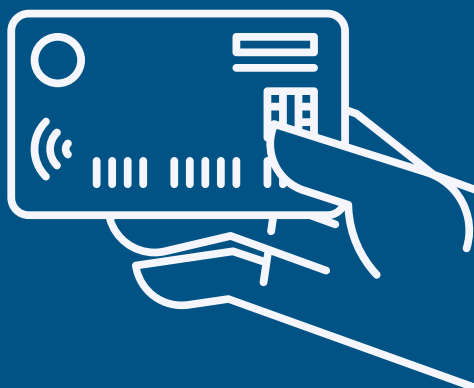
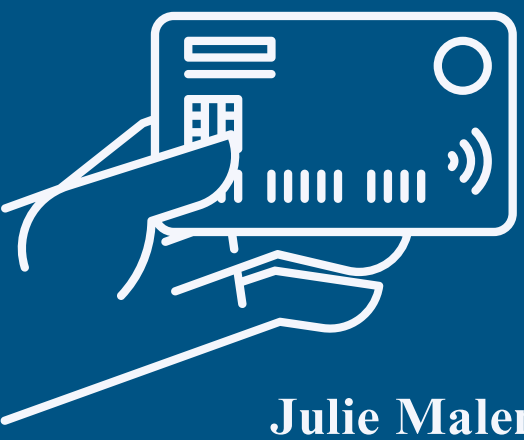
KORTLÆGNING AF BANKBUDSBEDRAGERI I DANMARK

Kandidatspeciale på Kriminologiuddannelsen
Vejleder: Rasmus Munksgaard
Antal anslag: 191.988
Aalborg Universitet
Den 03.06.2025





Julie Malene Thomsen & Freja Hvilsom Andersen

GAI-erklæring

I denne specialeafhandling er der anvendt *generativ artificial intelligence* (GAI) i overensstemmelse med Aalborg Universitets gældende retningslinjer (Aalborg Universitet, 2025). Vi har i nogen grad anvendt GAI som støtteværktøj til korrekturlæsning og sproglige forbedringer af tekstafsnit, der oprindeligt er udarbejdet af os selv. Endvidere har vi anvendt programmet 'Transcriber' til transskription af vores fire ekspertinterview.

Abstract

This thesis investigates the organization of a specific and emerging type of fraud in Denmark, known as “bank courier fraud” (*bankbudsbedrageri*). The research is based on legal documents involving seven criminal networks operating across the country with more than 360 victims, as well as expert interviews conducted with police representatives and banking professionals. Adopting an exploratory mixed methods approach, this study provides insights into several key elements: offender characteristics, network mobility and lifespan, modus operandi (including scripts, withdrawal strategies, and activity patterns), manipulation techniques, victim profiling, and financial gains. The study identifies a profitdriven crime with significant economic losses associated with the fraud, totalling at least 5,6 mio. dkk.

The findings reveal a high degree of professionalization, strategic planning, and the targeted exploitation of elderly women as victims. The fraud scheme is characterized by a clear hierarchical structure and division of roles. At the top are unknown orchestrators who maintain a central and controlling position. They recruit young men, typically with substance abuse issues and criminal records, to serve as couriers. These couriers are interchangeable and occupy the lowest level in the hierarchy, where they are exposed to a high risk of detection. In addition, the networks involve call agents and external actors, forming a multi-layered structure optimized for operational efficiency and financial gain. Our findings suggest that these networks operate with a high degree of professionalism and strategic planning. The perpetrators demonstrate efficiency and geographic mobility. The fraudsters are trained in persuasive techniques and know exactly how to act when interacting with victims.

From a criminological perspective, the findings highlight potential strategies for situational crime prevention. This includes adapting institutional procedures, enhancing victim resilience through public awareness campaigns, and implementing physical and procedural barriers in cash withdrawal processes. Ultimately, the study expands the understanding of cyber-enabled, contact fraud and provides a foundation for developing more effective prevention strategies.

Indholdsfortegnelse

1. Begrebsafklaring

It-kriminalitet / It-relateret økonomisk kriminalitet

Dette betyder, kriminalitet der er foretaget ved brug internettet/ kriminalitet foretaget ved brug af internettet, som har et økonomisk sigte (DKR, 2025; NCIK, 2025).

Spoofing

Spoofing er en betegnelsen for en svindelmetode, hvor svindlere via særlig teknologi forfalsker deres identitet og ringer op fra telefonnumre, der ikke er deres (Griffin & Rackley, 2008; Tjek det, 2025).

Modus Operandi (modus)

Modus operandi er en latinsk frase, som oversættes 'måde at operere på'. I en kriminalitets-sammenhæng referer udtrykket sig til ordet 'fremgangsmåde' (LII, 2000).

Kontaktbedrageri

Bedrageri, hvor der har været et element af kontakt mellem forurettede og gerningsperson (NSK, 2025).

Phishing / vishing

Phishing betyder, at svindlere udsender af falske e-mails, sms'er, links eller lignende, med henblik på at få offeret til at afgive følsomme oplysninger (Sikker Digital, 2025). *Vishing er en form for phishing, hvor svindlere, anvender telefonopkald til at narre ofre til at afsløre fortrolige oplysninger eller overføre penge* (Song et al., 2014).

2. Problemfelt

I følgende afsnit gør vi indledningsvist rede for danskernes digitale tilstedeværelse. Dette gøres for at belyse at der eksisterer en betydelig mængde potentielle ofre for It-relateret kriminalitet. På baggrund af danske data, giver vi indsigt i antallet af anmeldelser af It-relateret økonomisk kriminalitet, baseret på en årsrapport fra Nationalt Center for It-Kriminalitet (NCIK) samt data fra Finans Danmark, som dokumenterer de omfattende økonomiske konsekvenser, der er forbundet med denne form for kriminalitet. Der inddrages yderligere en juridisk forståelse af bedrageri og databedrageri, med henblik på at illustrere de juridiske rammer, herunder det strafbare aspekt ved bedrageri. Formålet er samlet set at undersøge bedrageriformen, *bankbudsbedrageri* (herefter BBB).

2.1 Danskernes digitale tilstedeværelse og trusselsbillede

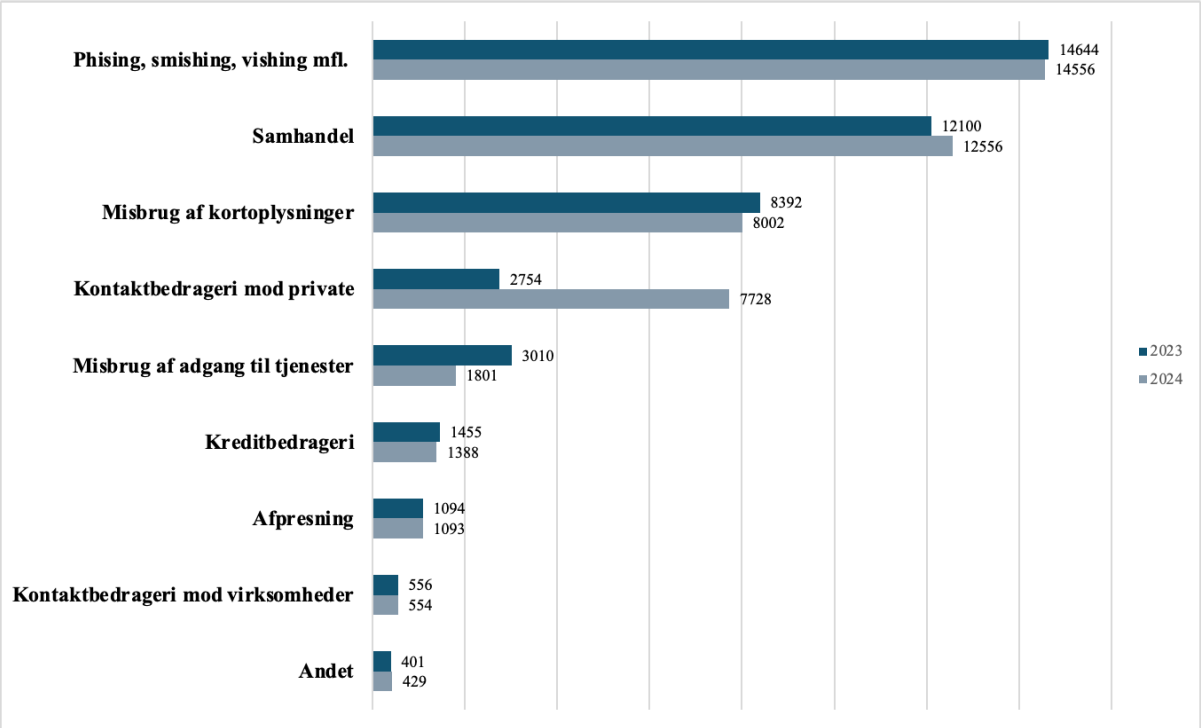
I løbet af de sidste årtier har den teknologiske udvikling og digitalisering revolutioneret de måder, hvorpå vi kommunikerer, interagerer og omgås med andre individer (Holt et al. 2022:2-3; Holt & Bossler, 2015:1). Den teknologiske udvikling har ført til en omfattende online-tilstedeværelse blandt størstedelen af den danske befolkning, hvilket har skabt en stor mængde potentielle ofre for It-relateret kriminalitet. Ifølge Danmarks Statistik ejede ni ud af ti danske familier i 2022 en eller flere smartphones (Danmarks Statistik, 2023). Endvidere rapporteres der, at 86 pct. af befolkningen mellem 16-74 år er online flere gange dagligt, samt at 98 pct. af befolkningen i alderen 15-89 år har anvendt internettet inden for de sidste tre måneder (Jacobsen et al. 2024:21). Denne omfattende tilstedeværelse gør befolkningen mere sårbar over for it-relateret kriminalitet. Dette understreges yderligere af regeringens 'Nationale strategi for cyber- og informationssikkerhed 2022-2024', hvor truslen for IT-relateret kriminalitet vurderes som værende "*meget høj*", og det formodes, at denne trussel vil forblive på et højt niveau i fremtiden (Regeringen, 2021:7; Moos-Bjerre A/S, 2024:9).

I forlængelse heraf, viser en offerundersøgelse fra Justitsministeriet, at næsten 190.000 danskere i 2023 blev udsat for It-relateret kriminalitet (Pedersen & Balvig, 2024:152). Alle aldersgrupper kan udsættes for dette, men der er forskel på, hvilke typer af IT-relateret kriminalitet grupperne udsættes for. Yngre borgere oplever oftere bedrageri i forbindelse med online handel, mens ældre borgere i højere grad udsættes for kontaktbedrageri (Moos-Bjerre A/S, 2024:12; NCIK, 2023:18).

2.2 It-relateret økonomisk kriminalitet i Danmark - udvikling og tendenser

NCIK har udgivet en årsrapport omhandlende anmeldelser indenfor IT-relateret økonomisk kriminalitet i 2024. Denne inddrages, for at give et indblik i det stigende antal anmeldelser af kriminalitetsformen. I 2024 modtog NCIK 39.824 anmeldelser vedrørende IT-relateret økonomisk kriminalitet, hvilket er 4.738 mere end i 2023, svarende til en stigning på 14 pct. Sammenlignet med 2020 er antallet af anmeldelser steget med 40 pct., hvilket udgør en markant stigning af anmeldelser (NCIK 2025:4). Hvorvidt denne stigning afspejler en reel vækst i antallet af sager, en øget anmeldelsestilbøjelighed, eller større politisk bevågenhed, kan være vanskeligt at fastslå. Uanset årsagsforklaringen ses der en stigning i antallet af sager i årsrapporten. Fordelingen af de anmeldte kriminalitetstyper samt antallet af sager fremgår af nedenstående oversigt.

Figur 1 - Fordeling af kriminalitetstyper



Kilde: Baseret på tal fra NCIK Årsrapport 2024.

I ovenstående oversigt kan der ses en betydelig variation i antallet af anmeldelser for de forskellige typer af kriminalitet samt, om antallet af anmeldelser er stigende eller faldende. Særligt

kategorien 'Kontaktbedrageri mod private' viser en markant stigning på 181 pct. i antallet af anmeldte sager fra 2023 til 2024. Denne form for kriminalitet er således i vækst og fremstår umiddelbart som særlig attraktiv for kriminelle. Derfor ønsker vi at bidrage med øget viden om denne samfundsudfordring. Ifølge NCIK er denne stigning:

> "*et klart tegn på en fortsat tendens om, at kriminelle i stigende grad bruger social engineering til at manipulere forurettede til selv at overføre penge eller udlevere oplysninger*" (NCIK, 2025:4).

Det er således en udfordring at svindlere i stigende grad udnytter privatpersoners tillid og manipulerer dem til at handle imod deres egen interesse. Dette bliver ofte kaldt S*ocial Engineering* (herefter SE), hvilket kan beskrives som en teknik, hvor en gerningsperson anvender psykologiske greb, for at manipulere den forurettede til at udføre en handling i god tro, som forurettede ellers ikke ville have udført (Center for Cybersikkerhed, 2022:6). Dette kan f.eks. ske ved at gerningspersonen pålægger tidspres, udviser empati, eller vækker en autoritetstro hos personen.

Når svindlere gør brug af SE, kan det for ofrene både resultere i økonomiske tab og psykiske konsekvenser, bl.a. i form af skyldfølelse, skam og mistillid til digitale systemer og myndigheder (Salahdine & Kaabouch, 2019:14; NCIK, 2024:51). Det, der gør SE særligt udfordrende, er, at teknikken udnytter menneskelige svagheder snarere end tekniske sårbarheder. Uanset hvor stærkt et sikkerhedssystem måtte være, kan en menneskelig interaktion mellem offeret og gerningspersonen stadig føre til, at den enkelte bliver narret til at afsløre fortrolige oplysninger (Salahdine & Kaabouch, 2019:1). SE kan dermed ikke forebygges ved at blot at lukke et teknologisk smuthul.

En yderligere udfordring består i at svindlerne løbende tilpasser deres metoder i takt med, at der opstår nye og mere profitable svindelstrategier. Dog bliver ofrene også gjort mere opmærksomme på eksisterende svindeltyper. Endvidere opnår myndigheder samt finansielle institutioner tilmed større succes med at forhindre bedrageri (Regeringen, 2021:7; Thorning, 2025; Moos-Bjerre A/S, 2024:11). På baggrund af dette er der, set fra svindlernes synsvinkel, et behov for kontinuerlig innovation og tilpasning for at kunne bibeholde økonomisk profit.

2.3 Bankbude - kontaktbedrageri i vækst

Den ovennævnte betydelige af mængde potentielle ofre, den markante stigning i kontaktbedragerier mod private samt svindlernes evne til løbende at tilpasse deres fremgangsmåder peger på et område, der kalder på en nærmere undersøgelse. På baggrund heraf retter vi vores fokus mod en særlig underkategori af kontaktbedrageri, som arbejder ud fra ét specifikt modus, *bankbudsbedrageri*.

Historisk set er et bankbud, også kaldet en bankbetjent, en person der er ansat i en bank til at udføre praktiske opgaver, f.eks. til at bringe og afhente dokumenter hos kunder (ordnet.dk, 2025). Brugen af disse er blevet udfaset grundet digitaliseringen i 1980'erne, hvorfor danskerne er gået fra fysiske bankservices til digitale værktøjer (Danske Bank, 2025).

I NCIK's årsrapport inddrages der forskellige former for kontaktbedrageri (NCIK, 2025:8), men vi ønsker som nævnt ovenfor, at gå i dybden med BBB. I årsrapporten refereres der til fænomenet som 'sikkerhedskonto' (Ibid.), mens Finans Danmark og Politiet benævner det som 'bankbudsbedrageri' (Midt- og Vestjyllands Politi 2024; Racina, 2025). Medierne omtaler det bl.a. som 'bankbudsbedrageri', 'falske bankbude' og 'bankbudssvindel' (Petersen, 2025; Kristiansen, 2025; Danielsen, 2024). Dette indikerer således, at fænomenet omtales ud fra forskelligartede betegnelser, hvorfor det endvidere kan være svært at afgrænse og måle (jf. afsnit 2.4).

'Sikkerhedskonto' fremgår for første gang som selvstændig kategori i årsrapporten, hvilket er med til at tydeliggøre, at det udgør en aktuel problemstilling. Sikkerhedskonto som kategori, dækker over:

> "*sager, hvor gerningspersonen kontakter forurettede telefonisk og typisk udgiver sig for at være fra deres bank eller politiet. De bliver herefter lokket til at overføre penge til en "sikker" konto, som gerningspersonen råder over"* (NCIK, 2025:8).

I 2024 blev der anmeldt 692 sager af sådanne karakter.

Finans Danmark definerer ligeledes deres forståelse af BBB. Ifølge dem, anvender gerningspersonerne en fremgangsmåde, hvor de kontakter ofrene telefonisk og udgiver sig for at være fra deres bank. Svindlerne fortæller ofrene, at der foregår mistænkelig aktivitet på deres konto,

hvorefter de tilbyder at hjælpe med at overføre pengene til en "sikker" konto. Pengene ender dog ikke på en sikker konto, men bliver i stedet overført til kontoer styret af svindlerne (Racina, 2025).

BBB har store økonomiske konsekvenser, og i de første 10 måneder af 2024 blev der svindlet for 20,5 mio. kr. fordelt på 1.390 anmeldte sager. Det svarer til næsten fem sager om dagen med et gennemsnitligt økonomisk tab på 14.707 kr., pr. sag (Ibid.).

NCIK og Finans Danmark benytter en omtrent ensartet terminologi for BBB. På baggrund af deres definitioner og den indledende research, forstår vi *bankbudsbedrageri* som en kriminel handling, hvor gerningspersonen tager kontakt til offeret under påskud af at være en repræsentant for offerets bank, og gennem manipulation bedrager offeret med henblik på økonomisk vinding.

