitet og økonomisk kriminalitet:

"Og dansk politi har jo så taget den beslutning, at det så er nødt til at hyre en masse it-kompetencer. Det er jo så ikke engang kun inden for it-området, men det er også inden for skatteteknik og økonomi, de er nødt til at ansætte civile eksperter, fordi tingene generelt bare bliver mere komplicerede. Og den tendens, vi kan se, jamen før i tiden med økonomisk kriminalitet, hvor man måske sad med et regneark og påførte nogle tal og måske brugte slettelak for at fjerne tallene igen, det er jo alt sammen blevet digitalt nu jo. Og digitale spor og avanceret økonomisk kriminalitet gør jo bare, at vi er på et helt andet niveau end tidligere."

Med den stigende forekomst af it-kriminalitetssager var efterforskningsnetværket altså blevet ustabilt, og det blev igen forsøgt stabiliseret ved at inddrage civile kompetencer som aktører og oprette centre som eksempelvis NC3 og LCIK (Landsdækkende Center mod It-relateret Økonomisk Kriminalitet). It-efterforskeren Jesper Thy fra Nordjyllands Politi mener ikke, det er realistisk, at en gennemsnitsefterforsker skal være specialist i it, og derfor er det bedre med specialafdelinger til at efterforske disse sager. Vigtigheden af efterforskernes it-evner fremgår også i translationsprocessen, hvor det er nødvendigt, at en efterforsker kan forhandle med beviserne for at finde ud af, hvem den skyldige er. Hvis en efterforsker mangler kendskab til it, er det ikke muligt at forhandle med beviserne i it-efterforskningen - derfor fejler tredje trin i translationsprocessen, *indrulning*. Det kræver en vis teknisk viden at kunne translatere it-spor såsom en ip-adresse til beviser mod gerningsmanden. Efterforskernes manglende it-kompetencer kan være en stor udfordring, da det kan betyde, at efterforskningen stoppes, fordi translationen ikke lykkes, og gerningsmanden fanges derfor ikke. Det problematiserer Waschke (2017, s. 73) og

forklarer, at hvis ikke de små it-kriminalitetssager bliver behandlet, vil de vokse sig store med tiden.

Efterforskernes manglende it-kompetencer kan på den måde relateres til juristernes manglende kendskab til it, når det gælder lovgivningen. Juraprofessor Birgit Feldtmann opfordrede til en samling af en kommission med teknologisk kyndige aktører, hvilket minder om politiets tilgang til bekæmpelse af it-kriminalitet ved at inddrage civile kompetencer i efterforskningen.

6.6.3 Efterforskning og lovgivning er et skridt bagud

I takt med at teknologien udvikler sig, finder de kriminelle nye metoder til at begå it-kriminalitet. En af udfordringerne ved at bekæmpe it-kriminalitet er derfor, at efterforskningen og lovgivningen altid er et skridt bagud. It-efterforskeren fra Nordjyllands Politi fortæller, at det altid vil være kattens jagt efter musen, hvor efterforskerne forsøger at følge med gerningsmændenes nye metoder:

"Jeg tror, det vil altid være et eller andet i kattens jagt efter musen. Der bliver udviklet et eller andet, som så gør det muligt at skjule noget (…) Altså det bliver en eller anden jagt. Det vil det simpelthen blive, fordi man kan altid finde nye metoder, som så ikke bliver fundet af de gamle metoder, man har, og så må man finde på noget nyt. Jeg tænker, at den jagt, den vil altid være der i et eller andet omfang.".

På den måde udvikler efterforskningen sig i takt med teknologien, men det samme gør gerningsmændenes metoder. Der er derfor stillet store krav til efterforskernes brug af it, og at de hele tiden følger med it-udviklingen. Juraprofessoren nævner også, at lovgivningen altid er et skridt bagud: *"(…) lovgivningen løber jo altid efter i forhold til den virkelige verdens udvikling, (…)"*. Både lovgivningen og efterforskningen er traditionelt set reaktive enheder, som reagerer på og udvikler sig efter det aktuelle kriminalitetsbillede. Grabosky (2016, s. 6) nævner også problematikken med, at gerningsmændene er hurtige til at udvikle nye metoder, mens det at definere nye love er en langsommelig proces, hvilket juraprofessoren giver udtryk for, når hun siger, at de altid er et skridt bagud.

6.7 Europæisk samarbejde som et netværk

Phishing indgår som aktør i det danske it-efterforskningsnetværk, men stort set alle phishingangreb, som rammer Danmark, kommer fra udlandet. Når dansk politi skal efterforske et phishingangreb, laver de selv den indledende efterforskning og indgår løbende i samarbejde med en række internationale og europæiske aktører.

6.7.1 Europæisk samarbejde som translationsproces

Phishing foregår over internettet og er derfor ikke begrænset af landegrænser. Phishingangreb kan udspringe fra alle steder i verden, og derfor indgår dansk politi som aktør i et større europæisk efterforskningsnetværk. I det europæiske efterforskningsnetværk figurerer der flere forskellige aktører, som interagerer med det danske politi med henblik på at finde frem til gerningsmanden.

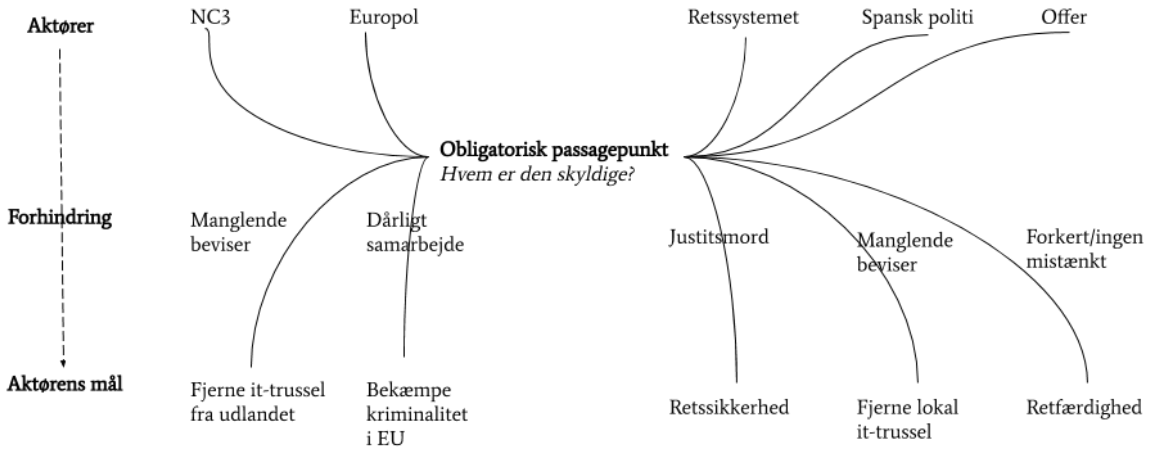
I det europæiske netværk interagerer NC3 med flere andre aktører. Juraprofessoren fortæller: *"(...) vi har eksempelvis noget i EU, som hedder Europol, som er et politisamarbejde (...)"*. Europol er dermed en aktør, men også et netværk sammensat af aktører fra de forskellige medlemslande i EU. It-ingeniøren belyser blandt andet dette: *"(...) så kan der jo godt være tre lande, der på Europol, europæisk niveau, er i gang med at efterforske en konkret sag."*. Europol er således en organisation i det europæiske efterforskningsnetværk, som den danske efterforskning kan samarbejde med. Europol samler altså de relevante aktører i en transnational efterforskning.

Ligesom den danske it-efterforskning kan det europæiske samarbejde ses som en translationsproces, hvor aktørerne samarbejder om et obligatorisk passagepunkt, der er: *Hvem er den skyldige?* Og eftersom dette passagepunkt er obligatorisk for alle aktørerne, foregår opklaringen som led i, at aktørerne når deres individuelle mål.

Europol er en aktør i det europæiske samarbejde, når NC3 skal efterforske en phishingsag i en transnational kontekst på vegne af Danmark. Aktørerne i translationsprocessen er derfor NC3, Europol, retssystemet, offeret og lokalpolitiet. I figuren anvendes spansk politi som eksempel på et lokalpoliti, der indgår i et internationalt samarbejde med blandt andre Danmark. Det danske retssystem er også en aktør, fordi dansk lovgivning har indflydelse

på, hvorledes NC3 kan efterforske i udlandet: *"(…) vi har jo en retsplejelov og nogle retssikkerhedsprincipper, som vi skal overholde, og det skal vi faktisk også overholde, selvom gerningsmanden måske sidder i Nigeria. Så det skal vi selvfølgelig tænke ind i efterforskningen også."*. Den danske efterforskning skal altså følge dansk lovgivning og skal retsforfølge herefter, også selvom lovgivningen i gerningsmandens oprindelsesland kan variere.

Følgende figur viser et eksempel på de enkelte aktørers individuelle mål og incitament for at gennemgå det obligatoriske passagepunkt:



Figur 10: Eksempel på det europæiske samarbejde som en translationsproces

Denne translationsproces minder på flere måder om den, der foregår ved en dansk it-efterforskning. I dette netværk er der dog flere internationale aktører. Offerets endelige mål ændrer sig ikke, fordi efterforskningen foregår på europæisk niveau, og offeret indgår derfor i translationsprocessen på samme måde som ved en dansk efterforskning. NC3, Europol og det spanske politi har lignende mål, da de alle ønsker at bekæmpe kriminalitet. Som it-ingeniøren fra NC3 forklarede, kan en omfattende phishingsag være af europæisk interesse, og Europol har derfor også et ønske om at gennemgå det obligatoriske passagepunkt. Spansk politi har som mål at fjerne kriminelle trusler, og de er derfor også interesserede i at indgå i translationsprocessen. It-ingeniøren fortæller om det danske samarbejde med Europol: *"(…) det fungerer faktisk rigtig godt (…) Altså vi udveksler*

oplysninger med Europol omkring efterforskninger. Ikke persondata, men omkring efterforskninger og gerningsmænd, der udveksler vi selvfølgelig oplysninger og modus og hændelser (…)". Europol er altså en aktør, der gør samarbejdet lettere mellem de europæiske nationer. It-ingeniørens udtalelse viser det tredje punkt i translationsprocessen, *indrulning*, hvor NC3 forhandler med spansk politi om at prioritere phishingsagen og bidrage til efterforskningen, så de finder den skyldige og hver især opnår deres endelige mål. Ved det fjerde punkt, *mobilisering*, agerer NC3 talsmand for det danske politi og de beviser, de har fremskaffet. I den forbindelse anses NC3 som en sort boks, da det er en kendsgerning, at de repræsenterer alle danske politikredse og Rigspolitiet i det europæiske samarbejde.

6.7.2 Prioritering af phishingsager i det europæiske samarbejde

En af udfordringerne ved at bekæmpe phishing i Danmark er, at bekæmpelsen er afhængig af andre europæiske eller internationale aktører. It-ingeniøren fra NC3 nævner, at det er udfordrende, da landene simpelthen kan have forskellige prioriteringer af sagerne:

"(…) de forskellige lande prioriterer sager forskelligt og afhængig af beløbsstørrelse, og hvor meget der er snyd for og alle de der ting, så er det forskelligt, hvor meget folk de gider at lægge i det. Det eneste område, hvor at det virkelig er nemt at samarbejde, det er omkring børnepornografi for eksempel. I forhold til phishing og den slags ting, der er det meget tilfældigt (…)"

I det europæiske samarbejdsnetværk er det altså sværere at samarbejde om efterforskning af eksempelvis phishing end børnepornografi, da landene kan prioritere sagerne forskelligt, hvorimod sager om seksuelle krænkelser af børn generelt prioriteres højt. Han nævner dog, at det kan være en fordel, at phishingsager bevæger sig mellem flere lande, da mange aktører bringes i spil og kan bidrage til efterforskningen:

"(…) når det nu skal ske, så er det selvfølgelig en fordel, at det bevæger sig rundt, fordi så får de jo gang i flere landes efterforskning, og så kan man jo begynde at samle de her informationer på tværs af regioner og sådan nogle ting. Ulempen er selvfølgelig så, at det

landene hver især bare ikke rigtig er gearet til sådan en global efterforskning. (…) det skal virkelig være noget, der fylder meget (…)"

It-ingeniøren giver udtryk for, at landenes individuelle efterforskninger ikke er problemet, men udfordringen er, at de hver især ikke er udrustet til transnationale efterforskninger. På den måde er det tydeligt, at en aktør som Europol har sin plads i netværket og spiller en vigtig rolle, da den faciliterer en europæisk efterforskning og styrker samarbejdet mellem de enkelte efterforskningsnetværk.

6.7.3 Internationalt samarbejde kontra EU-samarbejdet

Foruden EU-efterforskninger kan det danske politi også indgå i et internationalt samarbejde, hvor lande uden for EU er involveret. Kriminologiprofessor Peter Kruize forklarer, at det internationale samarbejde hurtigt kan blive en omfattende proces: *"(…) det er ret omfattende, hvis udlandet er indblandet i det. Man skal tit igennem retsanmodninger til oplysninger, og det kan være ret svært."*. Der er altså en del anmodninger og bureaukrati forbundet med internationale efterforskninger. It-ingeniøren fra NC3 nævner ligeledes, at et bredt internationalt samarbejde er meget mere kompliceret end et EU-samarbejde: "*Det er noget nemmere at samarbejde med europæiske myndigheder end resten af verden.*", og at "*Det er et meget bredt samarbejde, og det er et tungt samarbejde.".* Det kan hænge sammen med, at EU-landene har et samarbejde gennem Europol som fælles politimyndighed, som kan gøre efterforskningen af sagerne lettere. Hvis gerningsmanden opholder sig i et land uden for EU, gør det også udleveringen væsentligt sværere, som juraprofessor Birgit Feldtmann forklarer: *"Samtidig hvis det for eksempel er de her Nigeria-breve, hvor det er folk, som sidder i Nigeria, så er det så usandsynligt, at du nogensinde får fat i de her folk."*. Hun uddyber, at såfremt en dansk efterforskning ledes uden for EU, skal en kendelse sendes igennem de officielle organer: *"(…) og så er der er andre lande – der er det meget kompliceret, for der skal det gå via Justitsministeriet, Udenrigsministeriet og så videre, så altså ret kompliceret."*. Der skal altså i den forbindelse inddrages flere aktører i samarbejdsnetværket, nemlig danske og udenlandske ministerier.

Komplikationerne i det internationale samarbejde viser, hvordan Europol som aktør i det europæiske samarbejde har stor betydning for netværket. Med en fælles politimyndighed

lettes samarbejdet, hvilket styrker bekæmpelsen af phishing i EU-landene. En af udfordringerne ved at bekæmpe phishing for de danske myndigheder er derfor, at opklaringen ofte kræver samarbejde med lande uden for EU, som kan være kompliceret og tidskrævende.

6.8 Oplysning som aktør

En udfordring ved at bekæmpe phishing i Danmark er, at et succesfuldt phishingangreb afhænger af teknologisk sikkerhed og menneskers dømmekraft, fordi det er borgeren selv, der skal spotte et forsøg på bedrageri og forhindre phishingangrebet i at lykkes.

Borgeren er i den forbindelse en aktør, som interagerer med computeren og phishingmailen. Som tidligere illustreret i translationsprocessen med et vellykket phishingangreb interagerer gerningsmanden også med disse aktører i et forsøg på at få adgang til offerets konto- eller personoplysninger og anvender ofte social engineering som metode til at narre offeret. Det kommer til udtryk ved at anvende Nets som en tillidsvækkende afsender. For offeret er det afgørende, om vedkommende rent teknologisk har sikret sin computer eller har den fornødne viden til at gennemskue phishingangrebet. Phishingmailen skal i første omgang interagere med computerens antispam-systemer og antivirusprogrammer. It-sikkerhedschefen forklarer, at hvis phishingmailen alligevel når frem til offeret:

"(...) så handler det pludselig om, at angrebet ligesom er kommet igennem alle de her sikkerhedsforhindringer, vi har sat op, og nu rammer det så brugerens inbox, og nu er det så brugeren, der forhåbentlig har fået noget træning i at identificere phishingmails."

Hvis computerens sikkerhedssystem ikke forhindrer phishingangrebet, er det offerets dømmekraft, der kan forhindre, at angrebet lykkes. Der foregår således en forhandling mellem phishingmailen og offeret i netværket. Ifølge it-ingeniøren udnytter gerningsmændene bevidst borgernes uvidenhed og angriber mindre virksomheder og foreninger:

"Så de plukker jo bare de lavest hængende frugter for eksempel sådan noget som CEO-fraud, som virksomheder bliver udsat for, der kan vi jo se nu, hvor virksomheder er blevet bedre til at sikre sig, at nu er gerningsmændene begyndt at profilere og angribe private foreninger, altså sådan noget sportsforeninger og gymnastikforeninger og lokalforeninger og sådan nogle ting."