2.4 Bankbudsbedrageri - i juridisk forstand

BBB er i overordnet forstand karakteriseret som værende *økonomisk kriminalitet*. Inden for den økonomiske kriminalitet er en underkategori af lovovertrædelser defineret som *berigelseskriminalitet* (eller formueforbrydelser), som det fremgår af straffelovens kapitel 28 (Jakobsen, 2015:89). Berigelseskriminalitet betyder at en gerningsperson begår en strafbar handling med henblik på at opnå økonomisk vinding. De forskellige former for berigelseskriminalitet inkluderer *tyveri*, *røveri*, *underslæb* og herunder også *bedrageri*. Bedrageri som kriminalitetsform adskiller sig fra andre berigelsestyper, idet gerningspersonen ikke selv på egen hånd stjæler eller tilegner sig vinding, men i stedet får en anden person til at overdrage enten penge eller værdigenstande, hvorfor offeret lider et tilsvarende tab. Bedrageri optræder derfor som udgangspunktet ved, at gerningspersonen 'snyder' sit offer, hvorfor der ofte indgår en form for manipulation. Denne manipulation kommer i juridiske forstand til udtryk ved som straffeloven tilskriver det; *at udnytte en vildfarelse.*

Bedrageri ved brug af falske bankbude vil derfor kunne straffes efter straffelovens § 279, når bankbudenes vildledende handlinger resulterer i at de lykkedes med at opnå uberettiget økonomisk gevinst på en andens persons bekostning. STRL. § 279 lyder som følgende:

> *"For bedrageri straffes den, som, for derigennem at skaffe sig eller andre uberettiget vinding, ved retsstridigt at fremkalde, bestyrke eller udnytte en vildfarelse bestemmer en anden til en handling eller undladelse, hvorved der påføres denne eller nogen, for hvem handlingen eller undladelsen bliver afgørende, et formuetab."* (jf. Straffelovens § 279)

Gerningspersoner kan ikke blot bringes til strafferetligt ansvar jf. bedrageribestemmelsen, men også efter bestemmelsen vedrørende databedrageri jf. STRL. § 279a. De to bestemmelser er tilnærmelsesvis ens, med adskiller sig fra hinanden i det omfang, at der ved § 279 indgår et menneskeligt element, og derved menneskelig kontakt, som ses når bankbuddet henvender sig på forurettedes adresse. Ved § 279a indgår et elektronisk element. Det består i manipulation af tal, data eller programmer for derigennem at skaffe økonomisk vinding. I forbindelse med BBB, vil der bl.a. være tale om databedrageri, når en gerningsperson misbruger forurettedes betalingsoplysninger og digitale identitet. Når gerningspersonen har opnået adgang til offerets betalingsmidler og efterfølgende foretager kontanthævninger i en hæveautomat, 'manipulerer' gerningspersonen, så at sige, hæveautomaten. Databedrageri kan endvidere bestå i den indledende eller generelle *phishing*.

For at opsummere vil der således i de fleste hændelsesforløb indenfor BBB, indledningsvist blive begået databedrageri gennem indledende SMS og opkaldssvindel, dernæst "almindeligt" bedrageri ved at franarre offeret hævekort og betalingsoplysninger, igen efterfulgt af databedrageri når disse misbrugs og kortets anvendes til at foretage kontanthævninger (Hameed et. al, 2025).

Strafferammen for denne type kriminalitet er særdeles bred, men vil som udgangspunkt bestå i bødestraf eller fængsel indtil 1 år og 6 måneder jf. STRL. § 285 stk. 1. I de tilfælde hvor bedrageriet er karakteriseret som værende af særlig grov beskaffenhed, hvilket jf. bestemmelsen i STRL. § 286 stk. 2 indebærer at der er anvendt en særlig udførelsesmetode, mange gentagende bedragerier, at der er tale om organiseret kriminalitet eller at der er opnået en betydelig økonomisk vinding, kan gerningsperson straffen med op til 8 års fængsel.

Som det fremgår af ovenstående afsnit, er BBB er et særligt fænomen, hvor der opereres med mange termer og betegnelser alt afhængigt af, om det anskues fra et juridisk ståsted eller ej. Fænomenet er specielt i juridisk forstand, fordi de typiske sagskomplekser og hændelsesforløb

som regel har elementer af flere kriminalitetstyper, herunder både kontaktbedrageri (STRL. § 279) og databedrageri (STRL. § 279a). Når der i specialets ordlyd refereres til BBB hvor der kan pålægges strafferetligt ansvar, henvises der således til både bedrageri og databedrageri.

2.5 Opsummering og problemformulering

På baggrund af det ovenstående problemfelt står det klart, at BBB udgør en aktuel og kompleks problemstilling, som nødvendiggør en mere dybdegående forståelse af fænomenet. Dette incitament bygger på, at der findes mange potentielle ofre for IT-relateret økonomisk kriminalitet. Ud fra det stigende antal af anmeldelser af sager, indikerer det, at mange individer allerede er blevet ofre for denne kriminalitetsform. BBB har omfattende økonomiske og psykologiske konsekvenser for både ofrene og samfundet som helhed. Det er derfor særligt problematisk, at gerningspersonerne udviser en høj grad af innovation og tilpasningsevne i deres metoder. Dette er med til at øge deres mulighed for at begå og gentage kriminaliteten med succes. Derudover er BBB karakteriseret ved en vis juridisk kompleksitet, idet handlingerne ofte falder inden for flere strafferetlige kategorier. Med afsæt i, at BBB er både avanceret og aktuelt, tilstræber vi at opnå en øget viden om denne kriminalitetsform for således, at skabe bedre forudsætninger for at mindske forekomsten af kriminalitetsformer som denne. Vi finder det derfor aktuelt at kortlægge hele bankbudsbedrageriet trin for trin, hvorfor denne specialeafhandling udgangspunkt i følgende problemformulering:

Hvordan organiseres bankbudsbedragerisager fra start til slut?

3. Teoretiske perspektiver på bankbudsbedrageri

I følgende afsnit fremhæves en række teoretiske perspektiver, der kan anvendes som forståelsesramme for BBB. BBB kan opfattes som en form for kriminalitet, der har elementer fra flere forskellige kriminalitetskategorier, grundet de forskellige stadier som sådanne sagskomplekser typisk gennemgår. Heriblandt kan der på baggrund af de mange facetter, ses elementer af både cyberkriminalitet, økonomisk kriminalitet, og kontaktbedrageri. Det kan derfor være udfordrende at navigere i på en præcis og ensartet måde. Afhængigt af kontekst, fagområde og juridiske rammer kan forskellige betegnelser skabe uklarhed og gøre både formidling og analyse mere kompleks. Endvidere kan kriminalitetstyper være drevet af forskellige rationaler og motivationer, hvilket findes væsentligt at have for øje i følgende afsnit. På den baggrund, har afsnittet til formål at konkretisere hvordan BBB kan betragtes fra et kriminologisk perspektiv. Med udgangspunkt i cyberkriminalitet og profitdrevet kriminalitet som primært fokus afdækkes de forståelsesrammer, vi lægger til grund BBB.

3.1 Perspektiver på cyberkriminalitet

Dette afsnit har til formål at belyse nogle af de forskellige perspektiver, der beskæftiger sig med afgrænsningen og definitionen af cyberkriminalitet, samt vores egen forståelse af cyberkriminalitet. Indledende research har vist, at BBB indebærer teknologiske elementer, da svindlerne f.eks. kontakter ofrene telefonisk som en del af svindelakten. Det findes derfor relevant at afklare, hvad cyberkriminalitet indebærer, og om BBB kan kategoriseres som en form for cyberkriminalitet. En af udfordringerne ved at undersøge cyberkriminalitet er, at kriminalitetsformen både er kompleks og under konstant udvikling.

3.1.1 Cyberkriminalitet i bred forstand

I det følgende afsnit indleder vi med en bred introduktion til cyberkriminalitet. Herefter vil vi gradvist indsnævre fokus og fordybe os i udvalgte forståelser.

Der findes ingen universel definition af cyberkriminalitet (Viano, 2017:3), og forskellige definitioner inddrager forskellige niveauer og omfang af specialiseret viden og teknologi (Holt et al. 2022:10; Wall, 1998:2; Lusthaus 2012:72). Nogle forskere ser cyberkriminalitet som en konventionel kriminalitetstype udført med ukonventionelle metoder, mens andre betragter cyberkriminalitet som langt mere paradigmeskiftene og nyt (Lusthaus, 2024:379). Lusthaus

(2024) har præsenteret en bredere definition af cyberkriminalitet, baseret på flere forskeres forståelser af cyberkriminalitet. Denne forståelse anser cyberkriminalitet som "*a range of illegal activities taking place within cyberspace, rather than as a particular subset of crimes"* (Ibid.:371). Ifølge denne brede forståelse, er cyberkriminalitet ikke bare en type kriminalitet, men snarere et samlet fænomen, der dækker over flere former for ulovlige handlinger der sker i cyberspace (Ibid.). Fordelen ved at anvende denne brede definition er at den giver en mere helhedsorienteret forståelse af fænomenet, eftersom den ikke afgrænses som en bestemt type kriminalitet, der finder sted i det digitale rum. Endvidere er cyberkriminalitet et nyere fænomen, der udvikler sig i takt med teknologien, og ved ikke at begrænse cyberkriminalitet til en bestemt kategori tillader definitionen inklusion af nye former for cyberkriminalitet. Dog kan denne manglende præcision også være en ulempe, da det kan skabe en uklarhed om, hvilke specifikke handlinger der falder ind under cyberkriminalitet. Derudover præciserer definitionen ikke hvorvidt de kriminelle handlinger kun foregår i cyberspace, eller om det kan være ulovlige (offline) handlinger, der bliver effektiviseret ved brug af teknologi. Sammenfattende tilbyder denne brede definition en omfattende ramme for forståelse af cyberkriminalitet, men dens manglende specificering kan skabe udfordringer i praksis indenfor både forskning og retssystemet.

3.1.2 Teknologiske niveauer af cyberkriminalitet - en todelt forståelse

En anden forståelse, der forsøger at opveje ovenstående definitions mangler, er en todelt forståelse af cyberkriminalitet. Ifølge en rapport af UK Home Office, forstås cyberkriminalitet som "*... an umbrella term used to describe two distinct but closely related criminal activities: cyber-dependent and cyber-enabled crimes*" (Lusthaus, 2024:372; McGuire & Dowling, 2013:5). Cyber-afhængig kriminalitet (*cyber-dependent crimes)* er lovovertrædelser, der kun kan begås ved brug af en computer, computernetværk eller en anden form for informations- og kommunikationsteknologi (IKT). Eksempler på sådanne forbrydelser inkluderer spredning af virus, hacking samt distribuerede DDoS-angreb, hvilket betyder at internetservere overbelastes med det formål at lamme netværksinfrastruktur eller hjemmesider. Der kan derfor betragtes en kriminalitetsform, der kun kan forekomme ved brugen af teknologi (Lusthaus 2024:372; McGuire & Dowling, 2013:5). Dette forstås som kriminalitet begået af 'true cybercriminals', og kan derfor opfattes som en mere rendyrket form for cyberkriminalitet. Cyber-aktiveret kriminalitet (*cyber-enabled crimes*) er traditionel kriminalitet, hvis omfang eller rækkevidde forstærkes ved brug af computere, computernetværk eller anden IKT. I modsætning til cyber-

afhængig kriminalitet kan cyber-aktiveret kriminalitet stadig begås uden brug af teknologi (Ibid.).

I modsætning til den førstnævnte definition er UK Home Offices forståelse mere detaljeret i forhold til brugen af teknologi. En sådan afgrænsning af teknologiens rolle kan være fordelagtig, da det skaber bedre forudsætninger for praktisk anvendelse, f.eks. i forhold til lovgivning og retshåndhævelse (Lusthaus, 2024:381). Dette bidrager til en mere struktureret forståelse af, hvordan teknologi spiller en rolle i kriminalitet, og gør det lettere at identificere og håndtere forskellige former for cyberkriminalitet. Dog er en udfordring ved denne forståelse selve kategoriseringen, da nogle kriminelle handlinger ikke nødvendigvis passer entydigt ind i én af de to kategorier, men snarere udgør en kombination med elementer fra begge. Hacking kan f.eks. bruges til at udføre sabotage (Ibid.:380). Som nævnt udvikler teknologien sig hurtigt, hvilket medfører, at nogle forbrydelser enten ændrer karakter eller integrerer aspekter fra begge kategorier. Denne kompleksitet vanskeliggør en fast opdeling og kan resultere i, at visse former for kriminalitet ender i en gråzone, hvor alt ikke bliver tilstrækkeligt indfanget af de eksisterende kategorier.

3.1.3 Den anvendte definition af cyberkriminalitet

Vi finder det fordelagtigt at vælge en bred og simpel forståelse af cyberkriminalitet, hvorfor Lusthaus' egen definition: "*cybercrime is crime that makes use of digital technology in a significant way*" (Lusthaus, 2024:381) vil anvendes i specialet Denne definition findes bedst egent eftersom den adskiller cyberkriminalitet fra de forbrydelser, der ikke engagerer sig med teknologi. Endvidere har den også 'bløde grænser', hvilket skaber mulighed for at både "rendyrket" cyberkriminalitet og konventionel kriminalitet med teknologiske aspekter, kan inddrages. Den sikrer, at cyberkriminalitet kan strække sig over et større teknologisk spektrum, som kan variere fra lav inddragelse til høj inddragelse af teknologi (Ibid). I relation til spørgsmålet om, hvorvidt BBB er teknologisk styret eller understøttet, vurderes vi, at der ikke umiddelbart er belæg for at karakterisere kriminalitetsformen som fuldkommen cyber-afhængig. I stedet betragter vi den som en traditionel bedrageriform, der anvender teknologiske redskaber til at øge sin effektivitet og rækkevidde.

3.1.4 Et kriminologisk perspektiv på bankbudsbedrageri som cyberkriminalitet

Eftersom der er blevet etableret en grundlæggende forståelse for hvordan vi betragter cyberkriminalitet, vil det efterfølgende afsnit være en sammenkobling af cyberkriminalitet, kriminologiske perspektiver og BBB. Vi anvender Lusthaus' definition som rammesættende forståelse af cyberkriminalitet, dog tages der højde for de elementer, der indgår i de andre forståelser. Dette funderes ud fra tanken om, ikke at underkende andre eksisterende forklaringer, men blot fremhæve den forståelse der tilstrækkeligt indfanger fænomenet, for netop det, vi har til hensigt at undersøge.

3.1.5 Cyber-aktiveret bankbudsbedrageri som rationelt valg

Den indledende undersøgelse af BBB har belyst, at bedrageri kan tolkes som værende en traditionel kriminalitetsform, der ikke er opstået på baggrund af teknologiens udvikling. Tanken om at '*snyde gamle mennesker for deres penge*' er en form for svindel der har eksisteret længe (Smith, 2000:276-277), og det er således hverken nyt eller bemærkelsesværdigt at det er det modus de kriminelle anvender for at opnå profit. Dog er den nutidige svindel i højere grad præget af teknologiske foranstaltninger, samt nye, tilpassede metoder, der ikke før har været anvendt (Braun, 2024). Vi antager, at en udvikling som denne er sket, eftersom kriminelle aktører har opdaget, at det er mere effektivt at begå kriminalitet ved hjælp af teknologi, f.eks. til at skabe adgang til et stort antal potentielle ofre. I dag er internetadgang og digitale enheder udbredt og let tilgængelige i stort set alle dele af verden, hvilket betyder, at gerningspersonerne ikke er fastlåst i tid og sted. De har mulighed for at nå en større gruppe ofre uden rent geografisk at være forbundet til dem. En yderligere fordel ved teknologiens muligheder er de forbedrede forudsætninger for anonymitet, idet gerningspersonen kan operere bag en skærm, hvilket samtidig reducerer risikoen for opdagelse (Kripos, 2023:13-14; Grubb, 2010; Holt et al., 2020:13-14). På baggrund af sådanne fordele, og set gennem *Rational Choice-perspektivet* (RCT) fremstår det derfor logisk, at cyber-aktiveret kriminalitet er en attraktiv kriminalitetsform. Den teknologiske effektivisering styrker svindlernes muligheder for at handle nyttemaksimerende og opnå størst mulig profit. RCT bygger på antagelsen om, at kriminelle aktører foretager en bevidst kalkulation af deres kriminelle handlinger ved at afveje den potentielle gevinst mod risikoen for straf. Således, desto mere profit der er i sigte, desto større villighed er der for at begå kriminalitet. Ifølge RCT er kriminelle handlinger ikke et resultat af impulsive beslutninger, men derimod snarere, rationelle og velovervejede beslutninger (Cullen et al. 2021:405, Cornish & Clarke 2021:425).

Med afsæt i cyberkriminalitet, tolker vi i forlængelse heraf BBB som en form for cyberkriminalitet, hvor vi formoder vi BBB, har nogle af de samme rationelle overvejelser om profit og nyttemaksimering, hvorfor det med fordel kan opfattes indenfor forståelsesrammen om det rationelle valg. Endvidere blev det i afsnit 2.3 påvist, at BBB udgør en økonomisk indbringende kriminalitetsform, og i redegørelsen af fænomenet blev det klarlagt at BBB indebærer teknologiske elementer, uden at være udelukkende cyber-afhængig.

Dette teoretiske perspektiv er dog ikke uden begrænsninger. RCT forholder sig ikke direkte til, at kriminelle handlinger i visse tilfælde kan være irrationelle, impulsive eller udføres i affekt, og dermed ikke nødvendigvis udspringer af en bevidst kalkuleret afvejning om profit og risikoen for at blive opdaget. Endvidere antager teorien, at gerningspersonen besidder tilstrækkelig information til at foretage en nytte-/risikovurdering, hvilket i praksis ikke altid kan være tilfældet, da kriminelle handlinger ofte vil være præget af uforudsete faktorer. Desuden underkendes samfundsmæssige, sociale eller kulturelle påvirkninger (Herfeld, 2022). RCT kan således ikke alene forklare, hvorfor visse gerningspersoner vælger at begå BBB, men kan i samspil med andre teoretiske perspektiver, skabe forståelse for BBB.