Gerningsmændene er altså opmærksomme på, hvilke virksomheder der er bedre til at beskytte sig mod it-trusler og kan derfor rette deres angreb mod mindre foreninger, som ikke er lige så oplyste om phishing som trussel. Politiet kan bekæmpe phishing i et vist omfang, men når en privat borger eller en virksomhed bliver udsat for et forsøg på phishing, et det den enkeltes handlinger, der afgør, om phishingangrebet lykkes, og om det bliver til en politisag. Som tidligere vist er det afgørende for en vellykket translationsproces, at offeret manipuleres og opgiver sine kontooplysninger. It-sikkerhedschefen fortæller, at it-kriminelle forsøger at snyde borgerne ved at fremtvinge en følelsesmæssig reaktion og få dem til at reagere hurtigt, så de ikke når at tænke sig om:

"Det kan også være, at man sender dig en mail fra det sociale netværk, som du bruger for eksempel Linkedin eller Facebook (…) hvor man så får at vide, at du nu er blevet ekskluderet af den her gruppe, og klik her for at finde ud af hvorfor. Det er jo sådan noget, der får en følelsesmæssig reaktion hos modtageren, hvor de så ikke rigtig forholder sig til, om den her mail ser rigtig ud. Kommer den fra det rigtige sted, er der stavefejl og så videre. Og så kigger de måske på det, fordi de er nysgerrige, og der er så den her gode uddannelse, der er så afgørende (…) så hvis I bliver bedt om at gå til Facebook, jamen så i stedet for at klikke på noget, der er i e-mailen (…) så åbner man bare sin browser (…) logger ind og så ser om man kan finde den her notifikation, som der er henvist til."

It-sikkerhedschefen forklarer altså, at gerningsmændene benytter sig af social engineering som metode. Han nævner også, at uddannelse og oplysning af borgerne er vigtigt og kan forhindre, at de falder i disse fælder. Både it-efterforskerne fra Nordjyllands Politi og it-ingeniøren fra NC3 nævnte også oplysning af borgerne som den bedste måde at forhindre phishing på i fremtiden. It-efterforskeren nævnte for eksempel:

"(…) man bliver nødt til at gå derover på oplysning, fordi det vil blive ved med at komme i

stor stil fra de her Nigeria-lande, at man bliver nødt til at få det ind, så det er sådan set bare en del af folks bevidsthed, at det er bare noget, der eksisterer. Det er noget, der kommer, og det skal man lære at skelne. Altså lidt i stil med antivirus på computeren. At det skal ned i det der niveau, hvor det bare er noget, folk ikke reagerer på (…) Der vil altid være nogle, som ikke, man ikke kan nå med de kampagner. Men hovedparten skal simpelthen sorteres fra i oplysningskampagner, så det aldrig nogensinde bliver til en politisag."

Informanterne fra politiet giver udtryk for, at det er en form for samfundslæring i en digital tid, at der er trusler på internettet, som skal være en del af folks bevidsthed. De mener altså, at forebyggelse er den bedste måde at forhindre langt størstedelen af phishingangreb på. Det kan være et udtryk for erkendelsen af, at det er nærmest umuligt at stoppe de it-kriminelle i deres handlinger, men at mængden af tab hos borgerne kan minimeres, hvis de bliver oplyste om truslen. De mener, forebyggelse i form af oplysningskampagner rettet mod borgerne er den mest effektive form for bekæmpelse af phishingangreb i Danmark, selvom det kan være svært at nå alle med en oplysningskampagne. Denne pointe kom Gupta et al. (2017) også frem til i deres diskussion af forskellige måder at forebygge phishing på. De konkluderede, at det er vigtigt at informere brugerne om phishing som trussel, før antallet af angreb nedbringes.

I et ANT-perspektiv kan det ses som et udtryk for, at oplysning som aktør i netværket på nuværende tidspunkt er underrepræsenteret, da borgerne tilsyneladende ikke er oplyste nok til at undgå at blive snydt af phishingangrebene. Som det altid er tilfældet i et netværk, ændrer tilstedeværelsen af en aktør selve netværket, hvilket vil sige, at oplysning som aktør i phishingnetværket kan skabe forandringer i dette, så færre phishingangreb medfører tab hos borgerne. Politiet og andre kriminalpræventive organisationer kunne introducere denne aktør ved flere oplysningskampagner eller generelt bare mere oplysning om aktuelle it-trusler.

En oplysningskampagne kan på den måde også anses for at være en inskription af den nuværende viden om it-angreb. Denne viden inskriberes i en kampagne i form af enten en folder, en video eller andet og repræsenterer samt videreformidler politiets budskab til borgerne. Som tidligere nævnt anvender gerningsmændene ofte tillidsvækkende virksomheder som falske afsendere af deres mails, herunder eksempelvis SKAT eller Nets.

It-ingeniøren mener, at disse virksomheder også har en opgave i at ændre den måde, de kommunikerer med borgerne på: *"Man siger til virksomheder, lad være med at sende links med i jeres mails til kunderne. Sig, at de skal gå ind på deres login-side, så at man vænner folk fra at trykke på links."*. Virksomhederne kan på den måde understøtte folk i at spotte falske e-mails, hvis de ved, at deres egen bank ikke sender links. Ved at oplyse borgerne bedre fjernes en stor mulighed for gerningsmændene, da de på den måde bliver mindre velegnede mål. Dette relaterer sig til den tidligere gennemgang af rutineaktivitetsteorien i forbindelse med it-kriminalitet. Hvis brugerne i Danmark er veloplyste, bliver de mindre oplagte som mål for phishingangrebene. En generel kritik af de situationelle teorier er dog, at det ikke forebygger og forhindrer kriminalitet, men at de blot forskyder det til et andet tidspunkt, sted, metode eller forbrydelsestype - der er altså tale om *crime displacement* (Clarke, 2014, s. 484). Balvig (2017) gennemgår, hvordan ungdomskriminaliteten er på sit laveste nogensinde, men at det kan skyldes en stigende kriminel adfærd på internettet. Det kan være et eksempel på, at kriminaliteten har ændret sig i form, og hvilken platform det begås på, men at kriminaliteten ikke er væk - den er blot flyttet. Balvig (2017, s. 185) forklarer, at den rekordlave ungdomskriminalitet ikke skal ses som et udtryk for, at unge nødvendigvis er mindre kriminelle end tidligere. Hvis ungdomskriminaliteten har flyttet sig til internettet, kan det være et eksempel på, at forebyggelse af kriminalitet ét sted kan have den konsekvens, at kriminaliteten findes et andet sted. I en artikel fra Dansk Erhverv (2018) udtrykker de bekymring for de faldende anmeldelser inden for konventionel kriminalitet og stigning i it-kriminalitet. De mener, at de faldende anmeldelser inden for eksempelvis butikstyveri er et tegn på, at kriminaliteten er rykket over på en ny platform.

6.9 Delkonklusion

Ved at anvende ANT til at besvare og undersøge problemformuleringen er det blevet muligt at få indsigt i de forskellige aktører, som indgår både i phishing- og efterforskningsnetværket. Ud fra analysen kan det konkluderes, at der eksisterer en række udfordringer i forbindelse med bekæmpelse af phishing i Danmark. Det almene politi er ikke gearet til at løse it-relaterede kriminalitetsformer, og derfor er nye aktører som NC3 blevet introduceret med henblik på at støtte efterforskningen. Dog mener NC3, at der stadig er en mangel på ressourcer til efterforskningen af disse sager. Internt i politiet ses der også en forskel, i forhold til hvordan phishinganmeldelser håndteres. Det almene politi

har en reaktiv tilgang til anmeldelserne, mens NC3 også bruger dem proaktivt i form af efterretninger. Der er dog et stort mørketal af omfanget på kriminaliteten, da mange borgere ikke anmelder it-kriminalitet, hvilket hindrer, at flere ressourcer tilføres området.

Der ses også udfordringer i forhold til at opspore gerningsmændene bag phishingangreb. Politiet har udfordringer med at efterforske phishing, fordi gerningsmændene benytter ny teknologi til hele tiden at udvikle nye metoder, og derfor er politiet altid et skridt bagud. Gerningsmænd kan desuden sende flere tusind phishingmails på en dag, mens politiet må efterforske hver sag enkeltvist. Internettet er anarkistisk af natur, og derfor er det udfordrende at finde en praksis for en passende regulering.

Størstedelen af phishingangreb kommer fra udlandet, og derfor må de danske efterforskere ofte samarbejde med internationale aktører. I den forbindelse udfordres efterforskningen af lange sagsbehandlingstider, samt at nogle lande er mere samarbejdsvillige end andre. Det gør, at efterforskningen ofte bliver tung og langtrukken, og derfor må politiet prioritere i phishingsagerne.

Udfordringerne i forbindelse med efterforskningen af phishing gør, at det er en attraktiv kriminalitetsform for gerningsmændene på grund af anonymisering, kryptering og det dynamiske tid- og rumperspektiv, hvilket gør det udfordrende at finde frem til dem. Det afføder ifølge de kriminologiske teorier, at flere udfører phishingangreb, da det er opfattelsen, at få bliver retsforfulgt og straffet. Det ses desuden, at gerningsmændene søger at udnytte borgernes uvidenhed. I den forbindelse er der enighed blandt informanterne om, at oplysning er en vigtig faktor i forebyggelsen af phishing. Mange af de belyste udfordringer i analysen stemmer desuden overens med Browns (2015, 98-100) vurdering af udfordringer med bekæmpelse af it-kriminalitet.