3.1.6 Cyber-afhængig bankbudsbedrageri som rutineaktivitet

I andre elementer af BBB har teknologien en mere afgørende rolle. Det blev igennem den indledende research tydeliggjort, at nogle svindlere både anvender *spoofing* og køber datapakker (såkaldte fullz) på *the dark web* (Hameed et. al, 2025). Handlinger som disse ville isoleret set kunne betragtes som *cyber-afhængige.* Dog er de blot i denne henseende, ét led i et længere hændelsesforløb. Datapakkerne indeholder f.eks. viden om ofre der tidligere har været udsat for phishing-scams, og således har opgivet personfølsomme oplysninger, som svindlerne efterfølgende sælger videre. Vi vælger at fremhæve det teoretiske perspektiv, *Routine Activity Theory* (RAT), da vi finder den bedst egnet til at forklare hvordan rutineaktiviteter påvirker både frekvensen og sandsynligheden for BBB. Teorien kan som årsagsforklaring betragte kriminalitetsraterne i forhold til de rutinemæssige aktiviteter i hverdagslivet (Cohen & Felson, 1979:589). Dette undersøges som regel ud fra elementerne om; *attraktive mål, en motiveret gerningsperson* samt *fraværet af vogtere*. Cohen og Felsons (1979) forklaring bygger på, at selvom antallet af potentielle ofre og motiverede gerningspersoner forblev på et stabilt niveau

i et samfund, vil forandringer i rutineaktiviteter stadig ændre sandsynligheden for, at de forskellige komponenter mødes i tid og rum. Det betyder, at det ikke er tilstedeværelsen af de tre elementer der er afgørende, men i stedet sammenstødet mellem deres rutiner.

Med dette teoretiske afsæt ser vi, at teknologiske løsninger er hjælpemidler, til at udvælge de mest ideelle ofre. Tilstedeværelsen af potentielle ofre, og muligheden for at svindle dem, vil ifølge RAT afhænge af konvergensen af daglige rutiner, steder og tidspunkter. Desuden kan sandsynligheden for BBB øges hvis den baseres på en erfaring om rutineaktiviteter blandt specifikke persongrupper. I afsnit 2.1 har vi identificeret mønstre i hvilke personer der rammes af denne kriminalitetsform. Konkret fremgår sårbare grupper såsom ældre, enlige og demente borgere (Moos-Bjerre A/S, 2024:12; NCIK, 2023:18, Winchester, 2021). Med Christies (1986) tankegang om *ideelle ofre* for øje, fremstår disse persongrupper som *idealofre*, der kan betragtes som de mest legitime ofre i samfundet. Ifølge Christie, opfattes nogle offergrupper som mere legitime end andre i brede befolknings øjne, fordi de opfylder en række kriterier. Kriterierne indebærer bl.a. at ofrene er svage, er i færd med respektable opgaver, og er uden ansvar for deres egen udsathed (Christie, 1986:18-19). Sårbare grupper som nævnt ovenfor kan således placeres i en position, hvor de både fremstår som særligt attraktive ofre for gerningspersoner og samtidig anerkendes af samfundet som de mest "rigtige" eller legitime ofre. For en nærmere forståelse heraf, vil vores datamateriale inddrages senere i analysen i relation til teorien, for at undersøge, hvilke unikke rutiner der bevirker at netop disse ofre er sårbare og hvorfor.

Herudover er det vores forståelse, at rutineaktivitet understreger, at forekomsten af kriminalitet ikke alene afhænger af målet, men tilsvarende også af hvordan rutinerne i samfundet påvirker tilstedeværelsen – eller fraværet, af beskyttelse og sikkerhedsforanstaltninger (Cohen & Felson, 1979:590). Når vi anskuer BBB som værende cyber-afhængigt kriminalitet ser vi, hvordan forankrede rutiner, såsom automatiserede digitale arbejdsgange (f.eks. Netbank og MitID), begrænset menneskelig overvågning eller forsinket kontrol fra myndigheder eller pengeinstitutter, kan skabe et tidsrum og et scenarie hvor beskyttelsen er svag eller fraværende. Dette fravær, ser vi, gennem RAT som et element der øger sandsynligheden for at den motiverede gerningsperson bryder igennem sikkerhedsforanstaltninger og således får gunstige betingelser for at begå forbrydelsen. Den motiverede gerningsperson fungerer som en af de tre komponenter hvorigennem rutinerne undersøges, hvorefter sandsynligheden for at kriminalitet forekommer

kan vurderes. En målrettet gerningsperson er, ikke overraskende, en grundlæggende forudsætning for at kriminalitet opstår (Cohen & Felson, 1979:589). Med dette for øje, finder vi, at gerningspersonen ikke tilfældigt er til stede, men i stedet handler inden for rammerne af en rutinepræget adfærd, hvor muligheden for kriminalitet søges og udnyttes.

Ligesom ved foregående teori om RCT forekommer der lignende begrænsninger ved vores anvendelse af RAT. Disse indebærer et koncentreret fokus på situationelle forhold frem for overvejelsen af de strukturelle forhold. Endvidere rettes opmærksomheden mod 'den motiverede gerningsperson', dog tillægges det ingen betydning hvorfor gerningsperson er motiveret for sine handlinger. Teorien kalder ikke på nærmere undersøgelse, hverken om individets adfærdsmæssige og psykologiske mekanismer eller baggrundsmæssige og sociale forhold. Ved en afvejning af fordele og ulemper i forhold til brugen af teorien er vores vurdering imidlertid, at teoriens styrker opvejer for dens begrænsninger, når den anvendes i det henseende at undersøge BBB.

Vores opfattelse af BBB forstås som illustreret i ovenstående perspektiv, ikke som en "rendyrket cyberkriminalitet", men som en kriminalitetsform, der har elementer af cyberkriminalitet – det ses f.eks. som nævnt, ved opkøbning af *fullz* eller anvendelsen af *spoofing*. Dette finder sted, samtidigt med at der er elementer af konventionel kriminalitet, såsom svindleakter der er rettet mod sårbare individer. Kombinationen heraf, resulterer i, at der nu kan opleves elementer af konventionel kriminalitet i BBB der er opgraderet og effektiviseret ved hjælp af teknologien. Denne forståelsesramme danner således grundlaget for den ramme, der anvendes i specialet til at definere omfanget af cyberkriminalitet i sager om BBB.

3.2 Perspektiver på predatory crime

Ifølge Naylor (2003), kan økonomisk kriminalitet forstås som *profit-drevet kriminalitet*, hvilket gør det muligt at sammenligne de mange forskellige former for økonomisk kriminalitet på tværs. Fælles for al profit-drevet kriminalitet er, at der hersker et primært formål om at tilegne økonomisk vinding (Naylor, 2003:83). Forsøget på at skabe en kriminologisk forståelsesramme for profit-drevet kriminalitet har længe være besværliggjort af, at de traditionelle paradigmer hovedsageligt har været designet til at fremhæve 'hvem' og 'hvorfor' snarere end 'hvad' og 'hvordan' (Ibid.:81). Forståelsesramme afviger fra traditionelle perspektiver, idet den anskuer

det egentligt resultat og formål med en række handlinger, og ikke blot hvilke metoder der anvendes af gerningspersoner til at indfri dette. Perspektivet giver dermed anledning til en mere abstrakt tækning med den fordel, at skabe et sammenligningsgrundlag på tværs af forskellige svindelformer. Det kan i følge Naylor bunde i, at kriminologiens opgave har været at understøtte retssystemets behov i at retsforfølge, efterforske og straffe, hvorfor der på den baggrund har manglet belæg for at identificere hvad der ud fra en økonomisk logik adskiller den ene forbrydelse fra den anden. Der er derfor behov for en anden viden, end den der afdækkes i retssystemet, når hensigten er at forstå modus for BBB (Ibid.:82). Med andre ord, har økonomisk kriminalitet historisk set været *gerningsmandsbaseret* snarere end *procesbaseret*. Perspektiver som Naylors har dog kastet nyt lys over de traditionelle tendenser, hvorfor der kan anspores et ændret fokus, der i højere grad retter sig mod situationelle forebyggelsesmodeller og mod analyse af de faktiske mål for kriminelle handlinger. I denne ombæring udspringer samtidigt idéen om, at forbrydelser følger 'scripts' hvilket gør det muligt for at inddele dem i en række isolerede og konkrete handlinger, som er uafhængig af identiteten på den specifikke gerningsperson (Ibid.:81).

3.2.1 Bankbudsbedrageri som predatory crime

Naylor opererer med tre hovedkategorier indenfor profit-drevet kriminalitet 1) *predatory crime;* kriminelle handlinger der involverer den ulovlige omfordeling af eksisterende rigdom, 2) *market-based crimes;* kriminelle handlinger der involverer den ulovlige optjening af ny indkomst, og 3) *commercial crimes;* kriminelle handlinger der involverer en ulovlig omfordeling af lovligt optjent indkomst (Naylor, 2003:84-89).

Når fænomenet betragtes ud fra Naylors terminologi, er BBB en form for økonomisk kriminalitet, der falder ind under kategorien *predatory crime*. Det skyldes at bedragerierne kombinerer psykologisk manipulation, teknologisk udnyttelse og økonomisk bedrag, med henblik på økonomisk vinding. Da det endelige mål er at redistribuere værdi via bedrag, definerer vi BBB som værende predatory crime. BBB adskiller sig fra andre former for økonomisk kriminalitet, fordi det både handler om en ulovlig maksimering af profit, men også om et bevidst og målrettet misbrug af magtforhold og tillid hos privatpersoner. Ud fra vores kendskab, kan dette komme til udtryk gennem psykisk pres og vildledning, som resulterer i at de forurettede typisk, bliver narret til aktivt selv at overlevere betalingskort og pinkoder under falske forudsætninger. Denne klassificering fremhæver det direkte og aggressive aspekt af bedraget, hvor bankbudene aktivt

opsøger og udnytter deres ofre. I den forbindelse understreger forståelsen af BBB som predatory crime, hvordan økonomisk svindel ikke kun er et juridisk problem, men også et socialt og etisk spørgsmål, som må forventes, kan være på bekostning af samfundets mest sårbare grupper.

4. Eksisterende forskning

I den indledende kortlægning af forskning om BBB, har vi, efter bedste evne, forsøgt at identificere eksisterende forskning på området. Det har dog ikke været muligt at finde akademiske studier, der omhandler BBB i en dansk kontekst. Vi har i stedet inddraget international forskning, der beskæftiger sig med beslægtede former for bedrageri, karakteriseret ved både brugen af teknologi og økonomiske tab. Vores interesse har især været rettet mod, hvordan beslægtede former for svindel organiseres og udføres, hvilke økonomiske konsekvenser de medfører, samt hvilke persongrupper der i særlig grad udsættes for denne type kriminalitet.

Vi har udvalgt syv forskningsartikler fra Japan, Holland, Sydkorea og Storbritannien (Choi et al., 2017; Eguchi et al., 2024; Jansen & Leukfeldt, 2015; Jones et al., 2021; Loggen & Leukfeldt, 2022; Lusthaus et al. 2024; Euno et al., 2022; van't Hoff-de Goede et al., 2024), som opfylder vores kriterier og bidrager til at belyse fænomenet ud fra aspekter som gerningsmændenes fremgangsmåder, svindelens organisering, de økonomiske tab og offerprofiler. Inddragelsen af den eksisterende forskning af beslægtede svindelformer, bidrager til at underbygge vores analytiske fund. De fællestræk, der identificeres på tværs af svindeltyper og kontekster, kan således styrke validiteten af vores resultater og øge den analytiske generaliserbarhed.

4.1 Svindelmetoder og økonomisk omfang

I følgende afsnit afdækkes gerningspersonernes metoder og teknikker, de organisatoriske strukturer bag svindelnetværk og de økonomiske konsekvenser denne svindelform har.

Eguchi et al. (2024) undersøger i et japansk studie, hvordan gerningspersoner systematisk udvælger ældre borgere som ofre for såkaldt 'special fraud'. Dette indebærer, at svindlerne ringer til ofrene og udgiver sig for at være enten en autoritet eller et familiemedlem for at få dem til at overføre penge til svindlernes konto. Gerningspersonen kan også møde op i offerets hjem efter opkaldet og direkte modtage kontanter og/eller dankort (Eguchi et al. 2024:150). Fremgangsmåden, ved først at skabe en relation via telefon, for dernæst at iscenesætte en tilsyneladende legitim grund til at udlevere personfølsomme oplysninger, stemmer overens med de teknikker, vi indledningsvist har set ved BBB i Danmark. Den japanske forskning demonstrerer, at denne svindelmetode ikke er ny, men kan tilpasses til forskellige kontekster.

Et studie foretaget af Jansen og Leukfeldt (2015) analyserer 600 phishing- og malwarehændelser, indsamlet fra en hollandsk bank, hvor svindlere udgav sig for at være fra banken. Undersøgelsen bidrager med viden om ofrenes adfærd under svindelprocessen og giver os et indblik i hvordan lignende online svindel er foregået i udlandet. Ud af de 600 hændelser er 300 relateret til phishing (Jansen & Leukfeldt, 2015:24). Svindlen blev typisk indledt med, at det potentielle offer modtog en e-mail, et telefonopkald eller blev ramt af en virus. I 46 tilfælde skete svindlen via telefonisk kontakt. Denne fremgangsmåde er særligt relevant i specialets fokus på BBB, idet denne form for kriminalitet ligeledes involverer et telefonisk element. Under samtalen udgav gerningspersonen sig for at være ansat i offerets bank og præsenterede en tilsyneladende troværdig fortælling, f.eks. at der var en sikkerhedstrussel mod offerets konto. Hvis offeret accepterede forklaringen, fulgte vedkommende typisk svindlerens instruktioner, for at "sikre" pengene. Hertil skulle offeret tilgå en falsk hjemmeside og indtaste personfølsomme oplysninger. De indhentede oplysninger blev efterfølgende anvendt af gerningspersonen til at opnå en økonomisk gevinst (Ibid.:25).

Et centralt fund i studiet er, at ofrene i mange tilfælde selv indgår aktivt i svindelforløbet ved f.eks. at udlevere kort og pinkode. Ofrene fattede ikke mistanke til svindlen, hvilket bl.a. skyldes svindlernes professionalisme, ofrenes tillid til dem, eller manglende opmærksomhed på henvendelsens oprindelse (Ibid.:26). Det er muligt, at lignende mønstre og mekanismer også gør sig gældende i en dansk kontekst. Derfor vil vi være opmærksomme på lignende mønstre i analysen.

Svindlernes evne til at manipulerer deres ofre, synes at være et gennemgående tema i forskning om kontaktbedrageri og vishing. Flere forskere har i takt med det stigende antal vishing-angreb, undersøgt hvordan svindlere anvender overtalelsesteknikker, til at narre deres ofre til at handle imod deres egne interesser.
Eksempelvis har Gragg (2003) samt Stajano og Wilson (2011) hver især identificerede syv principper om psykologiske triggere, mens Cialdini (2007) fandt seks teknikker med væsentlig påvirkning på ofrene. I det seneste og mest anerkendte studie af Jones et al., 2021, undersøges det nærmere, hvordan de såkaldte 'social engineers' bruger overtalelsesprincipper og manipulation under svindelakter. Studiet tog afsæt i 86 konkrete svindelsager som blev kodet efter hvilke former for overtalelsesprincipper der blev anvendt til at snyde ofrene, samt hvilke elementer i svindelakten, der bidrog tilstedeværelsen af hvert overtalelsesprincip (Jones et al.,

2021). Det blev udledt, at der forekom i alt fem forskellige teknikker. Teknikkerne og deres betydning, illustreres i nedenstående oversigt:

Tabel 1 - Oversigt over SE-teknikker

Teknik	Beskrivelse	Typisk effekt på adfærd
1) Autoritet	Personers naturlige tilbøjelighed til at følge dem, de opfatter som eksperter eller autoritetsfigurer.	De adlyder uden at stille spørgsmål.
2) Forpligtelse, gengældelse og konsistens	Personer ønsker at fremstå troværdige, gengælder tjenester og handler i tråd med tidligere forpligtelser.	Øget sandsynlighed for at gennemføre en handling.
3) Afledning	Opmærksomheden fokuseres på én ting, såsom egne behov, gevinster, tab eller tidspres, mens vigtige signaler som måtte foregå omkring dem overses.	Lettere at narre eller manipulere under pres.
4) Sympati, "synes om" og bedrag	Personer stoler mere på dem, de kan lide, føler sig forbundet til, som minder om dem selv, eller virker bekendte/attraktive.	Mindre kritisk tænkning, højere tillid.
5) Socialt bekræftelse	Personer har en tendens til at følge flokken og ønsker at være en del af fællesskabet.	De lader sig påvirke af, hvad "alle andre" gør.

(Egen illustration, Jones et al., 2021)

I studiets resultater fremgik det, at 1) autoritet, 3) afledning og 5) social bekræftelse var de mest udbredte og hyppigst anvendte overtalelsesteknikker, da disse forekom ved størstedelen af alle svindelsagerne. Teknik 4) sympati, 'synes om' og bedrag blev også temmelig udbredt,

mens teknikkerne i 2) forpligtelse, gengældelse og konsistens var knap så anvendt. Udover det, fandt undersøgelse, at de forskellige teknikker ofte blev kombineret med hinanden og at de forekom i diverse konstellationer (Ibid.:8).

Teknikkerne og beskrivelserne heraf, vil være til inspiration for vores undersøgelse. Det skal forstås ved, at disse teknikker anvendes i vores tematiske kodning af dataene. Det skyldes, at vi ønsker at undersøge SE-teknikkernes eksistens, i en dansk kontekst.

På baggrund af afsluttede efterforskninger undersøger Lusthaus et al. (2023) gennem ti case-studier netværksstrukturer, kriminelt samarbejde og eksterne interaktioner i cyberkriminelle netværk. Fælles for casestudierne var, at der forekom økonomiske motiver hos svindlerne. En af de ti cases findes særligt relevant for denne undersøgelse, idet den omhandler en svindelmetode, der ligner den, vi undersøger. I casen udgav gerningspersoner sig for at være fagfolk med det formål at få virksomheder til at overføre penge til konti, de kontrollerede (Lusthaus et al., 2023:374). Selvom specialet fokuserer på BBB over for privatpersoner frem for virksomheder, er denne case relevant, idet begge svindeltyper bygger på samme grundlæggende mekanisme: at gerningspersonen påtager sig en autoritetsrolle for derved at manipulere ofret til at overføre penge. Lusthaus et al. identificerede to primære netværkskomponenter; 1) en phishingoperation med henblik på at skaffe adgang til mailkonti og adgangskoder, og 2) et netværk af muldyr, som modtog overførslerne fra ofrene og efterfølgende fordelte udbyttet blandt gerningspersonerne. Lusthaus et al. påviser, at cyberkriminelle netværk opererer med differentierede roller blandt gerningspersonerne. Da BBB indebærer lignende elementer, er det sandsynligt at der findes lignede rollefordelinger i de danske netværk. Derfor vil specialets analyse bl.a. fokusere på at kortlægge rollefordelingen i de danske netværk.

Eksisterende forskning i bedrageriformer med et teknologisk element og profit som drivkraft peger entydigt på, at de økonomiske konsekvenser af denne type kriminalitet er omfattende (Eguchi et al., 2024:150; Lusthaus et al., 2023:376; Choi et al., 2017:454). Lusthaus et al. (2023) har dokumenteret at ofrene for ovenstående cyberkriminalitet har lidt tab på over 500.000 britiske pund. Tilsvarende klarlægger Eguchi et al. (2024), at det samlede økonomiske tab forårsaget af "*special fraud*" i Japan i 2023 udgjorde omtrent 285 mio. amerikanske dollars. Også Choi et al. (2017) belyser det omfattende økonomiske tab ved svindel (vishing) og fremhæver, at der alene i perioden januar til oktober 2013 var et samlet tab estimeret til 42,6 mio. amerikanske dollars i Sydkorea. Samlet bekræfter disse fund, at bedrageri med et teknologisk

aspekt kan have omfattende økonomiske konsekvenser for ofrene. Dette understøtter vores viden, som ligeledes peger på betydelige økonomiske tab i forbindelse med BBB i en dansk kontekst (jf. afsnit 2.3).

Gennemgående for den ovenstående eksisterende forskning er, at svindlen har været velorganiseret og økonomisk indbringende. Svindlernes evne til at fremstå professionelle og som legitime aktører, spiller en afgørende rolle i at få ofrene til at handle imod deres egne interesser. Studierne viser, at svindlen har været systematisk opbygget, med forskellige roller og inddelt i flere trin, hvor den indledende kontakt sker telefonisk. Herefter fortæller gerningspersonerne overbevisende og troværdige historier, samt anvender autoritetsbaseret manipulation til at opnå ofrenes tillid. Dette muliggør at ofrene selv medvirker til svindlen ved at udlevere personfølsomme oplysninger eller værdier, og afslutningsvis lider et økonomisk tab. Da BBB også er en økonomisk indbringende svindelform, må det formodes at lignende fællestræk kan genfindes heri. Vi vil derfor have særligt fokus på gerningspersonernes teknikker, netværksstrukturen og offerets rolle i svindelforløbet.

4.2 Ofrenes profil og sårbarheder

I takt med den teknologiske udvikling og den tiltagende kompleksitet i moderne svindelmetoder, ses der i nyere tid et øget fokus på, hvad der kendetegner de mennesker, som ender som ofre for svindel. Særligt den ældre del af befolkningen står tydeligt frem som risikogruppe for bestemte typer af bedrageri. Det understøttes af danske data (jf. afsnit 2.1) samt internationale studier, der analyserer psykologiske sårbarheder og karakteristika ved offergruppen samt svindlernes bevidsthed herom.

Studier postulerer at tendensen med ældre som primære ofre for bedrageri, sker som følge af begrænsede teknologiske færdigheder samt en række psykosociale faktorer. Et japansk studie (Ueno et al., 2022) udarbejdede en tværsnitsundersøgelse blandt ældre borgere fra Japan og fandt, at ofrene for den såkaldte 'special fraud', scorede højere på en skala af adfærdsmæssige og psykologiske sårbarheder, som målte graden af henholdsvis social isolation, tillid og modstandsdygtighed overfor at blive manipuleret. Sidstnævnte ses ved, at ofrene typisk har en tendens til at stole på andre uden at udvise tilstrækkelig kritisk sans.

Dette underbygges af studiet fra Eguchi et al. (2024), som bekræfter, at ældre personer med begrænset social kontakt og interaktion, og som tilmed har et dårligt teknologisk kendskab,

dømmekraft og økonomisk sans, er i større risiko for at ende i svindlernes søgelys. Overraskende nok, scorede ofrene for svindel dog højere på livstilfredshed end 'ikke-ofre'. Det kan indikere, at ældre med en stor tillid til omverden og en mere positiv livsindstilling paradoksalt nok, kan være i større risiko for at blive udnyttet og ende som ofre (Eguchi et al., 2024). Den høje grad af livstilfredshed kan således muligvis medføre mindre mistro og lavere risikobevidsthed hos de ældre.

En fællesnævner ved den japanske forskning, er at køn opleves som et afgørende karakteristika, idet særligt ældre kvinder er overrepræsenterede blandt dem der udsættes for svindel (Eguchi et al.,2024: Ueno et al., 2022). En begrundelse for det, kan være, at kvinder typisk lever længere og hyppigere bor alene og derfor i højere grad kan være socialt isoleret, hvilket kan gøre dem lettere ofre for svindlerne (Eguchi et al., 2024).

Svindel rettet mod ældre anvender i høj grad psykologisk påvirkning og pres. Choi et al., (2017) illustrerer at de ældres sårbarheder udnyttes ved kontaktbedrageri. Det kommer til udtryk ved, at svindlerne, overfor de ældre, ofte udgiver sig for at være nogen de ikke er, typisk tillidsvækkende fagfolk fra banker eller myndigheder (Choi et al., 2017:463). Her kan de ældre udsættes for en akut problemstilling, hvor de føler sig nødsaget til at handle hurtigt og irrationelt. Dette stemmer overens med fundene fra Jones et al. (2021), der identificerer gerningspersonernes brug af klassiske overtalelsesteknikker heriblandt autoritet, medfølelse og tidspres. Netop de teknikker synes at have en særlig virkning på ældre, fordi de modsat andre persongrupper, har en stærk indlært respekt for autoriteter og en mindre tilbøjelighed til at kunne identificere digitalt bedrag (Jones et al., 2021:317).

Ifølge Loggen & Leukfeldt (2022) skal de ældres sårbarheder dog ikke kun ses som et individuelt anliggende, men også som et strukturelt problem, hvor de organiserede netværk målrettet udnytter ofrenes svagheder. I deres hollandske studie analyserede de 45 retssager imod kriminelle organiserede netværk. Resultaterne viste, at svindlerne besidder en stor bevidsthed om de ældres sårbarheder. Svindlerne udnyttede lækkede data til målrettet at identificere de ældre og udnytte dem gennem forskellige faser. De består henholdsvis af; at etablere en indledende kontakt, at opbygge tillid og til slut, af økonomisk udnyttelse (Loggen & Leukfeldt, 2022:208-211). Denne viden om potentielle ofre afspejles ligeledes i Lusthaus et al. (2024), der dokumenterer de cyberkriminelle netværks tydelige rollefordeling og målrettethed, hvor de ældre målgrupper bliver fremhævet som lavrisiko-ofre med potentiale for stor økonomisk profit.

I forlængelse heraf, viser andre studier dog, at alle ældre ikke nødvendigvis er lige sårbare. Det at udvise en selvbeskyttende adfærd, ved bl.a. at udvise skepsis mod personer der uopfordret forsøger at etablere kontakt, kan sammen med an afvejning af risici, reducere sandsynligheden for at blive et offer. Det fremgår desuden at viden om digitalt selvforsvar og oplysningskampagner kan være effektiv beskyttelse, endda hos den ældre befolkningsgruppe (Van't Hoff-de Goede et al., 2024:473).

Opsummerende er det gennem eksisterende forskning om offerprofilering for svindel, muligt at pege på, hvorfor netop de ældre mennesker udgør en særlig udsat gruppe. Denne risiko opstår som følge af både strukturelle og individuelle faktorer. En begrænset teknologisk erfaring, kombineret med sociale forhold som isolation og høj grad af tillid til omverden, gør de ældre til ideelle mål for at blive offer for de organiserede netværks teknikker.

5. Metode

I de følgende afsnit præsenteres specialets metodevalg samt de bagvedliggende metodiske overvejelser. Afsnittet indledes med en introduktion til den analytiske *crime script*-tilgang. Herefter følger en præsentation af den anvendte metodiske tilgang, *mixed methods*. Dernæst redegøres der for specialets empiriske grundlag, herunder de metodiske til- og fravalg i forbindelse med udvælgelsen af data. Datagrundlaget består af et eksplorativt forstudie, retsdokumenter af afsagte domme over dømte bankbudsbedragere samt kvalitative interviews med eksperter indenfor politiet og banker. I den forbindelse beskrives processen for indsamling af retspraksis samt rekruttering af informanter. Dernæst følger en præsentation af vores interviewguides, efterfulgt af en redegørelse for databehandlingen, som inkluderer transskription og kodning. Undervejs i det metodiske afsnit inddrages relevante kvalitetskriterier. Afslutningsvist diskuteres forskningsetiske overvejelser i forhold til brugen af hacket data.

5.1 Forskningsdesign – Casestudie

Vi har valgt at anvende et *eksplorativt, multipelt casestudie* som forskningsdesign i specialet. Casestudiet defineres som et forskningsdesign, der studerer fænomener i den kontekst, hvori de optræder (Antoft & Salomonsen, 2012:135). Formålet er at udarbejde en detaljeret analyse af den bestemte case, her BBB, hvortil kompleksiteten og den særlige karakter af casen klarlægges og analyseres (Bryman, 2021:60; Flyvbjerg 2010:464). Ved at anvende dette forskningsdesign, bliver det muligt at undersøge et større fænomen i en mindre kontekst. Det betyder, at netværkene fra vores retsdokumenter udgør repræsentative separate cases, der fremtræder som cases på det overordnede fænomen. Således studerer vi netværk af bankbude, for at forstå BBB som fænomen.

Dette casestudie er udført ud fra en induktiv tilgang, hvilket indebærer, at vi tager udgangspunkt i nyt empirisk materiale og søger at identificere mønstre heri. Får at generere ny viden, tilgår vi undersøgelsen med en åben og eksplorativ tilgang, hvor vi ikke på forhånd er styret af eksisterende teorier eller forståelser. Dette adskiller sig fra den deduktive tilgang, hvor undersøgelser bygger på et eksisterende teoretisk grundlag, som forskere har til hensigt at teste eller bekræfte i praksis (Bryman, 2021:19-21; Riis, 2005:29). Det er dog væsentligt at understrege,

at hverken fuld induktion eller fuld deduktion lader sig realisere i praksis, da begge repræsenterer idealistiske yderpunkter (Bryman, 2021:21-23). Vi bevæger os i stedet på et kontinuum mellem disse tilgange, men vores udgangspunkt er overvejende induktivt, idet vi søger at generere ny viden gennem datadrevet analyse og efterfølgende teoretisering (Riis, 2005:29).

En generel udfordring ved anvendelsen af casestudier er de begrænsede muligheder for generalisering (Flyvbjerg, 2025:640). Da vores data kun giver indblik i et udsnit af de netværk, der beskæftiger sig med BBB, kan resultaterne af vores analyse ikke umiddelbart overføres til hele populationen inden for denne kriminalitetsform. Den viden, vi opnår gennem de analyserede cases, er således specifik for de aktører, vi har haft adgang til. Ved at benytte et multipelt casestudie øges dog potentialet for generalisering (Bryman, 2016:63-64), da vi kan sammenligne netværkene på tværs og se hvilke mønstre der går igen, hvilket styrker vores udgangspunkt for at besvare problemformuleringen. Ydermere søger vi at højne generaliserbarheden af vores resultater ved at kombinere de empiriske fund fra retsdokumenterne med ekspertviden fra fagpersoner samt med relevant eksisterende forskning. Ved at integrere disse datakilder forbedres grundlaget for analytisk generalisering, hvor casens resultater relateres til eksisterende viden og teorier frem for til en bred population (Yin, 2014:20-21). Vi har casens begrænsninger for øje i analysen og konklusionen, hvor vi forholder os kritisk til rækkevidden af de indsigter, som casen generer.

5.2 Crime-script som analytisk redskab

I vores undersøgelse anvendes *crime script* metoden som et analytisk redskab til at praktisk at illustrerer og forstå hændelsesforløbene i BBB som en sekventiel og målrettet proces. Vores crime script vil ikke være rammesættende for hele analysen, men snarere anvendes som et værktøj. Tilgangen udgør således en bagvedliggende ramme for undersøgelsen, idet de forskellige faser af det kriminelle forløb udfoldes løbende. Dette visualiseres afslutningsvist i analysen ved et crime script.

Crime scripts stammer oprindeligt fra Cornish's (1994) antagelse om, at forbrydelser bør betragtes som en række særskilte begivenhedssekvenser, der på forskellig vis, bidrager til, at en forbrydelse eller et forsøg på en forbrydelse finder sted. Sekvenserne strækker sig over tid, og muliggør forekomsten af senere begivenheder (Cornish, 1994:158). Ifølge Cornish indebærer

crime scripts, elementerne *before*, *during* and *after* (før, under og efter). Som hver især beskriver de konkrete handlinger, gerningspersonen foretager fra forberedelsen, under selve udførslen, og i efterspillet. Andre forskere som Leclerc & Wortley har senere hen videreudviklet tilgangen og lavet modeller med både otte og ti trin forbrydelsestrin (Leclerc, 2017:123-124). Bedst egnet til netop vores undersøgelse findes, Cornish's tre-trins model eftersom vi med enkeltheden undgår kunstig fremstilling ved at tvinge hændelsesforløbet ned i en række bestemte 'kasser'. I stedet giver de tre mere overordnede faser os større fleksibilitet og mere flydende overgange mellem trinnene.

Med fokus på hvordan begivenheder udfolder sig, giver et crime script os mulighed for at generere og systematisere viden om de proceduremæssige aspekter i BBB, samt hvilke forudsætninger der indgår i at denne kriminalitet kan udføres (Cornish, 1994:160). Således sigter vi efter at skabe en mere specifik beskrivelse af hvordan BBB begås og de adfærdsmæssige rutiner de måtte indebære.

Ud fra vores forståelse, ser vi, at hver fase indebærer opnåelsen af et delmål, hvilket tjener at fremme forbrydelsens overordnede mål. Med det afsæt, ser vi, at det gennem et crime script bliver muligt at afdække BBB fra start til slut, hvilket er i overensstemmelse med vores problemformulering.

5.3 Mixed methods

Specialet anvender *mixed methods* som metodisk tilgang, hvor to metodiske modpoler forsøges at forenes. Mixed methods-forskning indebærer, at man ikke begrænser sig til én metodisk tradition, f.eks. en udelukkende kvalitativ eller kvantitativ tilgang, men i stedet kombinerer de metodiske retninger inden for samme undersøgelse (Bryman, 2021:556). Formålet med denne tilgang er at overskride de metodiske begrænsninger, der kan være forbundet med anvendelsen af én enkelt metode, for således at lade disse komplimentere hinanden (Creswell & Creswell, 2023:227; Bryman, 2021:556). Det kvantitative element anses for at være fordelagtigt, idet det muliggør en kvantificering af adfærds- og bevægelsesmønstrene blandt gerningspersonerne igennem numeriske data. Dette betyder, at den kvantitative tilgang muliggør identificeringen af mønstre og tendenser igennem store mængder tekstinformation, her retsdokumenter. Dette giver et dybdegående indblik i antallet af forekomster af de eksplicitte fremgangsmåder. Det kvalitative element anses som fordelagtigt, og giver indsigt i de underliggende mekanismer,

der bidrager til forklaringen af bankbudsbedrageriets forløb. Endvidere kan den kvalitative tilgang bidrage med viden, som ikke altid fanges gennem kvantitative målinger, hvorfor kombinationen fører til en optimal forståelse af fænomenet.

Det skal understreges, at sammensætningen af forskellige metoder ikke bør ske "hæmningsløst", eller med den forventning, at et bredere og mere varieret datagrundlag automatisk forbedrer undersøgelsen (Bryman, 2021:571). Metodernes kombination skal tilføre undersøgelsen reel værdi, hvilket vi vurderer, gør sig gældende i specialet, idet et enkelt metodisk greb ville medføre et mere begrænset datagrundlag, som ikke vil kunne besvare specialets problemformulering i tilstrækkelig grad.

Gennem validering sigter vi efter at tilføre værdi til vores resultater fra de to dataindsamlingsstrategrier, gennem *triangulering*. Triangulering referer til den praksis, hvor forskellige resultater sammenholdes og krydstjekkes med henblik på at opnå en mere valid forståelse af fænomenet (Ibid.:556-557). Konkret betyder det, at udsagnene fra de afholdte ekspertinterviews sammenholdes med den viden, der fremgår af retsdokumenterne.

Afhandlingen anvender en *konvergerende tilgang*, hvilket betyder at den kvalitative og kvantitative data indsamles simultant (Ibid.:567-568). Dette betyder, at de to datatyper ikke påvirker hinanden under udformningen af undersøgelsen. I den proces er trianguleringen med til at skabe *integreret analyse* (Ibid.:568). I nærværende undersøgelse vægter den kvantitative del tungest, eftersom den konkret kan fortælle om gerningspersonernes adfærd og bevægelsesmønstre igennem numerisk data. De kvalitative ekspertinterviews fungerer som supplerende empiri, som kan bekræfte nogle af de tendenser, der viste sig i den kvantitative del.

5.4 Forstudie

Da BBB er et nyere kriminalitetsmodus, er det ikke fundet belyst fra en dansk akademisk vinkel tidligere. Vi har som tidligere nævnt, ikke kunne fremsøge eksisterende forskning konkret herpå. Vi gennemførte derfor et forstudie for at opnå indsigt i fænomenet, inden vi foretog vores dataindsamling. Dette har været behjælpeligt med at pege os i en retning af, hvad der var interessant at undersøge, samt hvilke problematikker, begreber og forståelser der findes indenfor BBB. Vi har haft kontakt til fire forskellige aktører, der hver især har bidraget med grundlæggende viden om BBB.