7. Diskussion

Følgende afsnit præsenterer diskussioner af både fund i empirien og teoretiske uenigheder, herunder hvordan ANT bidrager til kriminologisk forskning. Derudover diskuteres også NC3 og Nordjyllands Politis forskellige tilgange til

kriminalitetsbekæmpelse. Disse diskussioner er med til at nuancere og kvalificere den endelige besvarelse af problemformuleringen.

7.1 ANT og kriminologi

I forbindelse med at besvare problemformuleringen er det væsentligt at overveje, hvad kriminalitet egentlig er, og hvordan ANT betragter kriminalitet som fænomen på en anden måde end mange kriminologiske traditioner. En del af Latours kritik af sociologien kan ligeledes anvendes om kriminologien. Latour (2005, 2008) kritiserer sociologien for at betragte "det sociale" som en ingrediens, der kan forklare forhold i samfundet - uden i virkeligheden at forklare noget. I kriminologien bliver det sociale også tilskrevet sit eget domæne, og kriminalitet anses for at være et socialt fænomen (Lam, 2015, s. 51). På den måde har kriminologien haft et binært skel i dens forestillinger af verdenen mellem eksempelvis mennesker som sociale og ting som ikke-sociale fænomener (Brown, 2006, s. 224), som ANT er direkte uenig i. Inden for kriminologien ændres repræsentationen af, hvorfor kriminalitet opstår, afhængigt af hvilke teorier der anvendes. I eksempelvis rutineaktivitetsteorien opstår kriminalitet, når situationen tillader det, hvorimod kriminel adfærd i Cesare Lombrosos teori om *The criminal man* er et medfødt karaktertræk. De kritiske kriminologiske teorier har en forståelse af kriminalitet som noget, der opstår på grund af samfundsstrukturen som et resultat af økonomisk eller politisk konflikt. De har derfor en mere samfundsorienteret tilgang til at forklare kriminalitet, men kriminalitet kan stadigvæk betragtes som et objekt, der opstår på grund af uligheden. På den måde er det den epistemologiske tilgang, der er dominerende, da de forskellige teorier er udtryk for, hvordan kriminalitet som et konstant objekt opstår. Lam (2015, s. 62) kritiserer kriminologien for at gøre kriminalitet til et stabilt objekt, der rent epistemologisk blot betragtes forskelligt af forskellige teorier. Kriminologen Nils Christie (2004) har et andet syn på kriminalitet. Ifølge ham eksisterer kriminalitet ikke, men det skabes, når en handling tillægges en bestemt mening. Men vil det sige, at kriminelle handlinger ikke er virkelige? Johansen (2014, s. 76) forklarer, at det er en misforståelse, at Christie ikke betragter kriminalitet som noget virkeligt, og at han undervurderer skadevirkningen. Christie gør blot opmærksom på, at definitionen af noget som kriminelt kan tilsløre den oprindelige handling. På den måde har Christie en opfattelse af kriminalitet som noget, der ontologisk

forandres, når det konstrueres på forskellige måder i forskellige sammenhænge, og han har derved en del til fælles med Latours opfattelse af kriminalitet som en dynamisk proces. Michel Foucault (1978, s. 93) deler også denne opfattelse af sociale fænomener, da han i sin beskrivelse af magt anser det som værende et relationelt begreb, som kommer til udtryk i relationer mellem individer. Magt er således ikke noget, som kan indfanges, men som kun eksisterer i interaktionen.

ANT i en kriminologisk analyse kan bidrage til et ontologisk syn på kriminaliteten, fordi teorien analyserer, hvordan kriminalitet ontologisk forandres og konstrueres i forskellige aktør-netværk. Tilgangen til kriminalitet som et stabilt objekt er et forsøg på at rydde op i dets rodede natur, men ANT viser, hvordan fænomenet er foranderligt og dynamisk. ANT kan dermed hjælpe os med at gøre op med den klassiske objekt-forståelse af kriminaliteten, og ved at have en ontologisk tilgang i stedet for en epistemologisk fremgår fænomenet som en aktiv ting, der konstrueres løbende, som det interagerer med forskellige aktør-netværk.

I analysen af it-kriminalitet har ANT givet overblik over, hvordan kriminalitet opstår som resultat af associationer mellem aktører i netværk. Det har været muligt at kortlægge, hvilke aktører der er til stede, når kriminaliteten opstår, og hvordan hver aktør agerer i den sammenhæng. På den måde har vi bevæget os væk fra Durkheims forståelse af det sociale som noget givet og mod Latours forståelse af det sociale som resultatet af associationerne i netværket. I en analyse af kriminalitet har ANT yderligere bidraget med en metode til at strukturere empirien, da kortlægningen af aktører viser, hvordan de hænger sammen på kryds og tværs. I en undersøgelse hvor genstandsfeltet er it-kriminalitet, er der mange forskellige aktørtyper til stede, og derfor er det relevant med en analytisk ramme, som inkluderer disse i analysen af kriminaliteten. ANT er en teori inden for det brede forskningsfelt STS, som er et relevant udgangspunkt, når it-kriminalitet skal analyseres. It-kriminalitet er et fænomen, som er opstået som resultat af den teknologiske udvikling, og det er derfor også et emne, der påvirker samfundet og videnskaben. Phishing som it-kriminalitetsform er afhængig af, at den nødvendige teknologi findes. Samtidig påvirker phishing samfundet, borgerne, verdensøkonomien og politiets arbejde. Det har den betydning, at it-kriminalitet er et emne, der er centralt for forskning i det kriminologiske

felt, og det er dermed et eksempel på, hvordan videnskab, teknologi og samfundet påvirker hinanden gensidigt.

Anvendelsen af ANT - og herunder særligt fokus på hvordan associationer etableres gennem translationsprocesser - har dog også givet nogle udfordringer i forbindelse med analysen af kriminalitet. Callons (1984) translationsproces viser, hvordan aktører indgår i en proces med et obligatorisk passagepunkt for hver især at nå deres mål. Men hvordan kan et offer have et mål, der betyder, at vedkommende udsættes for en forbrydelse? I vores anvendelse af translationsprocessen som analyseredskab var det derfor relevant at analysere den manipulation, der finder sted i netværket. Som det illustreres på figur 4, snydes offeret til at tro, at vedkommende sikrer sine oplysninger ved at besvare en phishingmail, mens phishingmailen og gerningsmanden i virkeligheden har en helt anden agenda. Callon selv berører ikke emnet manipulation i sin gennemgang af translationsprocessen, men i vores analyse af kriminalitet blev det tydeligt, hvordan manipulation er en del af det sociale samspil mellem offer og gerningsmand. Det viser, at en vellykket manipulation af offeret er nødvendig, før translationsprocessen gennemføres, og phishingangrebet bliver succesfuldt. Manipulation kan være en form for magt, og på den måde kommer Foucaults (1978, s. 93) perspektiv til udtryk, da han beskriver magt noget abstrakt, som kun eksisterer i relationen mellem individer. Kriminaliteten opstår altså som resultat af translationsprocessen og associationerne mellem aktørerne, og det er præcis det, en ANT-analyse kan vise os. På den måde anses kriminaliteten heller ikke som et stabilt objekt, men som et, der konstitueres i processen mellem aktørerne. I efterforskningen konstrueres det helt anderledes, da aktørerne ikke samarbejder om et succesfuldt phishingangreb, men derimod at finde ud af, hvem gerningsmanden er.

7.2 Gammel vin på nye flasker

Det er en igangværende diskussion, om it-kriminalitet teoretisk er gammel vin på nye flasker, gammel vin på ingen flasker eller helt ny vin på helt nye flasker. ANT som perspektiv på denne debat er også relevant. ANT fordrer en symmetri mellem samfund og natur, og det betyder, at teknologien ikke skal ses som et eksternt fænomen i samfundet, men blot som endnu en aktør i netværket. Den tidligere nævnte kritik af kriminologiens

tendens til at differentiere mellem mennesker og ikke-mennesker er derfor også relevant i forbindelse med diskussionen om gammel vin på nye flasker. Diskussionen insinuerer, at teknologien er noget fremmed og radikalt anderledes end de øvrige aktører i det kriminologiske forskningsfelt som netværk, hvilket går imod ANTs samfundsopfattelse. At teknologien skaber problemer, kan derimod ses som et udtryk for, at det er en aktør, der har været underrepræsenteret og ikke i tilpas omfang er indtænkt i det kriminologiske forskningsfelt af de øvrige aktører. Teknologien kan derfor forråde netværket og være skyld i mere kriminalitet. ANT ser derudover samfundet som en konstant proces mellem aktørerne. Sætningen "gammel vin på nye flasker" implicerer, at den gamle vin stadigvæk findes - altså at kriminologien før og uden teknologien fortsat eksisterer i det nye netværk og kan bruges til en sammenligning. I et ANT-perspektiv konstruerer aktører og netværk hinanden, og derfor forandres kriminologien i sig selv ved at indgå i et netværk med teknologi. Brown (2006, s. 236) pointerer i den sammenhæng, at der ikke er noget, der hedder teknologisk kriminalitet, som er adskilt fra traditionel kriminalitet - kriminaliteten opstår blot i netværk, som indeholder forskellige typer af aktører. Der eksisterer altså aldrig "gammel vin" i ANT-netværk, da aktørerne altid bliver modificeret og ændret.