Der blev etableret kontakt til en OSINT-specialist[1] og en efterretningsvirksomhed inden for cybersecurity igennem vores netværk. OSINT-specialisten har forfattet en artikelserie omhandlende spoofing-svindel, hvor BBB optræder (Tjek det, 2025). Artikelserien byggede på 100.000 datafiler fra et svindelnetværks computere og telefoner. Filerne viser bl.a. telefonsamtaler med mere end 9.000 danskere, hvor man kan høre "*... hvordan svindlerne manipulerer og snyder danskere til at give sig adgang til deres bankkonti, som derefter tømmes*" (Ibid.). Artikelserien har bl.a. afsløret svindlernes interne kommunikation og processer, hvilket dannede grobund for en række interessante undersøgelsesområder. Specialisten har efterfølgende givet et mere uddybende og aktuelt indblik i hvordan der blev arbejdet med den data, der ligger til grund for artiklerne. I denne dialog, fik vi stor viden om hvordan svindlen foregår samt nogle af rationalerne bag svindlernes handlinger. Endvidere blev det beskrevet hvordan et bedragerinetværk forventes at være organiseret, særligt i forhold til de medvirkende aktører og de dertilhørende roller og magtforhold.

Efter lidt nærmere research blev det gjort klart, at det data som artikelserien byggede på, stammede fra den efterretningsvirksomhed, som vi ligeledes tidligere var blevet sendt i retning af, af en person i vores netværk. Virksomheden introducerede os til deres omfattende arbejde og tilbød os fuld adgang til deres hackede data. Efter længere tids overvejelser og stor ærgerlighed, besluttede vi at takke nej til dette samarbejde (jf. afsnit 5.10).

Som yderligere supplement til vores viden, har vi gennem en længere periode haft en løbende korrespondance med Politiets Efterretnings- og Analyseenhed (herefter EAE), i Midt- og Vestjyllands Politikreds. Vi fik gennem vores kontakt, som er specialkonsulent og operativ analytiker, indsigt i politikredsens data, herunder anmeldelsesbilledet, køns- og aldersfordeling på ofre samt mønstre i konkrete dage og tidspunkter af døgnet, hvor bedragerierne foregår (jf. Bilag 1-4)[2]. Denne viden har medført, at vi har fundet inspiration til bestemte elementer, der kunne undersøges.

I fjerde del af forstudiet fik vi kontakt til en journalist fra TV2, som havde udarbejdet en undersøgelse af BBB, her særligt med et fokus på netværkenes færden, mobilitet og kontanthævninger. Kendskabet til journalistens arbejde blev vi gjort bekendt med hjælp af specialets vejleder, Rasmus Munksgaard. Journalistens viden bestod af analyse af aktindsigter i afsagte

[1] Open-source Intelligence specialist er en person, som indhenter data fra allerede tilgængelige kilder på internettet (PET, 2025)
[2] Tallene er ikke udarbejdet med henblik på forskning, og der kan forekomme fejlkilder.

domme. Journalisten delte et mindre antal sagsnumre med os, for at hjælpe os på vej med selv at opnå adgang til lignende retsbøger.

Opsummerende har forstudiet spillet en central rolle for afhandlingens endelige produkt. Den indledende research og afdækning af viden, har gjort det muligt at indkredse problemstillingen indenfor et område med begrænset forskning. Vores research har åbnet vores nysgerrighed for, hvilke elementer i BBB der kunne være interessante at undersøge. Det har bl.a. været emner som rekrutteringsproces, organisering af kriminelle netværk, mobilitet, og viktimologi. Vi fandt det relevant at inddrage forskellige aktører som hver især havde en faglig vinkel på fænomenet, med henblik på, at få adgang til nuancer, som vi ikke nødvendigvis ellers ville have været opmærksomme på. Forstudiet har resulteret i, at vi har opnået et solidt vidensgrundlag om BBB, hvilket har været af væsentlig betydning for vores videre studie. Selvom at denne viden ikke direkte afbilledes i vores endelige udformning, har det dannet et afgørende fundament, som i høj grad har præget vores tilgang og forståelse.

5.5 Dokumentanalyse af retsdokumenter – som primære data

Dokumenter anvendes som den primære empiri i undersøgelsen, hvor de danner grundlag for analyse, diskussion og konklusion. Det betyder, at dokumenter udgør undersøgelsens genstand (Ingemann et al., 2019:69). Dokumenter ses i mange afskygninger (Prior, 2003:4), hvorved nærværende afhandling tager afsæt i retsdokumenter. Disse retsdokumenter er fikseret i tid, hvilket betyder, at der arbejdes med statisk skriftligt materiale der ikke kan forandres mens det analyseres (Ingemann et al., 2019:69; Lynggaard, 2020:165). Dokumenter anvendes på vanlig vis enten til vidensgenerering eller vidensafsøgning. Relevant for specialets formål, er vidensgenerering snarere end vidensafsøgning. Det gøres med udgangspunkt i, at skabe ny viden, ved at analysere allerede bearbejdet information (Ingemann et al., 2019:69-70).

Ved at anvende dokumentanalyse af retsdokumenter til at undersøge BBB, bliver der skabt grobund for at identificere handlemønstre og tendenser, i hvordan denne type af forbrydelser bliver henholdsvis begået, opklaret og sanktioneret. Her vil vores hovedfokus rettes mod gerningspersonens færden, særligt i forhold til metoder, mobilitet og målgrupper af ofre. Dette gøres med henblik på at præcisere modus og arbejdsgangen fra start til slut, i overensstemmelse med afhandlingens problemformulering.

Et opmærksomhedspunkt ved anvendelsen af retsdokumenter som empirisk grundlag er, at disse dokumenter ikke er udarbejdet med et forskningsformål for øje, men derimod med henblik på domsfældelse. Det indebærer, at oplysninger, som kunne have været relevante i en forskningssammenhæng, ikke nødvendigvis fremgår af aktindsigterne (Leukfeldt & Loeggen, 2022:219). Informationsniveauet varierer således fra sag til sag, hvortil nogle retsdokumenter indeholder detaljerede oplysninger såsom navn, alder og adresse, mens andre alene rummer begrænsede informationer om særligt ofrene. Denne variation kan have betydning for undersøgelsens resultater, idet den påvirker, hvilke karakteristika ved personerne der indgår i sagerne vi faktisk kan analysere og udtale os om. Vi forholder os derfor i analysen til omfanget og karakteren af de tilgængelige data og er opmærksomme på, hvorledes vi reelt kan drage konklusioner ud fra det samlede materiale.

I overvejelsen af kvaliteten og styrken ved dokumenter, fremkommer det, at de løbende bør vurderes i forhold til deres *autenticitet, troværdighed, repræsentativitet* og *mening* (Lynggaard, 2020:176). *Autenticiteten* refererer til dokuments oprindelse, og dermed hvorvidt det er tydeligt hvor det er forfattet og hvem der er afsender. Således elimineres risikoen for både forfalskninger samt ukonkrete eller skjulte afsendere (Ibid.). Da alt indsamlet retspraksis er indhentet og kommunikeret direkte igennem de danske domstole, findes en stærk autenticitet. Dette betyder, at materialet er objektivt og verificerbart.

Dokumenternes *troværdighed* illustrerer hvorledes valget af dokumenter kan være forbundet med bias og skævheder som kan påvirke analysens konklusioner og resultater i en bestemt retning (Ibid.). Kriteriet om troværdighed kan endvidere være vanskeligt at indfri, da fænomenet er nyt og aktuelt, hvorfor datamaterialet blot indfanger en kort årrække. Såfremt troværdigheden skulle højnes yderligere, kunne fænomenet undersøges over en længere tidsperiode. Dog er det hverken muligt eller formålet med afhandlingen.

Med *repræsentativitet* opstår spørgsmålet om, i hvilket omfang den anvendte retspraksis præsenterer det typiske fænomen for BBB, eller om de i stedet er præget af en uregelmæssighed (Ibid.:176-177). Afhandlingen kan ikke garantere fuldkommen repræsentativitet, da datamaterialet 'blot' består af syv sagskomplekser (netværk). Datamaterialet er baseret på dømte forbrydere, og udgør derfor ikke det samlede billede af det BBB der begås i Danmark. Havde vi haft mulighed for, at få indsigt i ikke-dømte forbrydere, kan resultaterne potentielt have set anderledes ud (Leukfeldt & Loeggen, 2022:219). Vi har forsøgt at styrke repræsentativiteten

ved at indhente sager fra hele landet, på tværs af regioner, for at imødekomme eventuelt geografiske forskelligheder.

Et sidste begreb om kvalitetsvurdering er *mening*. Mening skal stille spørgsmålstegn til hvorvidt meningen og forståelsen af et dokument fremstår klar og tydeligt. Det vil sige, om dokumentet er præget af uklart sprog, f.eks. af ældre dato, tekniske termer eller vendinger der giver anledning til forvirring hos forskeren (Lynggaard, 2020:177). Det vurderes, at vi som undersøgere er fortrolige med retsdokumenternes retorik, hvorfor der ved gennemgang af dokumenterne ikke umiddelbart forekommer os uklarheder i forhold til det databehandlingen har til hensigt at udlede.

5.5.1 Indsamling af retspraksis

For at belyse BBB indhentes autentisk og valideret information om svindlernes adfærd og handlemønstre via retsdokumenter.

Første fase i dataindsamlingen af retsdokumenter bestod i en eksplorativ søgning efter, i hvor stort et omfang der var sagsakter og retsdokumenter offentligt tilgængeligt. Her fik vi adgang til et sagskompleks, der fungerede som eksempel på viden der var ønskværdig i søgen efter øvrige retsdokumenter (Bilag 22).

Næste fase var at udarbejde skriftlige anmodninger om aktindsigt med fokus på reglerne i retsplejeloven. Ifølge Domstolsdatabasen (2025) kræves sagsnumre for aktindsigt i civile og straffesager. Via en journalist fik vi fire sagsnumre, men denne var ikke tilstrækkelig fyldestgørende. Derfor indsamlede vi yderligere information om bankbudssager fra medierne, da retten i visse tilfælde imødekommer aktindsigt uden sagsnummer, hvis sagen er tilstrækkeligt belyst. Oplysninger som domsdato, køn, alder, lokation, svindelbeløb og antal ofre blev samlet og systematiseret i tabeller fordelt på relevante domstole (Bilag 8), hvorefter anmodninger om aktindsigt blev sendt i de udvalgte sager.

Der var muligt at identificere 21 sager fordelt på syv domstole i Danmark. Som resultat heraf er der opnået indsigt i syv sagskomplekser, herunder tilhørende retsdokumenter (Bilag 16-22). Den samlede oversigt over retsdokumenterne fremgår af nedenstående tabel.

Tabel 2 - Oversigt over domsafgørelser

Domstol	Længde på dom	Antal direkte ofre (erstatningskrav)	Antal indirekte ofre (mislykket forsøg på svindel) *
Københavns byret	2 år	9 stk.	0 stk.
Retten i Odense	1 år	14 stk.	10 stk.
Retten i Herning	Person A: 1 år og 9 måneder Person B: 6 måneder	12 stk.	6 stk.
Retten i Næstved	Person A: 2 år Person B: 1 år og 3 måneder	29 stk.	1 stk.
Retten i Viborg	Person A: 3 år Person B: 1 år og 3 mdr.	49 stk.	0 stk.
Retten i Aarhus	1 år og 3 måneder	16 stk.	5 stk.
Retten i Svendborg	2 år og 9 måneder	38 stk.	172 stk.

5.6 De kvalitative ekspertinterviews – som sekundære data

Specialets datagrundlag består delvist af kvalitative ekspertinterviews som supplement til retsdokumenterne. Kombinationen af disse dataindsamlingsmetoder skaber både indsigt i processerne bag BBB såvel som følgerne og resultaterne heraf. Interviewene vægtes som sekundære data, der både skal fungere som supplering og validering, samt ud fra formålet om at etablere et praksisnært og dybdegående vidensgrundlag. Inddragelsen af ekspertinterviews er funderet ud fra ønsket om at få adgang til specialiseret viden gennem fagfolk fra organisationer, der på daglig basis er i interaktion med fænomenet (Ingemann et al. 2019:156). Fælles for eksperterne er, at de besidder en unik og praksisnær forståelse for hvilke udfordringer der er på spil, og ligeledes hvor der ses udviklingspotentiale i forhold til forebyggelse af BBB. De besidder alle, qua deres faglige position, en særlig ekspertise der vurderes relevant i forsøget på at kortlægge, hvordan processen for et bankbudsbedrageri udspiller sig. Denne erfaring danner således

grundlaget for relevant baggrundsviden til brug for besvarelse af afhandlingens problemformulering.

5.6.1 Rekruttering og udvælgelse af organisationer

På baggrund af forudgående research blev det tydeligt, at danske banker og pengeinstitutter spiller en central rolle i både bekæmpelsen og håndteringen af BBB. Bankerne fungerer som et etableret sikkerhedsnet, der skal varetage forurettedes interesse når vedkommende f.eks. bliver udsat for bankbudsbedrageri. Bankerne er selv ansvarlige for dække de økonomiske tab der er forbundet hermed, hvorfor de har interesse i at modvirke, advare og etablere sikkerhedsforanstaltninger der forhindrer denne type svindel (jf. Betalingslovens § 100). Bankernes rolle synes dermed væsentlig i forståelsen af udviklingen, hvilke mekanismer der er på spil i sagerne, og hvordan der tilsvarende kan udvikles initiativer som modsvar til svindlerne.

Vi startede med at identificere 14 store banker i Danmark (baseret på arbejdende kapital) (Finanstilsynet, 2022). Disse blev gennemgået for at finde ud af, hvilke der aktivt advarer mod BBB via deres hjemmeside. På den baggrund blev listen reduceret til syv banker (jf. Bilag 5), hvor tre udviste interesse og deltog i interview. Denne udvælgelse bunder i en formodning om, at de banker der aktivt, advarer mod en bestemt type svindel må have oplevet det, og derfor have etableret en fast sagsproces eller et team der varetager håndteringen heraf. Der blev efterfølgende rettet skriftlig henvendelse til de syv banker, hvoraf tre banker udviste interesse i emnet, hvorfor de indviede i at deltage i et interview.

Foruden de tre banker, indgår også politiet som ekspert i undersøgelsen. Denne rekrutteringsproces var simpel, idet denne kontakt allerede var etableret som en del at vores faglige netværk. Det skyldes, at vi begge har gennemført et praktikforløb ved Midt- og Vestjyllands Politi som led i vores kandidatuddannelse. Heraf opstår også kontakten til kredsens EAE-afdeling. Denne kontakt er særlig brugbar, idet netop Midt- og Vestjyllands EAE-afdeling helt isoleret set fokuserer på at monitere netop BBB, og har gjort det siden september 2022 (Bilag 10). Der blev på den baggrund rettet henvendelse til vores kontakt, som indviede i at deltage, hvorefter det blev etableret et interview.

Præsentationen af de medvirkende informanter, fremgår af bilag 26.

5.7 Semistruktureret interview og interviewguide

Den semistrukturerede interviewform anvendes som en af to metoder til dataindsamling, for at opnå indsigt i BBB ud fra eksperters perspektiv. Interviewformen befinder sig på et spektrum mellem det ustrukturerede og det strukturerede interview (Ingemann et al. 2019:158). Dette betyder, at samtalen, med de prædefinerede spørgsmål, målrettes de konkrete temaer, mens der samtidig er mulighed for afvigelser fra interviewguiden, hvis nye, relevante emner opstår. Interviewformen formår altså at holde styr på retningen af interviewet, uden at styre det fuldstændigt (Ingemann et al., 2019:158).

Med udgangspunkt i forstudiet, blev der udarbejdet to separate interviewguides. De fungerede som en rettesnor undervejs i interviewprocessen, hvilket skabte en flydende samtale, samtidig med at de mest centrale fokusområder blev indfanget (Ingemann et al., 2019:173). Spørgsmålene i interviewguiden blev udformet i overensstemmelse med problemformuleringen, hvilket bidrager til at specialets gyldighed øges, hvilket sikrer, at de tiltænkte undersøgelsesområder faktisk også er dem, der undersøges (Brinkmann & Tanggaard 2015:40). Et eksempel herpå findes i interviewguiden til politiet: "*Hvordan foregår BBB, ifølge din ekspertviden, trin for trin?"* (Bilag 6:2). Formålet var her, at informanten på egen hånd skulle forklare hvordan de erfarer de forskellige trin, der forekommer ved BBB.

Interviewguiden til bankerne er inddelt i fire kategorier (Bilag 7). Kategorierne er udarbejdet med henblik på at belyse bankens forståelse og kendskab til BBB, dens rolle i beskyttelsen af ofrenes penge, de udfordringer banken står over for i bekæmpelsen af denne svindelform samt bankens ansvar i forebyggelsen heraf. Med afsæt i vores crime script-tankegang, bidrog bankerne med indsigt i henholdsvis *undervejs* og *efter.* Eksperterne kan ikke give en direkte indsigt i svindlernes specifikke handlinger og rationaler, men de kan belyse visse aspekter af svindlen, da deres kontakt med ofre giver dem en forståelse af svindlernes modus. Et eksempel hvor interviewguiden forsøger at indfange dette lyder således: "*Er der særlige mønstre eller mistænksom adfærd, der typisk afslører BBB?*" (Bilag 7:2). Det bliver igennem spørgsmål som dette muligt at udlede svindlernes handlemønstre, set fra bankens perspektiv og tilsvarende hvilke faresignaler der fremtræder for banker.

Interviewguiden til politiet er inddelt i fem kategorier (Bilag 6). Kategorierne er udformet for at skabe indsigt i politiets opfattelse af BBB herunder; svindlernes modus, netværk og orkestrering af bedrageriet, indtjening og profitfordeling, det tværfaglige samarbejde mellem rele-

vante aktører samt bedrageriformens levetid og mulighederne for forebyggelse. Derudover ønskedes det at belyse de beslutningsprocesser, som gerningspersonerne foretager *før*, *under* og *efter* de kriminelle handlinger.