7.3 Kritik af ANT

ANT er ofte blevet anset som en provokerende teori, og den har også selv været udsat for kritik gennem årene. Ifølge ANT er det væsentligt, at aktørerne ikke vurderes på forhånd, men at forskeren følger aktørerne og lader dem optræde for sig (Latour, 2005, s. 11-12). Derfor kritiserer Winner (1993, s. 374-375) blandt andet, at STS-teorier typisk er deskriptive og kortlægger processen i den teknologiske udvikling, men at de ikke bidrager til en dybere forståelse af, hvad den egentlig betyder, og hvilke konsekvenser den har. Han siger derfor provokerende, at den sorte boks åbnes, men at den er tom (Winner, 1993, s. 374-375). Det hænger også sammen med Lee og Browns (1994, s. 778) kritik om, at ANT søger at forklare alt i samfundet - både teknologier, mennesker, systemer og organisationer, og den afgrænses derfor ikke og tager ikke stilling til sin (manglende) forklaringskraft. Det betyder ifølge Lee og Brown (1994, s. 780), at ANT i et forsøg på at forklare alt ender med ikke at forklare noget.

Et af de mest kritiserede elementer ved ANT er symmetrien mellem menneskelige og ikke-menneskelige aktører. Kritikerne mener, at menneskers intentionalitet adskiller dem fra dyr og ting, og at aktørerne derfor ikke kan sidestilles i en analytisk sammenhæng. Collin og Yearley (1992) kritiserer blandt andet Latour for ikke at underbygge intentionaliteten ved ikke-menneskelige aktører. Som eksempel fremhæver de Latours (1987, s. 221) beskrivelse af, hvordan vinden og bølgerne agerer som allierede i forhold til skibe. Her stiller Collin og Yearley (1992, s. 315) spørgsmålstegn ved, hvordan naturens kræfter kan blive allierede og forklarer, at det skal kunne bevises videnskabeligt, hvis det kan lade sig gøre, før det videnskabeligt kan krediteres. De efterspørger en metodisk underbyggelse af, hvordan ikke-menneskelige aktører kan agere på samme vis som menneskelige aktører, hvilket de kritiserer Latour for ikke at præsentere, men i stedet blot opfinde kreative beskrivelser af (Collin og Yearley, 1992, s. 320). Yderligere kritiseres ANT af blandt andre Susan Leigh Star (1990) for ikke at inkludere magtforhold og marginaliserede grupper i analysen. Eksempelvis kan transkønnede have svært ved at genkende sig selv i heterogene strukturer, og dette tager ANT ikke højde for. ANT bliver på den måde en analyse af samfundet set gennem et standard, heterogent synspunkt (Star, 1990, s. 33). Star (1990, s. 43+53) mener derfor, at en ANT-analyse bør tage udgangspunkt i en marginaliseret aktør, da netværk ofte forekommer stabile for dem, der passer ind i standarden. I vores analyse af et phishingangreb er magtforhold et vigtigt element, da der er tale om en forbrydelse, hvor der er et magtspil mellem offer og gerningsmand. I anvendelsen af ANT og analysen af translationsprocessen viste det sig, at der foregår en manipulation af offeret, når forbrydelsen finder sted. Stars (1990) kritik af, at ANT ikke som udgangspunkt tager højde for magtforhold er til dels rigtig, men i analysen var det netop magtforhold i form af manipulation, der viste sig som "det sociale", der opstod i forbindelsen mellem aktørerne. Vi fandt derfor, at ANT kan anvendes til at belyse, hvordan magtforhold opstår i aktørernes associationer til hinanden. Ved at anvende ANT har vi opnået en forståelse for emnet i stedet for bare at være deskriptive, hvilket Winner (1993) kritiserer teorien for. Vi kan dog til dels anerkende hans pointe om, at vi kunne have opnået en dybere forståelse, hvis der kun havde været fokus på en enkelt aktør. At en undersøgelse kan være deskriptiv, er dog en naturlig konsekvens af ANT, som er en netværksteori og ikke en teori, som kun koncentrerer sig om et enkelt element.

ANT postulerer, at alt konstrueres i forskellige netværk. Det har i sidste ende den betydning, at ANT selv konstrueres forskelligt afhængigt af, hvilket netværk teorien indgår i, og derfor er det besværligt at give et entydigt svar på, hvad ANT er. Den meste kritik af ANT opstår dog, når teorien bliver forsøgt gjort stærk og entydig. Latour (1996, s. 374-375) selv opfordrer derfor til, at ANT fortsat anvendes som en mere vag teori, der kan formes og tilpasses det netværk, den skal indgå i. En del af kritikken af ANT falder således i takt med, at den bliver sværere at definere og modsætte sig. Det betyder dog også, at der findes mange forskellige versioner af teorien, hvilket kan være en styrke, da den kan anvendes på den mest passende måde i netop det netværk, der skal analyseres. Det kan dog også være en svaghed, da ANT anvendes som synonym på de mange forskellige versioner, som hver især har deres implikationer.

7.4 Proaktiv vs. reaktiv kriminalitetsbekæmpelse

Som tidligere nævnt er der en forskel på, hvordan NC3 og Nordjyllands Politi håndterer phishinganmeldelser. Det kan være et spørgsmål om ressourcer, men også et spørgsmål om, om der arbejdes reaktivt eller proaktivt med kriminalitetsbekæmpelsen. I en rapport fra Det Kriminalpræventive Råd (2016, s. 14) har centerchefen for NC3 forklaret, at it-kriminalitet bedst bekæmpes med en proaktiv indsats, da det ellers altid vil være kattens jagt efter musen, når det kommer til it-kriminalitet som phishing. NC3 vurderer, at en mere analytisk tilgang, hvor de generelle it-kriminalitetsformer studeres, er bedre end blot at reagere ud fra de enkelte anmeldelser. Nordjyllands Politi råder anmeldere til at slette phishingmails, men foretager ikke noget aktivt, medmindre der er sket et økonomisk tab:

"(…) man kommer i politiet langt med bare at råde og vejlede i, at de bare skal ignorere det og slette det, fordi det er så masseforekomst. Så det er først i det øjeblik, hvor det ligesom er kommet skridtet videre, hvor der er nogle, der har brugt oplysningerne, at det ligesom bliver til en politisag."

De anvender altså ikke anmeldelserne proaktivt, da de behandler phishingsagerne enkeltvis, fordi de ikke mener, at de kan stoppe, at der sidder tusindvis af kinesere eller russere som sender spam mod Danmark. NC3 har dog en anden tilgang til kriminalitetsbekæmpelsen, da de mener, gerningsmændene kan stoppes, hvis de modtager

anmeldelser nok, så de kan forudsige mønstre i deres adfærd. Informanten fra NC3 udtaler: *"Vi vil gerne have anmeldelsen, også selvom det kun er et forsøg, men så bruger vi det mere som sådan en form for efterretninger (…)"*. Hos NC3 er der altså en mere proaktiv tilgang til bekæmpelse af phishing, hvor de gerne vil have anmeldelser ind, da disse benyttes som efterretninger til bekæmpelse af fremtidige phishingangreb. Denne overgang fra reaktiv kriminalitetsbekæmpelse til en proaktiv berører Lucia Zedner (2007, s. 262), som beskriver, at samfundet generelt er skiftet til at have mere fokus på sikkerhed og proaktiv kriminalitetsbekæmpelse.

Informanterne fra Nordjyllands Politi er almindeligt politiuddannede betjente med en basisuddannelse i it og økonomisk kriminalitet. De er derfor uddannede i at have en reaktiv tilgang til kriminalitet, hvilket kommer til udtryk i deres måde at håndtere phishingsager på. Hos NC3 har de dog indhentet civile eksperter til bekæmpelse af it-kriminalitet. Disse har ikke en politiuddannelse, men derimod en akademisk, og rammerne for hvordan it-kriminalitet bekæmpes er også anderledes end hos det almene politi. Zedner (2007, s. 263) forklarer, at denne udvikling skal ses i takt med, at samfundet bliver mere proaktivt, og derfor bliver flere private aktører introduceret til at varetage sikkerhedsopgaver.

Oplysning og vejledning er forebyggende tiltag, som kan betegnes som proaktive. Dog løser de ikke udfordringen, men begrænser kun skadevirkningen af den. NC3 erkender dog også, at det er en generel udfordring med ressourcer til den proaktive bekæmpelse af phishing:

"Så jeg vil sige, lige nu som ressourcerne er, så har vi selvfølgelig, vi har mange ressourcer til opklaring, men vi har knap så mange ressourcer til den proaktive del af efterforskningen, det vil sige, det der med at vi måske selv sætter os ned og finder ud af, jamen hvor er der huller henne, vi måske kan lukke, før de kriminelle opdager hullerne. Så den proaktive, altså nu kan man sige, at nu er politiet selvfølgelig også en reaktiv enhed, der er sat i verden for at opklare forbrydelsen, men det kan være rigtig svært, og rigtig meget it-kriminalitet kan faktisk forhindres ved en proaktiv indsats, så hvor skal man så lægge sine ressourcer henne, det er jo så det spørgsmål. Der tror jeg, man kan lave rigtig meget, hvis man også satsede proaktivt, men altså der er ikke nok ressourcer, det er der ikke."

Der ses altså fra NC3s side en konkret udfordring ved, at politiet er reaktivt, mens it-kriminalitet som phishing fordrer en proaktiv indsats. Politiet har altid arbejdet reaktivt, og derfor lægges ressourcerne også derefter. Dog har den proaktive tilgang til kriminalitetsbekæmpelse også konsekvenser for samfundet. Holmberg og Kyvsgaard (2003, s. 136) belyser hvordan det danske politis proaktive indsats ofte medfører en høj grad af profilering og deraf også en høj grad af bias. De advarer i den forbindelse om, at proaktiv kriminalitetsbekæmpelse kan føre til diskriminering og fejlprofilering. Derudover forklarer de, at ved en proaktiv indsats kan en kriminalitetstype blive overrepræsenteret og dermed retfærdiggøre en større indsats (Holmberg og Kyvsgaard, 2003, s. 139). I forhold til phishing kan det være en fordel, hvis der kommer mere fokus på kriminalitetsformen, da den i dag er overvejende underrepræsenteret. En proaktiv indsats fra politiet vil betyde, at eventuelle sikkerhedshuller i it-systemer kan lukkes, før gerningsmændene finder frem til dem. Derudover kan efterretningsmæssigt arbejde hjælpe med at forudse potentielle phishingangreb, og politiet kan på den måde drage fordel af en proaktiv tilgang til bekæmpelse af phishing.

8. Konklusion

I Danmark er it-kriminalitet og herunder phishing en stigende udfordring for samfundet. I forskning fra andre lande fremgår det, at der er udfordringer med at bekæmpe phishing effektivt, men der er ikke forsket specifikt i det i en dansk kontekst. Med udgangspunkt i en række ekspertinterviews har dette speciale søgt at afdække, hvilke udfordringer der opstår ved bekæmpelse af phishing i et dansk efterforskningsnetværk. Disse kan sammenfattes til tre overordnede punkter:

1. Udfordringer relateret til efterforskning og lovgivning
2. Udfordringer relateret til anmeldelser
3. Udfordringer i forbindelse med it-kriminalitetens natur

Udfordringerne i forbindelse med efterforskningen relaterer sig især til, hvor tids- og ressourcekrævende det er for politiet at efterforske it-kriminalitet. Efterforskningen kræver ofte, at et internationalt samarbejde etableres, hvilket kan være meget tidskrævende, da sagerne prioriteres forskelligt af de involverede lande. Det problematiseres yderligere af

den store forekomst af it-kriminalitetssager, hvor antallet af sager udfordres af den tid, det kan tage blot at opklare en enkelt sag, fordi det er kompliceret at finde gerningsmændene, som ofte benytter sig af teknologiske hjælpemidler til at maskere deres aktivitet og lokation. Der ses desuden en forskel på, hvordan Nordjyllands Politi og NC3 håndterer phishinganmeldelser. Nordjyllands Politi arbejder hovedsageligt reaktivt, hvorimod NC3 arbejder mere proaktivt mod phishing ved at anvende anmeldelser som efterretninger. Phishing er en kriminalitetsform, som i nogle tilfælde kan bekæmpes proaktivt ved at begrænse gerningsmændenes muligheder, og det kan derfor ses som en udfordring, at politiet traditionelt er en reaktiv enhed. Flere af informanterne forklarede, at de tror, at forebyggende oplysningskampagner er det mest effektive tiltag mod phishing. Den danske lovgivning er derudover udformet med udgangspunkt i den fysiske verden, og det kan betyde, at it-kriminalitet som phishing kan være svær at passe ind i den eksisterende lovgivning, som til tider kan være mangelfuld, da den digitale udvikling skaber nye muligheder for kriminalitet. Det skaber den udfordring, at det kan være nødvendigt at strække den eksisterende lovgivning for at få den til at passe på it-kriminalitet.

Udfordringerne relateret til anmeldelser af it-kriminalitetssager har også betydning for politiets efterforskning. Selvom antallet af databedragerisager har været stigende i Danmark, er det politiets opfattelse, at phishing ikke i særlig høj grad anmeldes af borgerne, hvilket skaber en negativ spiral, hvor der ikke bliver tilført flere ressourcer til bekæmpelse af kriminaliteten. Hvis borgerne ikke anmelder forsøg på phishing, betyder det også, at det ikke er muligt at danne sig et fyldestgørende billede af, hvor mange der udsættes for kriminaliteten, samt hvilke virkemidler gerningsmændene bruger og derudfra udforme konkrete proaktive tiltag. Derfor er en af udfordringerne ved at bekæmpe phishing i Danmark, at der foreligger et stort mørketal. Det besværliggøres yderligere, da phishingsager i politiets statistik kategoriseres under databedrageri, hvilket gør det svært at lave en distinktion mellem phishing og andre typer af it-kriminalitet og overskue omfanget af phishing i Danmark.

Dette relaterer sig yderligere til den sidste identificerede udfordring med it-kriminalitetens natur. Der kan gå lang tid, fra et phishingangreb startes, til offeret opdager, at vedkommende har været udsat for noget kriminelt. Derfor kan det være svært for offeret

at give en kvalitativ anmeldelse til politiet, som derved får sværere ved at opklare forbrydelsen. Dertil kan offeret og gerningsmanden være på stor afstand af hinanden, og internettets dynamiske tid- og rumsammensætning gør det kompliceret at finde ud af, hvor gerningsmanden befinder sig, samt hvor og hvornår angrebet er startet. Phisherne kan med brug af internettet sende flere tusind phishingmails på kort tid, men det tidskrævende internationale samarbejde og de begrænsede ressourcer har den konsekvens, at der sker en yderligere skævvridning af sagsbehandlingen, fordi politiet er nødt til at koncentrere sig om de største sager. Samtidig er phishing ofte organiseret som en virksomhed, hvor bagmændene holder sig i det skjulte og får andre til at udføre opgaverne for sig. Det betyder, at det er svært at bekæmpe kriminaliteten, fordi bagmændene ikke stoppes og derfor kan fortsætte deres angreb. Det har yderligere den konsekvens, at potentielle it-gerningsmænd ikke afskrækkes, da disse kun i lav grad retsforfølges og straffes.

Udfordringerne er identificeret gennem en række semistrukturerede interviews med eksperter inden for forskellige felter, som er analyseret med Latours (2005, 2008) aktør-netværksteori som metodisk og teoretisk værktøj. I litteraturen er der ikke tidligere eksempler på, at ANT har været anvendt til at analysere phishing som kriminalitetsform. Ved brug af Callons (1984) translationsproces til at analysere dynamikken i et vellykket phishingangreb er det muligt at belyse, hvordan manipulation af offeret til at indgå i forhandlinger med de øvrige aktører er væsentligt for, at forbrydelsen finder sted. Vi har dog ikke set tidligere eksempler på translationsprocessen anvendt til at belyse en kriminel handling, og vi fandt derfor, at manipulation er et væsentligt begreb i ANT-sammenhæng, når kriminalitet studeres med teorien som analytisk ramme. Vi har som sagt taget udgangspunkt i eksisterende forskning i phishing fra udlandet, og resultaterne i dette speciale bekræfter på flere områder, at mange af de samme udfordringer gør sig gældende i Danmark, hvilket hænger sammen med, at it-kriminalitet af natur er et transnationalt fænomen og derfor udgør mange af de samme udfordringer i forskellige lande. Foruden de empiriske fund har vi dog også klarlagt, hvordan det er muligt at bruge ANTs translationsproces til at synliggøre aktørernes dynamik i netværk, hvor kriminaliteten finder sted.

Med udgangspunkt i denne undersøgelse kan vi konkludere, at der er brug for yderligere forskning på området i en dansk kontekst. Dette speciale har identificeret udfordringerne ved at bekæmpe phishing i Danmark, og derfor kan yderligere undersøgelser med fordel analysere mulige løsninger på disse. Herunder ville det også være interessant med flere undersøgelser, hvor ANTs translationsproces benyttes til at analysere netværk, hvori kriminaliteten opstår som dynamik mellem offer, gerningsmand og teknologi.