Selvom eksperten ikke kunne besvare dette direkte, blev der indsamlet værdifuld viden gennem spørgsmål som f.eks. "*Hvordan rekrutteres man til at være en del af et BBB-netværk?*" (Bilag 6:3). Spørgsmål som dette skabte en dybere forståelse af hele processen bag BBB – fra start til slut. Politiet er i besiddelse af en mere konkret og detaljeret viden om svindlen end bankerne, da de er ansvarlige for efterforskningen af den. Denne specifikke viden blev forsøgt indfanget gennem spørgsmål som: "*Hvordan kommunikerer svindlerne?*" (Bilag 6:3). Herved blev der skabt grobund for at indhente mere praksisnær viden om, hvordan svindlerne opnår succes med BBB.

Ved at præsentere en detaljeret beskrivelse af processen for udarbejdelsen af interviewguiden, gives der indsigt i, hvordan den konkrete viden om fænomenet blev indfanget. Endelig, er de to udarbejdede interviewguides vedlagt som bilag (Bilag 6-7). Denne åbenhed om udformningen af interviewguiden øger specialets transparens, da det konkret afspejler, hvordan specialet har struktureret dens tilgang. I forlængelse heraf, bliver det muligt for andre forskere at forstå den udvalgte fremgangsmåde og reproducere undersøgelsen, hvilket styrker undersøgelsens replicerbarhed (Bryman 2021:38-39) Dette øger chancen for, at resultaterne i undersøgelsen kan bruges som vejledning i fremtidige studier.

5.8 Databehandling

5.8.1 Interviewsituationen

Følgende afsnit har til hensigt at beskrive interviewsituationen. To interviews fandt sted ved fysisk fremmøde, mens de resterende to blev afholdt online (se tabel 3). Vi var begge til stede under samtlige interviews, hvor vi fordelte interviewrollerne imellem os. Skiftevis havde den ene rollen som primær interviewer, og havde ansvaret for at lede samtalen, mens den anden fungerede som sekundær interviewer med fokus på at sikre, at interviewguiden blev overholdt, og at potentielle opfølgende spørgsmål ikke blev overset. Vi valgte, at begge skulle deltage i alle interviews, idet dette vurderedes at give de bedste forudsætninger for at bevare overblik i

interviewsituationen samt for at sikre en mere nuanceret og fyldestgørende indsamling af empiri.

Tabel 3 - Interviewoversigt

Organisation	Placering	Interviewlængde
SparNord	Fysisk	1:10:04
Arbejdernes Landsbank	Online	53:03
Sydbank	Online	53:34
Efterretnings- og Analyseenheden, Midt- og Vestjyllands Politi	Fysisk	1:46:46

Vi er bevidste om, at computerstøttede (online) interviews i nogen grad begrænser muligheden for at vi kan opfange nonverbal kommunikation, såsom kropssprog og mimik (Kvale & Brinkmann, 2015:204-205). Set i lyset af interviewenes formål og karakter har vi dog vurderet, at denne begrænsning ikke har haft væsentlig betydning for undersøgelsen.

Selvom vi erfarede at interviewene forløb problemfrit, oplevede vi, at særligt i interviewene med bankrepræsentanterne, at vi var udfordret af at holde fokus på udelukkende BBB, idet deres daglige arbejde omfatter arbejdet med en bred vifte af svindelformer. Dette betød, at samtalen indimellem bevægede sig hen imod andre former for kontaktbedrageri som f.eks. 'Bekendt i knibe'[3]. Vi tilstræbte løbende at minimere dette ved at pointere specialets hovedfokus, og vi vurderer derfor, at det ikke har haft indvirkning på interviewenes kvalitet.

5.8.2 Transskriptionsprocessen

Fælles for de gennemførte interviews er, at de blev optaget på lydfil med henblik på efterfølgende transskription. Efter endt transskribering er optagelserne blevet slettet. Transskription betegner den proces, hvor mundtlige samtaler omsættes til skrift, hvilket udgør er nødvendigt for den videre analyse i specialet (Kvale & Brinkmann, 2015:235, 243). Transskriptionerne er

[3] Et modus, hvor gerningspersoner indleder kontakt via sms med beskeden "Hej mor/far" og udgiver sig for at være offerets barn. Under påskud af eksempelvis at have mistet adgang til MitID, fået stjålet telefonen eller fået kortet spærret, forsøger de herefter at manipulere offeret til at overføre penge (NCIK, 2025:8).

vedlagt som bilag for at sikre transparens i undersøgelsesprocessen (Bilag 10-13). Når relevante bilag vedlægges, øger det muligheden for at andre forskere kan replikere undersøgelser som denne (Bryman, 2021:41).

Eftersom vi er to personer, der har foretaget transskriptionerne, udarbejdede vi fælles retningslinjer for processen (jf. Bilag 9). Endvidere er usammenhængende ytringer poleret og omskrevet til mere læsbart skriftsprog, når det vurderedes nødvendigt for forståelsen. I tilfælde, hvor informanternes udtalelser ikke kunne tydes, er "XXX" anvendt. Vi er bevidste om, at denne tilgang indebærer en risiko for, at dele af informanternes oprindelige udtryk er gået tabt. Vi er bevidste om, at denne tilgang kan medføre tab af nuancer, men vurderede, at en poleret transskription var nødvendig for at sikre læsbarhed og et solidt analytisk grundlag.

5.8.3 Kodning

Dette afsnit indeholder en præsentation af, hvordan vi har foretaget kodningen af henholdsvis vores retsdokumenter og ekspertinterviews.

Kodning af retsdokumenter

Da vi havde fået adgang alle til retsdokumenterne, anlagde vi en eksplorativ strategi, hvor vi indledningsvist læste alle domme igennem. Dette gjorde vi i overensstemmelse med vores induktive tilgang, for at identificere mønstre og karakteristika ved både ofre og gerningspersoner.

Efter en grundig gennemlæsning fandt vi frem til 24 variable, som hver især kunne give indsigt i BBB (Bilag 15). De relevante variable blev noteret ned, og senere anvendt i databehandlingen (Bilag 14a-d). I udvælgelsen af relevante variable havde vi den eksisterende forskning for øje, uden at lade den være styrende. Vi var bl.a. interesseret i hvorvidt, der var viden om det økonomiske aspekt, viktimologiske mønstre, anvendelsen af SE-teknikker, den konkrete aktivitet og svindelmetode samt gerningspersonernes samarbejde.

Ud fra retsdokumenterne er der udført fire separate kodninger med henblik på at belyse forskellige dimensioner af bankbudsbedragerierne. Kodningerne var således, at 1) fokuserer på de direkte ofre og er baseret på 24 udvalgte variable, som giver et overblik over viktimologiske forhold, geografisk fordeling, fremgangsmåder samt hvilke værdier ofrene har udleveret (Bilag 14a). 2) beskæftiger sig med hævnings- og aktivitetsmønstre i relation til det enkelte offer, og

kortlægger gerningspersonernes konkrete handlingsmønstre trin for trin (Bilag 14b). 3) omhandler gerningspersonerne, deres netværk og oplysninger såsom køn, alder, svindlens varighed, samlet økonomisk udbytte, succesrate samt eventuel tidligere kriminalitet (Bilag 14c). Denne kodning skaber indsigt i, hvilke typer personer der begår denne form for kriminalitet. 4) følger samme struktur som 1), men tager udgangspunkt i de indirekte ofre, hvilket er ofre, hvor svindelforsøget er mislykket og de derfor ikke har lidt et økonomisk tab (Bilag 14d). Formålet med at inddrage de indirekte ofre har været at opnå indsigt i, hvilke personer gerningspersonerne forsøger at ramme, med henblik på at identificere eventuelle mønstre i udvælgelsen af ofre.

Som nævnt varierer mængden af information tilgængelig i retsdokumenter (jf. afsnit 5.5). Under kodningsprocessen viste det sig at oplysninger om hjemmehjælp, anvendte kommunikationsapps, varigheden af samtaler mellem offer og gerningsperson samt gerningspersonernes påklædning kun i begrænset omfang fremgik af materialet.

Disse variationer i datagrundlaget udfordrer generaliserbarheden, da ikke alle variable er systematisk tilgængelige på tværs af sagerne. Det vil sige, at de identificerede mønstre og tendenser kan give vigtig indsigt i fænomenets karakter og dynamikker, selvom de ikke nødvendigvis kan overføres direkte til hele populationen af BBB.

Kodning af ekspertinterview

I kodningen af vores afholdte ekspertinterviews har vi ligeledes anvendt en åben og induktiv kodningsstrategi. Efter endt transskribering har vi som første trin i kodningsprocessen foretaget en grundig gennemlæsning af transskriptionerne for at opnå en helhedsfornemmelse af hvert interview. Under denne indledende gennemgang havde vi særligt fokus på at identificere de gennemgående temaer og centrale pointer. Når vi stødte på særligt interessante udsagn, markerede vi dem med farvekoder, hvilke relaterer sig til de overordnede tematiske kategorier (Bilag 24).

For at styrke undersøgelsens validitet har vi med udgangspunkt i vores mixed methods-tilgang bestræbt os på at genbruge kodninger fra både retsdokumenter og interview, med henblik på at lade dem validere hinanden. På den måde har vi kunnet undersøge, hvorvidt der optræder konsistens og sammenfald i empirien afhængigt af de forskellige kontekster, hvori de optræder. Dette bidrager til en mere nuanceret og pålidelig undersøgelse af BBB.

5.9 Etiske overvejelser - brugen af hacket data

Dette afsnit har til formål at belyse de etiske overvejelser forbundet med brugen af hacket data.

I den indledende fase af specialet blev vi præsenteret for muligheden for et samarbejde med efterretningsvirksomheden Truesec, som var i besiddelse af en større mængde *hacket data* i form af chat-logs og optagelser af svindelopkald. Hacket data betyder, at dataen er opnået på uautoriseret vis gennem ulovlig adgang til en computer eller et computernetværk (Ienca & Vayena, 2021:744). En af udfordringerne ved brugen af hacket data er, vi ikke kender formålet med, og motivet bag selve hackingen. Forskere påpeger, at hacket data kan være "*helt eller delvist fabrikeret af svært identificerbare aktører med uigennemsigtige motiv*er" (Ibid.:746, oversat til dansk). Eftersom vi ikke har viden om, hvem der har indsamlet dataene og med hvilken hensigt, gør det, det udfordrende for os, at sikre datakvaliteten. Endvidere kan hacket data stride imod forskningsetiske principper og svække forskningens integritet på flere måder, f.eks. ved at ignorere informeret samtykke, forsage sekundær skade på ofrene, krænke privatliv og fortrolighed og ved at sænke kvalitetsstandarderne (Ibid.).

Vores indledende tanke var, at datamaterialets omfang og indhold kunne give os en unik indsigt i centrale aspekter af fænomenet, herunder rekrutteringsstrategier, den interne organisering i netværket og kommunikation mellem aktørerne. Særligt muligheden for at få et sjældent kig ind bag scenetæppet gjorde materialet forskningsmæssigt attraktivt.

Efter grundig faglig og etisk overvejelse valgte vi imidlertid ikke at inddrage materialet i vores undersøgelse. Selvom dataene kunne have bidraget med væsentlig viden om svindelpraksisser og netværksstrukturer, vurderede vi, at brugen af materiale opnået gennem hacking ville svække specialets integritet i for høj en grad. Datamaterialet fremstod som unik, men vi vurderede, at tilsvarende indsigter kunne opnås gennem alternative, mere etisk forsvarlige kilder såsom de anvendte retsdokumenter.

6. Analyse

Specialistens analyseafsnit omfatter tre delanalyser, som hver bidrager med et unikt perspektiv på forskellige aspekter af BBB. Afslutningsvis visualiseres fænomenet i et crime script.

6.1 Delanalyse 1) Netværk og organisering

Analysens første del består af en række korte deskriptive analyser, som har til formål at kortlægge centrale karakteristika ved de enkelte kriminelle netværk, for at kunne sammenligne netværkene på tværs. Netværkene er inddelt ud fra retsdokumenter, så personer dømt i samme sag regnes som del af samme netværk. I nogle tilfælde har vi kun haft adgang til én eller to domsudskrifter, hvilket betyder, at nogle netværk omfatter flere personer, mens andre kun baseres på én.

Endvidere sammenlignes generelle tendenser i netværkene, særligt i forhold til netværkenes fremgangsmåder, succes, organisering og rollefordeling. Et væsentligt formål med denne del af analysen er at danne et overblik over ligheder og forskelle mellem netværkene, samt give indsigt i deres organisatoriske opbygning og operationelle praksis.

Tabel 4 - Oversigt over netværk

Netværk	Køn	Alder	Svindlens levetid	Økonomisk indtjening	Samlet antal ofre* (succesrate %)
Netværk 1	Mand	35 år	10 måneder og 28 dage	1.345.408 kr.	9 (100 %)
Netværk 2	Mand	46 år	21 dage	187.000 kr.	24 (58 %)
Netværk 3	2 mænd	21 år og 24 år	1 måned og 26 dage	151.800 kr.	18 (66 %)
Netværk 4	Mand og kvinde	27 år og 29 år	2 måneder og 28 dage	1.485.797 kr.	31 (91 %)
Netværk 5	2 mænd	19 år og 24 år	2 måneder og 19 dage	737.888 kr.	50 (98 %)
Netværk 6	Mand	22 år	1 måned og 26 dage	191.270 kr.	21 (76 %)

Netværk 7	Mand	30 år	9 måneder og 14 dage	1.571.919 kr.	210 (18 %)

6.1.1 Netværk 1)

Analysens første netværk tager udgangspunkt i en 35-årig mand, dømt ved Københavns Byret. Gerningspersonen har foretaget svindlen i forening med ukendte medgerningspersoner. Denne gerningsperson har udelukkende været aktiv på Sjælland. Han er ikke tidligere straffet, hvilket adskiller ham fra aktørerne i analysens øvrige netværk. I den aktuelle sag er han dog dømt for overtrædelser af våbenloven, knivloven, hvidvasklovgivningen samt hæleri.

Svindlens levetid er en periode på ti måneder og 28 dage og omfatter ni identificerede ofre. Med "levetid" henvises der til den periode, hvor netværket har opereret, frem til anholdelse. Der ses en succesrate på 100 pct., idet retsdokumentet ikke indeholder oplysninger om mislykkede svindelforsøg, dog kan sådanne ikke udelukkes. Dette netværk adskiller sig ved at have den højeste dokumenterede økonomiske gevinst pr. offer. Den samlede fortjeneste udgør 1.345.408 kr., svarende til knap 150.000 kr. pr. offer. Det forholdsvis lave antal ofre indikerer en mulig strategi, hvor fokus har været på færre, men økonomisk mere profitable bedragerier. Nedenstående citat illustrerer et eksempel på et særligt indbringende bedrageri beskrevet i retsdokumentet:

> *" [red: tiltale] kontaktede (offer) telefonisk og oplyste at nogen var ved bryde ind på (offers) bankkonto, hvilket bestemte (offer) til via sin bank at overføre i alt 355.000 kr. fra sin konto til en række anviste konti, samt overførte 85.000 kr. fra forurettedes kones konto til en anvist konto, ligesom tiltalte mødte op på forurettedes bopæl, og under påskud af at være fra banken og bestemte (offer) til at give tiltalte adgang til forurettedes computer og netbank, hvorved tiltalte uberettiget overførte i alt yderligere 49.500 kr. fra XX's konto, alt hvorved (offer) og (offer) samlet led et formuetab på ikke under 489.500 kr."(Bilag 16:25).*

Det særlige ved netværkets metode er, at fokus i højere grad ligger på at få ofrene til selv at foretage bankoverførsler, frem for at tilegne sig deres fysiske betalingskort med henblik på kontanthævninger. Denne tilgang muliggør en større gevinst, da netbank-transaktioner ikke er underlagt samme beløbsgrænser som kontanthævninger. Dog indebærer dette modus en øget

risiko for, at overførslen kan stoppes eller spores, i modsætning til kontanter fra hæveautomater, som udbetales øjeblikkeligt. Alligevel synes gerningspersonen at foretrække denne fremgangsmåde, da den både giver mulighed for større økonomisk gevinst og en lavere opdagelsesrisiko. Informanten fra Politiet fortæller, at videoovervågning fra hæveautomater spiller en væsentlig rolle i efterforskningen og opklaringen af sagerne (Bilag 10). Det kan derfor fremstå som en bevidst strategi fra gerningspersonen at undgå fysiske hævninger for dermed at reducere risikoen for identifikation. Set i lyset af *RCT* betragter vi denne adfærd som et udtryk for en strategisk og rationel beslutningstagning, hvor gerningspersonen afvejer risici og gevinst, og dermed vælger den fremgangsmåde, der giver størst udbytte med mindst sandsynlighed for opdagelse.

6.1.2 Netværk 2)

Analysens næste netværk består af en mand på 46 år, som er dømt ved Retten i Odense, sammen med hans, for os ubekendte, medgerningsmænd. Der er ingen indikation for tidligere kriminalitet, misbrug eller tilknytning til euforiserende stoffer. Netværket er yderligere kendetegnet ved, dets geografiske spredning som viser en høj grad af mobilitet, på tværs af flere danske landsdele.

Gerningspersonen var aktiv i blot 21 dage før han blev anholdt, men nåede at opnå en dokumenteret indtjening på 187.000 kr. fordelt på samlet set 24 ofre, svarende til en gevinst på 13.357 kr. pr. offer. Med en succesrate på 58 pct.fremstår bedragerierne relativt effektive, selvom der var en stor andel mislykkedes forsøg, formentlig fordi ofrene blev mistænksomme. Netværkets fremgangsmåde følger den klassiske metode, som fremgår af netværk 3, hvor offeret informeres om mistænkelig aktivitet på kontoen, hvorefter 'banken' sender en medarbejder ud for at hente kortet og sikre pengene.

Ydermere anvender dette netværk et karakteristisk hævningsmønster, hvor bankbuddet først hæver det maksimale beløb, som hæveautomaten tillader, f.eks. 15.000 kr. eller 6.000 kr., og derefter foretager yderligere hævninger af et mindre beløb, typisk omkring 2.000 kr.

6.1.3 Netværk 3)

Analysens tredje netværk omfatter to mænd på 21 og 24 år, som er dømt ved Retten i Herning. Den 24-årige har desuden begået BBB ed to andre, hvor han tilsyneladende havde en koordinerende rolle og dirigerede andre til ofrenes adresser. Kommunikationen er primært foregået via Signal og Snapchat, hvilket tyder på et ønske om at undgå politiets søgelys. Brug af krypterede og hurtigt slettende beskeder kan tolkes som en bevidst strategi. Set ud fra RCT kan dette være et udtryk for en mindre risikovillig adfærd, ud fra et forsøg om bevidst at undgå at lave et digitalt spor. Således reduceres risikoen for opdagelse og retsforfølgelse, hvilket fremhæver deres strategiske og kalkulerede overvejelser.

Begge gerningspersoner er dømt for besiddelse af euforiserende stoffer til både videresalg og eget forbrug, hvilket indikerer et aktivt misbrug. Den ene er desuden dømt for våbenbesiddelse og dokumentforfalskning, hvorfor historikken peger på en vedvarende kriminel løbebane.

Geografisk opereres der udelukkende i Midtjylland, specifikt i Herning og Holstebro. Begge gerningspersoner har bopæl i Herning, hvilket antyder, at netværket har handlet i nærområdet og udnytter deres lokale kendskab, muligvis også til at identificerer potentielle ofre. Denne lokale forankring kan indikere en lavere grad af organisatorisk kompleksitet og mobilitet.

Netværket var aktivt i 1 måned og 26 dage har i denne periode opnået en samlet indtjening på 151.800 kr. fordelt på 18 bedrageriforsøg. I 12 tilfælde led ofrene økonomisk tab, svarende til en succesrate på 66 pct. og en gennemsnitlig gevinst på 12.650 kr. pr. succesfuld svindel. Nedenstående citat illustrerer hvordan sagerne i dette netværk overvejende er struktureret og gennemført:

> *" […] i forening og efter forudgående aftale eller fælles forståelse, for derigennem at skaffe sig eller andre uberettiget vinding, retsstridigt at have fremkaldt og udnyttet en vildfarelse hos (offer), idet de tog telefonisk kontakt til (offer) og under påskud af at være fra banken formåede (offer) til at udlevere kreditkort med tilhørende kode, hvorefter de retsstridigt påvirkede resultatet af en elektronisk databehandling, idet tiltalte [red: 21-årig] […], hævede […] kontanter […] ved brug af kreditkortet og koden, hvorved (offer) led et tilsvarende formuetab*" (Bilag 18:2).

Denne metode er typisk, dog kan der i dette netværk betragtes en tydeligere rollefordeling mellem de involverede. Begge deltager i den indledende telefoniske kontakt, men den 24-årige har en mere koordinerende rolle, mens den 21-årige er udføreren, der afhenter betalingskortene og

foretager kontanthævninger. Dermed påtager den 21-årige sig den mest risikofyldte opgave, idet han nemmere kan identificeres via overvågningsmateriale og dermed direkte forbindes til bedrageriet. Dette kan tolkes som et udtryk for, at han indtager den laveste position i det interne hierarki. Vi formoder, at den 24-årige må besidde en mere koordinerende rolle, med en smule mere ansvar for at organisere operationerne og udvælge adresserne, hvor svindlen skal finde sted. Den ledende rolle bekræftes også eksplicit i retsdokumentet (Bilag 18:28).

6.1.4 Netværk 4)

Det fjerde netværk, dømt i retten i Næstved, udgør et søskendepar bestående af en mand på 27 år, som primært står for at misbruge kortene og en kvinde på 29 år, som bl.a. står for opringninger og intern kommunikation (Bilag 19). Det er det eneste netværk, hvor en kvinde deltager aktivt i bedrageriet. Netværket virker mobilt, da de opererer på tværs af store dele af landet, med undtagelse af Nordjylland. Begge gerningspersoner er tidligere straffet, og er i den pågældende sag ligeledes dømt for anden kriminalitet, ud over BBB.

Søskendeparret var aktive i en periode på to måneder og 28 dage inden anholdelse. I perioden har de genereret en samlet dokumenteret indtjening på 1.485.797 kr., fordelt på 31 bedrageriforsøg. Ud af disse har 29 resulteret i økonomisk tab for ofrene, hvilket svarer til en gennemsnitlig indtjening på cirka 51.234 kr. pr. succesfuldt bedrageriforhold. Med en dokumenteret succesrate på 91 pct. har netværket således opnået økonomisk gevinst i ni ud af ti tilfælde, hvilket vidner om en særdeles effektiv og målrettet fremgangsmåde.

Søskendeparret har ligeledes anvendt den klassiske fremgangsmåde, som beskrevet ovenfor, og i lyset af den høje gennemsnitlige indtjening pr. offer må metoden betragtes som både effektiv og lukrativ for gerningspersonerne.

6.1.5 Netværk 5)

Det femte netværk består af to mænd på henholdsvis 19 og 24 år, som blev dømt ved Retten i Viborg. Deres svindel har primært foregået i Nordjylland og Midtjylland, med enkelte tilfælde i Sønderjylland. Dette afspejler, i lighed med flere af de øvrige netværk, en vis bevægelighed og villighed til at flytte sig for opgaverne. Den 24-årige er tidligere dømt for bl andet berigelseskriminalitet, mens den 19-årige ikke tidligere er straffet. Dog er vedkommende i denne sag er dømt for yderligere lovovertrædelser, herunder overtrædelse af færdselsloven, Lov om euforiserende stoffer samt ordensbekendtgørelsen.

Netværket var aktivt i to måneder og 19 dage, hvor de generede en dokumenteret indtjening på 737.888 kr., fordelt på 50 direkte og indirekte ofre. Den gennemsnitlige indtjening pr. succesfuldt offer udgør cirka 15.000 kr.

Netværkets fremgangsmåde er i overensstemmelse med det mønster, der ses i de øvrige netværk, hvor en systematisk og koordineret tilgang benyttes for at opnå økonomisk gevinst gennem BBB. Noget særligt er, at de to dømte bankbude har haft klare overvejelser om deres roller i mødet med ofrene, samt hvordan de skal fremstå, for at virke så troværdig som muligt. Personen med etnisk dansk udseende blev sendt ud til ofrene, mens den anden, som er af somalisk oprindelse, stod for kontanthævningerne. I retten forklarede de, at " [...] f*ordelingen af rollerne skyldes, at de ældre nemmere ville tro på ham, mens de ikke ville tro på en somalier*" (Bilag 20:33). Dette vidner om en bevidst udnyttelse af sociale og etniske fordomme som en strategisk komponent i svindlens iscenesættelse.

6.1.6 Netværk 6)

Det sjette netværk består af en 22-årig mand, som er dømt ved Retten i Aarhus. Manden arbejder i forening med, for os, ukendte gerningsmænd. Der opereres bredt, med geografisk aktivitet i både Syddanmark, Midtjylland og Nordjylland.

Gerningspersonen er tidligere straffet, og dømmes samtidigt i den verserende sag for overtrædelser inden for både euforiserende stoffer, knivlov, hæleri, trusler samt diverse færdselsforseelser. Der forekommer konkrete eksempler, der vidner om et aktivt misbrug.

Netværket var aktivt i 1 måned og 26 dage har i denne periode opnået en samlet indtjening på 191.270 kr. fordelt på 21 bedrageriforsøg. I 16 tilfælde led ofrene økonomisk tab, svarende til en succesrate på 76 pct.og en gennemsnitlig gevinst på 11.954 kr. pr. succesfuld svindel.

Metodemæssigt læner gerningspersonen sig op ad den tidligere omtalte fremgangsmåde, og har ligeledes økonomisk profit for øje. Netværket foretager hovedsageligt kontanthævninger, hvor der kan betragtes en systematik i, at der først hæves et højere beløb á 15.000 kr., 10.000 kr., eller 6.000 kr., hvorefter dette næsten hver gang efterfølges af en kontanthævning på 2.000 kr.

6.1.7 Netværk 7)

Det syvende netværk består af 30-årig mand, dømt i retten i Svendborg. Hans svindelaktiviteter har fundet sted både i Jylland og på Fyn. Gerningspersonen er tidligere straffet og blev i samme dom ligeledes dømt for salg af euforiserende stoffer.

Svindlen har fundet sted over en periode på 9 måneder og 14 dage, hvor gerningspersonen har opnået en samlet dokumenteret indtjening på 1.571.919 kr., fordelt på 210 direkte og indirekte ofre. På trods af det høje antal ofre, viser datene en relativt lav succesrate på 18 pct., hvilket vil sige, at under hver femte svindelforsøg har resultere i et økonomisk tab for offeret. Selvom succesraten er relativt lav, er den gennemsnitlige indtjening pr. direkte offer, forholdsvis høj, hvor det økonomisk tab på ligger på 41.366 kr. Dette indikerer, at når svindlen lykkes, er gevinsten betydelig.

Vi har en formodning om, at grunden til, at der indgår en stor mængde mislykkedes forsøg i dette retsdokument er, at den er baseret på data fra TrueSec, som vi blev præsenteret for i vores indledende research. Denne formodning baseres på en samtale med en specialist fra TrueSec, hvor det fremgik, at de havde givet data til politiet, som hjalp med optrevlingen af et større netværk med tilknytning til en retssag på Fyn. Selvom vi ikke med sikkerhed kan bekræfte denne forbindelse, fremstår det som en plausibel forklaring, da materialet rummer en betydelig mængde opkald, hvor modtageren ikke er identificeret. Dette indikerer, at oplysningerne ikke stammer fra ofrenes egne anmeldelser, men snarere fra teknisk overvågning.

Derudover rummer retsdokumentet informationer om årsagerne til, at flere svindelforsøg mislykkes. Blandt disse faktorer nævnes, at familiemedlemmer griber ind, ofre fatter mistanke undervejs og afbryder samtalen, at ofrene ikke befinder sig hjemme, eller at kontakten sker på uhensigtsmæssige tidspunkter, f.eks. under handleture eller middagslure. Disse forhold illustrerer, hvordan selv små sociale eller praktiske forstyrrelser kan forhindre svindlen i at lykkes, hvilket understreger svindlernes afhængighed af timing.

6.1.8 Sammenfatning – generelle tendenser

Formålet med dette afsnit er at belyse nogle overordnede karakteristika ved de personer, der begår BBB. På baggrund af retsdokumenterne samt ovenstående tabel 4, fremgår det, at ni ud af ti dømte bankbudsbedragere er mænd. Dette peger på, at BBB primært er en mandligt domineret kriminalitetsform Den ene kvindelige gerningsperson fremstår derfor som en bemærkelsesværdig undtagelse fra et ellers entydigt kønsmønster. Ifølge vores informant fra Politiet,

som har viden om 70 bankbudsbedragere fra sin politikreds, udgør kvinder kun en marginal andel af de identificerede gerningspersoner (Bilag 10: linje 407). Han oplyser, at han alene har kendskab til tre til fire kvinder, som er dømt for denne type kriminalitet.

Gennemsnitsalderen for de dømte bankbude er 28 år, hvilket ligger lidt højere end den typiske top i den velkendte *age-crime curve*, som ofte viser, at kriminalitet topper i de sene teenageår til tidlige 20'ere (Moffitt, 2022:576). Denne tendens kan indikere, at succesfuldt BBB, kræver et vist niveau af modenhed eller organisatoriske evner, som er noget man kan tillære med tiden. Set i lyset af, at de fleste af gerningspersonerne har en kriminalitetshistorik, kan denne højere alder indikere, at de ikke er nået til deres "*turning point*" i livet endnu. Ydermere viser dataene, at 70 pct. af gerningspersonerne udviser tegn på aktivt misbrug. Behovet for at kunne finansiere et sådant misbrug kan være en central drivkraft, der fastholder dem i kriminalitet, idet penge til stofferne skaber et konstant incitament til fortsat kriminel aktivitet.

To personer har hverken tidligere domme, andre sigtelser i denne sag eller tegn på aktivt misbrug. Øvrige gerningspersoner har næsten alle en historik med tidligere domme og/eller aktivt misbrug. Dette kan altså betyde, at de har en risikoadfærd, hvilket kan øge sandsynligheden for gentagen kriminalitet.

På baggrund af ovenstående, kan det udledes at det typiske bankbud, der bliver anholdt, er en mand på cirka 28 år med en kriminalitetshistorik og et aktivt misbrug.

<u>Aktivitet – opsummering</u>

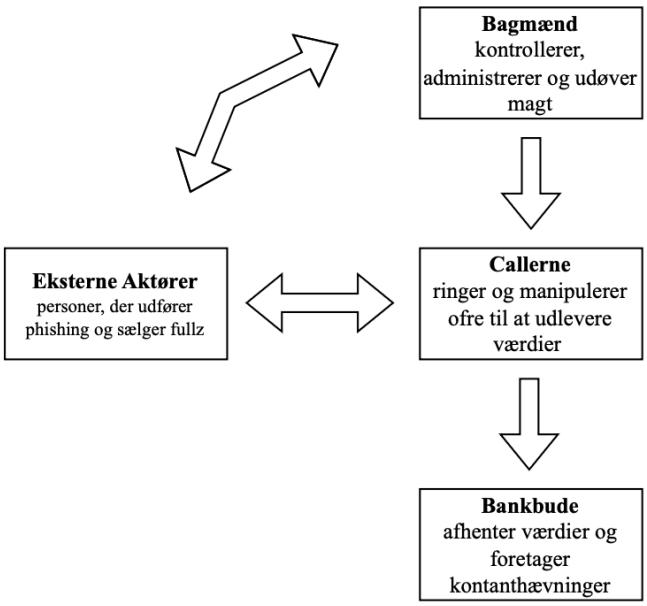
For hvad angår netværkenes aktivitetsmønstre, har vi forsøgt at komprimere vores data, for således at kunne udlede nogle mere generelle tendenser om svindelnetværk som vores. I forhold til netværkenes levetid, som henviser til, i hvor lang en tidsperiode de begår svindel, frem til at de bliver anholdt, ser vi bred variation. Netværkenes levetid spænder fra blot 21 dage, til op til 10 måneder og 28 dage. Gennemsnitligt kan vi påvise en levetid på 3 måneder og 23 dage, hvilket således udgør den tidsperiode, hvori det typiske netværk formår at udføre svindlen, inden de bliver 'fanget'. I forbindelse med anholdelsestidspunktet, har vi klarlagt at tre ud af de i alt syv netværk, bliver pågrebet på såkaldt 'fersk gerning*',* og dermed mens de aktivt er i færd med at udføre et bankbudsbedrageri (Bilag 14c). Endvidere har vi udledt, at det at være en del af et sådant netværk, sjældent er en dårlig forretning. Vi har udført en kronologisk gennemgang af hver enkel aktivitet, hvor et bankbud enten elektronisk overfører penge til egen

konti, laver en fysisk kontantafhentning, eller som den hyppige, fortager en hævning i en hæveautomat. Resultatet heraf, består af omfattende pengesummer, hvor svindelnetværk som disse faktuelt tjener alt i mellem 187.000, og op mod 1.571.919 kr., hos det mest indbringende netværk. Overordnet har vi identificeret en samlet økonomisk gevinst, på 5.671.082,71 mio. kr., fordelt på de syv netværk. Her opnår det typiske netværk en gennemsnitlig profit på 810.154,57 kr., hvortil vi må anerkende, at gerningspersonernes motivation og øje for profitmaksimering, for dem, har fordelagtige resultater på bundlinjen. På trods af, at tallene er af betydelig størrelse, har alle netværk ikke lige stor succes. Vi har kortlagt hvor ofte og i hvilket omfang, svindlerne lykkedes med deres plan. Hertil vi ser en markant variation i succesraten som fordeler sig mellem 18 – 100 pct., hvoraf hele tre af netværkene opererer med en succesrate på minimum 91 pct. Vi er opmærksomme på, at der her kan eksistere mulige fejlkilder (jf. afsnit 6.1.7). Gennemsnitligt udleder vi en generel succesrate, hvor bankbude ved 72 pct. af tilfældene lykkedes med at op opnå et økonomisk udbytte. Som led i undersøgelsen af al aktivitet i netværkene, har vi som allerede nævnt, fundet mønstre i deres geografiske mobilitet under deres aktivt processer. Et enkelt netværk opererer udelukkende i deres eget nærområde (baseret på gerningspersonernes privatadresser), mens de resterende netværk udviser særdeles høj grad af geografisk mobilitet. Derfor vurderer vi, at et generelt kendetegn ved BBB er, at aktørerne konstant flytter sig rundt, afhængigt af opgaver og således ikke er geografisk forankret. Hertil tænker vi, at deres hyppige forflytninger kan finde sted med afsæt i en risiko for at blive opdaget ved stilstand og meget aktivitet i konkrete geografiske områder.

Rollefordeling og organisering

Dataene viser, at al BBB er begået i forening med andre gerningspersoner, hvilket understøtter en forståelse af disse grupperinger som kriminelle *firmaer* (netværk) (Bilag 14c). I disse firmaer har gerningspersonerne forskellige roller, som hver især er afgørende for bedrageriets gennemførelse og succes. På baggrund af datene har vi identificeret fire hovedroller: *bankbude, callere, bagmænd* og *eksterne aktører* (se figur 2).

Figur 2: Organisering af bankbudsnetværk



Rollen som bankbud er den, hvor gerningspersonerne klart hyppigst identificeres og retsforfølges, hvilket tyder på, at denne funktion er forbundet med den højeste risiko for opdagelse. Det tolker vi som et udtryk for, at bankbudene indtager den nederste position i netværkets hierarki. Vi uddyber denne fortolkning i afsnit 6.3.8, hvor vi forholder os til bankbudenes udsatte position i "fødekæden". På baggrund af vores analyse vurderer vi desuden, at bankbudene som udgangspunkt primært fungerer udførende aktører, hvilket vidner om en klar struktur og rollefordeling. I nogle tilfælde ser vi at bankbudene også, til tider, påtager sig rollen som caller.