9. Litteraturliste

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, *68*, 160–196. https://doi.org/https://doi.org/10.1016/j.cose.2017.04.006

Ankersborg, V. (2011). *Specialeprocessen - Tag magten over dit speciale!* København: Samfundslitteratur.

Armor. (2018). *The Black Market Report - A Look Inside the Dark Web*. Richardson.

Balvig, F. (2017). *Fra barndommens gade til et liv i cyberspace*. Det Kriminalpræventive Råd. Retrieved from https://dkr.dk/media/9798/fra-barndommens-gade-til-cyberspace-web.pdf

Beccaria, C. (2014). An Essay on Crimes and Punishments. In F. T. Cullen, R. Agnew, & P. Wilcox (Eds.), *Criminological Theory: Past to Present, essential readings* (5th ed., pp. 27–30). New York: Oxford University Press.

Berlingske. (2018). Paraderne op: Her prøver it-kriminelle at snyde dig nu. Retrieved May 30, 2019, from https://www.berlingske.dk/dine-penge/paraderne-op-her-proever-it-kriminelle-at-snyde-dig-nu

Birk, D., Gajek, S., Grobert, F., & Sadeghi, A. (2007). Phishing Phishers - Observing and Tracing Organized Cybercrime. In *Second International Conference on Internet Monitoring and Protection* (pp. 1–6). https://doi.org/10.1109/ICIMP.2007.33

Bogner, A., Littig, B., & Menz, W. (2009). Introduction: Expert Interviews – An Introduction. In A. Bogner, B. Littig, & W. Menz (Eds.), *Interviewing Experts* (pp. 1–16). Hampshire: Palgrave Macmillan.

Brinkmann, S., & Tanggaard, L. (2010). Introduktion. In S. Brinkmann & L. Tanggaard (Eds.), *Kvalitative Metoder - En Grundbog* (pp. 18–29). København K: Hans Reitzels Forlag.

Brown, C. S. D. (2015). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology*, *9*(1), 55–119. https://doi.org/10.5281/zenodo.22387

Brown, S. (2006). The criminology of hybrids - Rethinking crime and law in technosocial networks. *Theoretical Criminology*, *10*(2), 223–244. https://doi.org/10.1177/1362480606063140

Brown, S. E., Esbensen, F.-A., & Geis, G. (2013). *Criminology: Explaining Crime and Its Context* (8th ed.). Waltham: Anderson Publishing.

Bryman, A. (2012). *Social Research Methods*. (A. Bryman, Ed.) (4th ed.). New York: Oxford University Press.

Callon, M. (1984). Some elements of a sociology of translation: domestication of the scallops and the fishermen of St Brieuc Bay. *Sociological Review*, *31*(S1), 196–223. https://doi.org/10.1111/j.1467-954X.1984.tb00113.x

Christie, N. (2004). *A Suitable Amount of Crime*. New York: Routledge.

Christmann, G. B. (2009). Expert Interviews on the Telephone: A Difficult Undertaking. In A. Bogner, B. Littig, & W. Menz (Eds.), *Interviewing Experts* (pp. 157–183). Hampshire: Palgrave Macmillan.

Citron, D. K. (2016). *Hate Crimes in Cyberspace*. USA: Harvard University Press.

Clarke, R. V. (2014). Situational Crime Prevention. In F. T. Cullen, R. Agnew, & P. Wilcox (Eds.), *Criminological Theory: Past to Present, essential readings* (5th ed., pp. 480–489). New York: Oxford University Press.

Clough, J. (2010). *Principles of Cybercrime*. Cambridge: Cambridge University Press.

Cohen, L. E., & Felson, M. (2014). Routine Activity Theory. In F. T. Cullen, R. Agnew, & P. Wilcox (Eds.), *Criminological Theory: Past to Present, essential readings* (5th ed., pp. 469–479). New York: Oxford University Press.

Collin, F. (2003). *Konstruktivisme*. Frederiksberg: Roskilde Universitetsforlag.

Collins, H. M., & Yearley, S. (1992). Epistemological Chicken. In A. Pickering (Ed.), *Science as Practice and Culture* (pp. 301–326). Chicago: University of Chicago Press.

Cornish, D. B., & Clarke, R. V. (2014). Crime as a Rational Choice. In F. T. Cullen, R. Agnew, & P. Wilcox (Eds.), *Criminological Theory: Past to Present, essential readings* (5th ed., pp. 437–443). New York: Oxford University Press.

Curtis, S. R., Rajivan, P., Jones, D. N., & Gonzalez, C. (2018). Phishing attempts among the dark triad: Patterns of attack and vulnerability. *Computers in Human Behavior*, *87*, 174–182. https://doi.org/10.1016/j.chb.2018.05.037

Dansk Erhverv. (2018). De kriminelle er blevet mere digitale. Retrieved May 16, 2019, from https://www.danskerhverv.dk/presse-og-nyheder/nyheder/de-kriminelle-er-mere-digitale/

Deacon, D., Pickering, M., Golding, P., & Murdock, G. (2007). *Researching Communicantions*. London: Bloomsbury Publishing.

Demant, J., & Dilkes-Frayne, E. (2015). Situational Crime Prevention in Nightlife Spaces: An ANT Examination of PAD Dogs and Doorwork. In D. Robert & M. Dufresne

(Eds.), *Actor-Network Theory and Crime Studies - Explorations in Science and Technology* (pp. 5–19). Farnham, England: Ashgate Publishing.

Demetriou, C., & Silke, A. (2003). A Criminological Internet 'Sting'. Experimental Evidence of Illegal and Deviant Visits to a Website Trap. *A British Journal of Criminology*, *43*(1), 213–222. https://doi.org/10.1093/bjc/43.1.213

Det Kriminalpræventive Råd. (2016). *Når forbrydelser bliver digitale*. Glostrup.

Det Kriminalpræventive Råd. (2019a). It-kriminalitet i tal. Retrieved February 20, 2019, from https://www.dkr.dk/it/it-kriminalitet-i-tal/

Det Kriminalpræventive Råd. (2019b). Hvordan måles kriminalitet? Retrieved March 1, 2019, from https://www.dkr.dk/kriminalitet-og-forebyggelse/hvordan-maales-kriminalitet/

Digitaliseringsstyrelsen, & DKCERT. (2017). *Danskernes informationssikkerhed 2016*. Kgs. Lyngby. Retrieved from https://digst.dk/media/13800/danskernes-informationssikkerhed-2016.pdf

Digitaliseringsstyrelsen, & DKCERT. (2018). *Danskernes informationssikkerhed 2018*. Kgs. Lyngby. Retrieved from https://digst.dk/media/18755/danskernes_informationssikkerhed_december_2018_191218.pdf

Dion, M. (2010). Advance Fee Fraud Letters as Machiavellian/Narcissistic Narratives. *International Journal of Cyber Criminology*, *4*(2), 630–642.

Douillet, A.-C., & Dumolin, L. (2015). Actor Network Theory and CCTV Development. In D. Robert & M. Dufresne (Eds.), *Actor-Network Theory and Crime Studies - Explorations in Science and Technology* (pp. 21–35). Farnham, England: Ashgate Publishing.

Finans Danmark. (2019). Netbankindbrud og phishing. Retrieved March 1, 2019, from http://finansdanmark.dk/toerre-tal/institutter-filialer-ansatte/kriminalitet/netbankindbrud-og-phishing/

Foucault, M. (1978). *The History of Sexuality: Volume 1: An Introduction*. New York: Pantheon Books.

Gad, C., & Jensen, C. B. (2007). Post-ANT. In C. B. Jensen, P. Lauritsen, & F. Olesen (Eds.), *Introduktion til STS - Science, Technology, Society* (pp. 93–118). København K: Hans Reitzels Forlag.

Grabosky, P. (2001). Virtual Criminality: Old Wine in New Bottles? *Australian Institute of Criminology, Australia*, *10*(2), 243–249. https://doi.org/https://doi.org/10.1177/a017405

Grabosky, P. (2016). *Cybercrime - Keynotes in Criminology and Criminal Justice Series*. New York: Oxford University Press.

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, *28*(12), 3629–3654. https://doi.org/10.1007/s00521-016-2275-y

Hedström, K., Dhillon, G., & Karlsson, F. (2010). Using Actor Network Theory to Understand Information Security Management. In K. Rannenberg, V. Varadharajan, & C. Weber (Eds.), *Security and Privacy – Silver Linings in the Cloud* (pp. 43–54). Berlin, Heidelberg: Springer. https://doi.org/https://doi.org/10.1007/978-3-642-15257-3_5

Hirschi, T. (2014). Social Bond Theory. In F. T. Cullen, R. Agnew, & P. Wilcox (Eds.), *Criminological Theory: Past to Present, essential readings* (5th ed., pp. 229–237). New York: Oxford University Press.

Holmberg, L., & Kyvsgaard, B. (2003). Are Immigrants and Their Descendants Discriminated against in the Danish Criminal Justice System? *Scandinavian Studies in Criminology and Crime Prevention*, *4*(2), 125–142.

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in Progress - Theory and prevention of technology-enabled offenses*. New York: Routledge.

Jaishankar, K. (2008a). Space Transition Theory of Cyber Crimes. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283–301). Pearson.

Jaishankar, K. (2008b). Identity related Crime in the Cyberspace: Examining Phishing and its impact. *International Journal of Cyber Criminology*, *2*(1), 10–15. Retrieved from http://www.cybercrimejournal.com/Editorialijccjan2008.htm

Jansen, J., & Leukfeldt, E. R. (2016). Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization. *International Journal of Cyber Criminology*, *10*(1).

Jensen, C. B. (2010). STS. In S. Brinkmann & L. Tanggaard (Eds.), *Kvalitative Metoder* (pp. 375–388). Frederiksberg: Hans Reitzels Forlag.

Jensen, C. B., Lauritsen, P., & Olesen, F. (2007). Introduktion. In C. B. Jensen, P. Lauritsen, & F. Olesen (Eds.), *Introduktion til STS - Science, Technology, Society* (pp. 7–15). København K: Hans Reitzels Forlag.

Johansen, N. B. (2014). Kriminalitetens eksistens - kategorisk form og stoff. *Nordisk Tidsskrift for Kriminalvidenskab*, *1*, 70–83.

Konradt, C., Schilling, A., & Werners, B. (2016). Phishing: An economic analysis of cybercrime perpetrators. *Computers and Security*, *58*, 39–46. https://doi.org/10.1016/j.cose.2015.12.001

Kruize, P. (2009). *Identitetstyveri*. København K. Retrieved from http://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/2011/2009/Rapport_identitetstyveri.pdf

Kruize, P. (2013). *Kriminalitet i en digitaliseret verden*. København K. Retrieved from https://www.dkr.dk/media/10083/kriminalitet-i-en-digitaliseret-verden-samlet-rapport.pdf

Kruize, P. (2018). *Internetkriminalitet 2017*. København V. Retrieved from https://www.dkr.dk/media/13026/internetkriminalitet-2017-final.pdf

Kvale, S., & Brinkmann, S. (2009). *Interview - Introduktion til et håndværk*. København K: Hans Reitzels Forlag.

Lam, A. (2015). Making Crime Messy. In D. Robert & M. Dufresne (Eds.), *Actor-Network Theory and Crime Studies - Explorations in Science and Technology* (pp. 51–65). Farnham, England: Ashgate Publishing.

Latour, B. (1987). *Science in Action - How to Follow Scientists and Engineers through Society*. Cambridge: Harvard University Press.

Latour, B. (1996). On actor-network theory: A few clarifications. *Soziale Welt*, *47*(4), 369–381. Retrieved from https://www.jstor.org/stable/40878163

Latour, B. (1999). *Pandora's Hope - Essays on the Reality of Science Studies*. Cambridge: Harvard University Press.

Latour, B. (2005). *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford: Oxford University Press.

Latour, B. (2008). *En ny sociologi for et nyt samfund*. København K: Akademisk Forlag.

Lee, N., & Brown, S. (1994). Otherness and the Actor Network - The Undiscovered Continent. *American Behavioral Scientist*, *37*(6), 772–790.

Leukfeldt, E. R. (2014). Phishing for Suitable Targets in The Netherlands: Routine Activity Theory and Phishing Victimization. *Cyberpsychology, Behavior, and Social Networking*, *17*(8), 551–555. https://doi.org/10.1089/cyber.2014.0008

Li, S., & Schmitz, R. (2009). A novel anti-phishing framework based on honeypots. In *2009 eCrime Researchers Summit* (pp. 1–14). https://doi.org/10.1109/ECRIME.2009.5342609

Lindsø, A. (2019). Plastvirksomhed udsat for it-kriminalitet: Snydt for tocifret millionbeløb. Retrieved May 30, 2019, from https://plast.dk/2019/02/plastvirksomhed-udsat-for-it-kriminalitet-snydt-for-tocifret-millionbeloeb/

Luppicini, R. (2014). Illuminating the Dark Side of the Internet with Actor-Network Theory: An Integrative Review of Current Cybercrime Research. *Global Media Journal - Canadian Edition*, *7*(1), 35–49.

Moore, D., & Singh, R. (2015). Seeing Crime: ANT, Feminism and Images of Violence Against Women. In D. Robert & M. Dufresne (Eds.), *Actor-Network Theory and Crime Studies - Explorations in Science and Technology* (pp. 67–80). Farnham, England: Ashgate Publishing.

Nets A/S. (2019). Aktuelle phishing eksempler - Advarsel mod phishing-mails, snyde-sms'er og fup telefonopkald. Retrieved May 3, 2019, from https://www.nets.eu/dk-da/digital-sikkerhed/Pages/Phishing.aspx

Nørgaard, C. (2018). Tillidsfulde danskere snydes af it-kriminelle. Retrieved May 30, 2019, from https://www.dr.dk/nyheder/regionale/nordjylland/tillidsfulde-danskere-snydes-af-it-kriminelle

Ordnet. (2019). Anarkisme. Retrieved May 13, 2019, from https://ordnet.dk/ddo/ordbog?query=anarki&tab=for

Pedersen, K. L. (2019). Dansk cyberchef: »Cyberkriminalitet er den mest risikofri kriminalitetsform, der findes«. Retrieved April 16, 2019, from https://finans.dk/tech/ECE11132353/dansk-cyberchef-cyberkriminalitet-er-den-mest-risikofri-kriminalitetsform-der-findes/?ctxref=ext

Politi. (2019). Politiets Statistikbank. Retrieved May 24, 2019, from https://statistik.politi.dk/QvAJAXZfc/opendoc.htm?document=QlikApplication%2F2999_Public%2FPublic_IndsatsResultater.qvw

Reyns, B. W., & Henson, B. (2015). The Thief With a Thousand Faces and the Victim With None. *International Journal of Offender Therapy and Comparative Criminology*, 1–21. https://doi.org/10.1177/0306624X15572861

Sharp, R. (2010). *CIT-AWARE-09 - En undersøgelse af it-sikkerhed blandt borgerne i Danmark*. Kgs. Lyngby. Retrieved from http://orbit.dtu.dk/files/4369904/tr10_07-1.pdf

Shipley, T., & Bowker, A. (2014). *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*. Waltham: Elsevier.

Stafford, M. C., & Warr, M. (2014). Reconceptualizing Deterrence Theory. In F. T. Cullen, R. Agnew, & P. Wilcox (Eds.), *Criminological Theory: Past to Present, essential readings* (5th ed., pp. 431–442). New York: Oxford University Press.

Star, S. L. (1990). Power, technology and the phenomenology of conventions: on being allergic to onions. *The Sociological Review, 38*(1), 26–56.

Tanggaard, L., & Brinkmann, S. (2010). Interviewet: Samtalen som forskningsmetode. In S. Brinkmann & L. Tanggaard (Eds.), *Kvalitative Metoder - En Grundbog* (pp. 29–53). København K: Hans Reitzels Forlag.

Thomas, D., & Loader, B. D. (2000). Introduction - Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. In D. Thomas & B. D. Loader (Eds.), *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age* (pp. 1–14). New York: Routledge.

Vendius, T. T. (2015). *Europol & cyberkriminalitet – proaktiv efterforskning og forbrydelser mod børn*. København K: Ex Tuto.

Wagen, W. Van Der, & Pieters, W. (2015). From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks. *British Journal of Criminology*, *55*(3), 578–595. https://doi.org/https://doi.org/10.1093/bjc/azv009

Wagen, W. Van Der, & Pieters, W. (2018). The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory. *European Journal of Criminology*, *3*(1), 400–420. https://doi.org/https://doi.org/10.1177/1477370818812016

Wall, D. (2001). Cybercrimes and the Internet. In D. S. Wall (Ed.), *Crime and the Internet* (pp. 1–17). New York: Routledge.

Waschke, M. (2017). *Personal Cybersecurity - How to Avoid and Recover from Cybercrime*. Washington, USA: Apress.

Winner, L. (1993). Upon Opening the Black Box and Finding It Empty: Social Constructivism and the Philosophy of Technology. *Science, Technology, & Human Values*, *18*(3), 362–378.

Yar, M. (2005). The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407–427. https://doi.org/101177/147737080556056

Zedner, L. (2007). Pre-crime and Post-criminology? *Theoretical Criminology*, *11*(2), 261–281. https://doi.org/10.1177/1362480607075851

Aas, K. F. (2007). *Globalization & Crime*. London: SAGE Publications.

10. Bilagsoversigt

- Bilag 1: Transskription – Birgit Feldtmann
- Bilag 2: Transskription – Peter Kruize
- Bilag 3: Transskription – Torbjørn Bonde-Jensen
- Bilag 4: Transskription – Nicolai Larsen
- Bilag 5: Transskription – Jesper Thy og Søren Nielsen