At være *caller* udgør en central rolle i netværket, hvor gerningspersonen via telefonisk kontakt manipulerer ofrene til at udlevere værdier samt koordinerer bankbudenes bevægelser. Ifølge politiet er callernes identitet ofte vanskeligt at afdække, og kun få er blevet identificeret og anholdt (Bilag 10). Callerne er som udgangspunkt ikke fysisk til stede ved ofrenes adresser, men opererer fra forskellige lokationer. Disse lokationer fortolker vi, som 'kontorer', der kan antage to former: *callcentre* og "*rullekontorer"*. Et *callcenter* betegner en fast fysisk lokation, hvor flere gerningspersoner foretager opkald fra samme sted. *Rullekontorer* derimod, refererer til mobile enheder, hvor callere foretager opkald direkte fra bilen, hvor bankbudene også er til stede. Rullekontoret er anvendes i høj grad i netværk 7.

Hierarkisk over callerne findes en gruppe mere magtfulde og styrende aktører, som flere bankbud omtaler som "grimme" og farlige personer (Bilag 19; 20a-b). Disse opfattes som de egentlige bagmænd, hvis identitet forbliver ukendt. De besidder en magtfuld og kontrollerende rolle over de lavere rangerende aktører i netværket og fremstår som centrale koordinatorer i den kriminelle infrastruktur. Flere bankbud forklarer, at kommunikationen med bagmændene foregår på engelsk, hvilket kan indikere internationale forbindelser og et mere omfattende organiseret netværk. Trusler og kontrol synes at være integrerede elementer i deres arbejdsgang, hvilket bl.a. fremgår af en hændelse, hvor en 29-årig kvindelig gerningsperson i netværk 4 blev truet med, at hendes barn ville blive dræbt, fordi hun angiveligt havde snydt bagmændene (Bilag 19). Dette vidner om en udpræget voldsparathed og en intimiderende autoritet i netværkets øverste lag.

I en ideel kriminel organisation vil det være rationelt at opbygge strukturen, så risikoen for anholdelse minimeres, særligt for de ledende aktører, der koordinerer svindlen. Denne logik synes også at præge opbygningen af bankbudsnetværkene, hvor de bliver bygget op således, at det er vanskeligt at identificere og retsforfølge bagmændene. Netværkene konstrueres således, at kun enkelte led kan anholdes ad gangen, hvilket reducerer sandsynligheden for, at hele organisationen afsløres samlet og går i opløsning. Det ses bl.a. ved, at bankbudene ofte ikke har direkte kontakt med bagmændene, og derfor heller ikke kender deres identitet. Den manglende retsforfølgelse af bagmændene kan således forstås som en konsekvens af denne bevidste organisatoriske adskillelse.

Rekruttering til bankbudsnetværk kan foregå på flere måder. Nogle tilbyder selv deres arbejdskraft via krypterede platforme, mens andre rekrutteres grundet gældsrelationer til organiserede kriminelle miljøer. Vi formoder, at bagmænd opkøber bankbuddets gæld fra andre kriminelle organisationer, og tilbyder en form for gældsnedsættelse i bytte for deltagelse i svindlen (Bilag 10; 20a). I netværk 5 fremgår det f.eks., at den ene gerningsperson blev involveret for at hjælpe en kammerat med at afdrage gæld til en kriminel organisation. Den anden gerningsperson blev introduceret til svindlen af sin kammerat, og lod sig rekruttere med henblik på hurtig indtjening, efter at have fået indtryk af, at BBB var en nem og effektiv måde at skaffe penge på (Bilag 20a).

På baggrund af al ovenstående fremstår BBB som en velorganiseret kriminalitetsform, kendetegnet ved en tydelig rollefordeling og hierarkisk struktur. Denne organisatoriske kompleksitet

og professionalisme kan være medvirkende til den lave risiko for opdagelse (for bagmændene) og til svindelens høje udbytte.

6.2 Delanalyse 2) Det oplagte offer for bankbudsbedrageri – viktimologi

Den indledende analyse af offerprofilen ved BBB tager udgangspunkt i ofrenes objektive karakteristika, for at identificere ofrenes typiske kendetegn og position i samfundet. Formålet er at identificere mønstre, og formulere et kvalificeret bud på en typisk offerprofil. De objektive karakteristika omfatter bl.a. køn, alder, navn, boligsituation og ressourcer.

Dernæst går analysen i dybden med ofrenes adfærd og vaner i forbindelse med svindlen. Analysen inddrager løbende neutraliseringsteknikker og relevante teoretiske perspektiver, for at belyse de mekanismer, der gør visse personer mere udsatte for denne type kriminalitet. Afslutningsvis behandles spørgsmål om skyld og skam, herunder de psykologiske og sociale konsekvenser for ofrene.

6.2.1 Et kønnet bedrag – kvinder som primære ofre

Et af de mest fremtrædende mønstre, som vi udleder af både retsdokumenter og informanter, er kønnets betydning for at blive et offer. I de tilfælde, hvor det er lykkedes svindlere at bedrage deres ofre, og disse dermed har lidt et økonomisk tab, viser vores data, at 24 mænd og 144 kvinder kan registreres som værende *direkte* ofre. Ser vi derimod på de *indirekte* ofre, altså personer, der har været udsat for et svindelforsøg uden nødvendigvis at have lidt et tab, optræder 182 kvinder og blot 12 mænd. Vi har valgt at inddrage både de direkte og indirekte ofre i denne sammenhæng, hvilket skyldes en undren over, hvorvidt det lykkedes at svindle kvinder oftere end mænd, eller om svindlerne systematisk går efter at ramme kvinder. Denne tese kan være med til at indikerer at der ligger nogle konkrete rationaler bag svindlernes udvælgelse af ofre. Statistikken viser således en klar kønsmæssig skævhed i svindlernes målretning. Både blandt de direkte og indirekte ofre ses en markant overrepræsentation af kvinder, hvor 90 pct. udgøres af kvinder. Det indikerer, at svindlerne i overvejende grad retter deres henvendelser mod kvinder frem for mænd uagtet om svindlen lykkes eller ej. Vores første karakteristika hos 'det oplagte offer', er således, at hun er en kvinde. Som årsagsforklaring til denne skævhed er der flere overvejelser. Selv ser vi, at der kan herske en række biologiske og psykologiske faktorer der adskiller kvinder fra mænd, hvoraf nogle faktorer kan svække deres påvirkelighed for manipulation i forskellige kontekster.

I relation til de kvindelige ofre spiller sociale kompetencer en væsentlig rolle, idet kvinder i højere grad opdrages til at være mere samarbejdsvillige, hjælpsomme og relationsorienterede. Det viser forskningen om kvinders adfærd, som tilmed beskriver hvordan de i gennemsnit har større følelsesmæssig resonans end mænd (Haselhuhn et al., 2015). Med andre ord har de tendens til at føle mere intenst med andre, hvilket kan resultere i, at de har en større påvirkelighed overfor manipulation, særligt når en potentiel svindler ganske velovervejet spiller på deres følelsesregister. Med udgangspunkt i SE, ser vi, hvordan det at opbygge relationer, kan gøre kvinder til en særligt udsat gruppe når det kommer til manipulation. En informant fra banken, som jævnligt er i direkte kontakt til disse kvinder udtaler:

> *"Kvinder på 80 år eller derovre har et eller andet med autoriteter. De er ekstremt autoritetstro, så hvis de køber ind på præmissen om, at der er en bankmand de taler med, så kan de få dem til hvad som helst […] men så er der en hel masse andre modus, der rammer mænd"* (Bilag 11:linje 212-216)

Det ovenstående citat er langt fra enestående og illustrerer, hvordan kvinder til tider investerer mere i følelsesmæssige relationer end mænd. Dette gør dem mere sårbare over for svindlere, der bevidst udnytter disse psykologiske triggere.

Os bekendt, er der et mønster i, at det ofte er nemmere at få fat i kvinderne end mændene. Det kan skyldes den simple årsag, at kvinderne lever længere, hvorfor en større andel kvinder end mænd er enlige og bor alene, når de kommer op i årene (jf. Bilag 10). Herudover, er der blandt den ældre generation en tydeligere opdeling i kønsrollerne blandt de sammenboende. Politiet beskriver hertil at:

> *"Mænd over 70-80 år, de er jo gift på den 'gamle ordning', så der er det kvinden der tager telefonen. Manden siger, 'Jeg gider fandme ikke sidde og snakke i telefonen, det må du klare.' Så der er formentligt så mange traditioner og adfærd, og vaner, der gør at det er kvinderne der står for det her"* (Bilag 10: linje 526-529)

I relation til kvinders sårbarhed har ovenstående studie vist, at kvinder, sammenlignet med mænd, i højere grad har tendens til at stole på personer, de opfatter som troværdige, især når

relationen er opbygget over tid (Haselhuhn et al., 2015). "Over tid" kan dog være et vidt begreb, der kan dække over forskellige tidsforløb. I forhold til tilliden der opbygges, har vi valgt at undersøge, hvor lang tid der reelt er direkte kontakt mellem calleren og offereret. I den forbindelse bemærker vi, at selve telefonopkaldet mellem de to parter ofte er af længere varighed.

I en vidneforklaring fra retsmødet i Næstved, fremgår det, at et samtaleforløb mellem et offer og netværket har strukket sig over 6 timer. I samme vidneudsagn har offeret beskrevet hvorledes vedkommende fik besked på, at de ikke måtte afbryde opkaldet. Ydermere har vidnet beskrevet hvordan der blev pålagt et akut tidspres, idet vedkommende skulle handle inden midnat, fordi deres formue ellers ville gå tabt (Bilag 19: linje 93)

I en dialog på op mod flere timer, bliver det således muligt for gerningspersonerne rent faktisk at opbygge en vis relation til deres offer. Her ved vi, at de anvender deres sociale kompetencer såsom sympati og venlighed med henblik på, hurtigt at etablere en tillidsrelation. Ikke nok med det, sikrer de langvarige opkald tilmed at forurettede holdes beskæftiget med samtalen, så deres opmærksomhed afledes fra, hvad der realiteten foregår omkring dem. Således har forurettede ikke mulighed for at kontakte andre i mellemtiden, inden ofrenes betalingskort bliver misbrugt. Dette afspejler en bevidsthed om, at flere har for vane at rådføre sig med andre, hvis de står i en tvivlsom eller vanskelig situation.

Vi lægger vægt på, at de overstående nedslagspunkter ikke nødvendigvis betyder, at kvinder har vanskeligere til at udøve kritisk tænkning end mænd. Som vores informant fra SparNord fortæller, kan mænd naturligvis også blive ofre for svindel, men det er typisk andre former for svindel, de udsættes for. Når svindlere er så rationelle og professionelle, som de ofte er, og samtidig har en klar forståelse for psykologiske forskelle mellem kønnene gennem deres erfaring, kan de målrette deres manipulationsteknikker mod netop de følelser, behov og triggere, som kvinder typisk reagerer stærkere på.

6.2.2 Svindlernes navnelister – når fornavnet gør dig sårbar

I kortlægningen af netværkenes færden, blev vi opmærksomme på, at der kan betragtes en vis form for systematik i hvilke ofre, gerningspersonerne sigter efter når det gælder konkrete navne. Helt lavpraktisk ser vi, at svindlerne henvender sig til en person, med et bestemt navn hvorefter de i de efterfølgende timer systematisk går videre til andre personer med nøjagtigt

det samme fornavn, som har bopæl inden for en kort radius af deres første offer (Bilag 14a-b). Svindlerne arbejder sig således igennem konkrete fornavne inden for konkrete områder. For at kunne bekræfte denne metode i offerselekteringen, ser vi helt konkret 14 kvindelige ofre, som alle har fornavnet *'Inge*' eller *'Inger'*. Dette skal ses i lyset af, at vi udelukkende er i besiddelse af ofrenes fornavne i 114 tilfælde af de gennemførte svindelsager. Vi kan derfor fastslå, at der blandt alle de syv netværks samlede gruppe af ofre, er 10 pct. som bærer fornavnet *'Inge'* eller *'Inger*'. Mønstre i selekteringen som disse, vidner om en tydelig systematik. Blandt de indirekte ofre, har vi kun fundet 24 fornavne. Igen ser vi helt konkret, at 8 ud af de 24 ofre, svarende til en tredjedel, bærer fornavnet '*Inge'* eller *'Inger'*.

Vi tror på, at denne målrettethed afspejler en bevidsthed om, at navnet '*Inge'* og '*Inger'* primært er at finde blandt den ældre befolkningsgruppe. Det bekræfter vi efterfølgende gennem Danmarks statistik, som påviser at navnet er kraftigt nedadgående, idet navnet er blevet halveret fra perioden 2002 til 2025 (Danmarks statistik, 2025). Andre navne som svindlerne ofte har i søgelyset, er særligt *'Ruth'* og *'Else'*, og for mænd, indtager navnet *'Vagn'* en førsteplads. Alle navne, som ifølge vores overbevisning, primært er tilhørende den ældre generation.

Metoden i, at selektere ofre ud fra lavpraktiske karakteristika såsom navne kan pege på flere bagvedliggende rationaler, idet svindlernes forarbejde for at nå hertil, kan være foregået på flere måder. Vi ved, at udvælgelsen af ofre sommetider tager afsæt i ulovligt, handlede *fullz,* som kan indeholde personoplysninger, her bl.a. navne, bankoplysninger, telefonnumre og adresser (Hameed et. al, 2025). Disse oplysninger kan sælges rundt mellem kriminelle på krypterede platforme. Oplysningerne er ofte indhentet ved, at der forinden er foretaget diverse phishing-scams, hvor dem, der nu er oplysninger om, er 'hoppet i fælden'. Det sker bl.a., når der trykkes på et uægte link, eller der udleveres personlige oplysninger under falske forudsætninger. Dette kan styrke svindlernes incitament til at gå efter personer, der tidligere er blevet svindlet, ud fra deres formodning om, at de samme personer også ville kunne narres igen. At svindlerne forbereder sig grundigt, og skaber sig adgang til vigtige oplysninger, understreger vores fund af, at svindlerne er strategiske, motiverede og orienterede mod profitmaksimering, hvilket understøtter, at der er tale om *predatory crime*. De går efter personer, der allerede er mulige at manipulere, for at bibeholde en høj succesrate og således en høj økonomisk profit.

Vi ser, at denne *cyber-aktiverede* anvendelse af teknologiske løsninger, er med til at effektivisere og understøtte processen i, at gerningspersonerne opnår en identifikation af potentielle

ofre, hvor de får bedre forudsætninger for at opnå succes. Vi formoder, ud fra denne viden, at svindlerne helt specifikt kommer i besiddelse af én lang liste med bl.a. navne, som de systematisk arbejder sig ned igennem, de dage, de er aktive i svindlen.

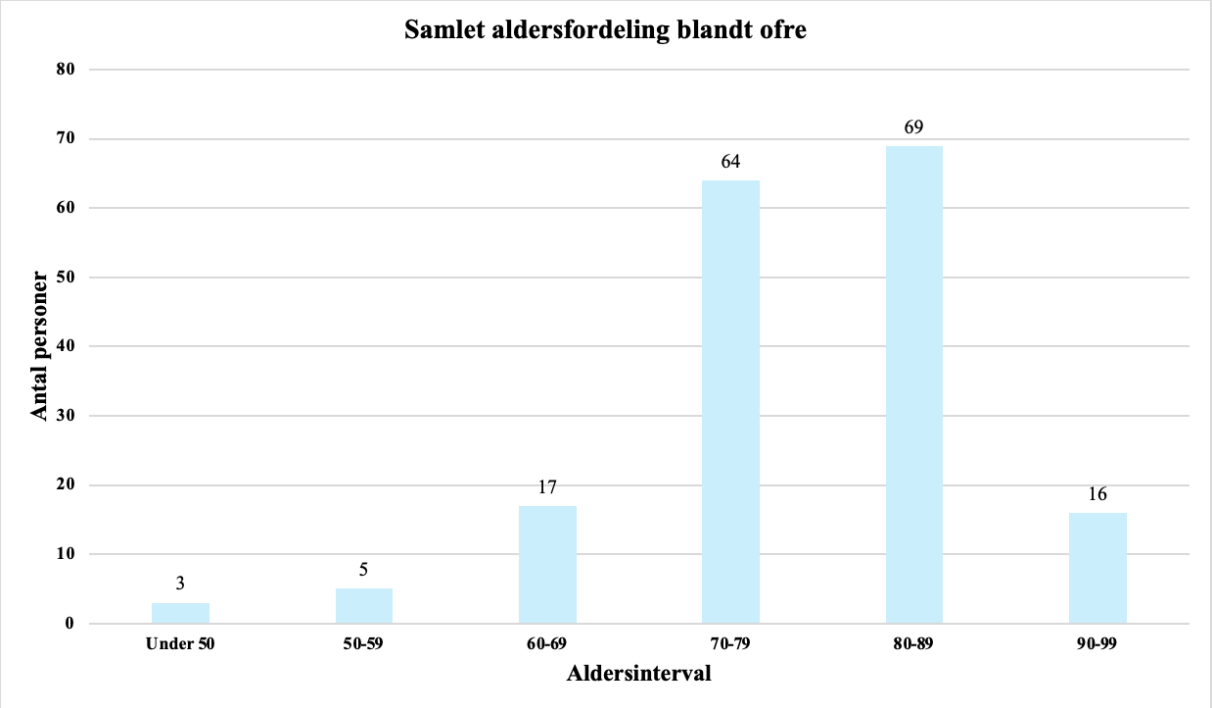
En anden, knap så innovativ metode til at udpege ofre, som vi har kendskab til, er at netværkene sommetider anvender 'Krak.dk', som er en offentlig tilgængelig kilde (Bilag 12). Denne metode er både simpel, legal og let tilgængelig. Dog kan svindlerne ikke få indsigt i, hvilke konkrete borgere der i forvejen allerede er blevet narret.

På baggrund af ovenstående vurderer vi, at udvælgelsen af ofrene og adgangen til dem ikke er tilfældig, men derimod afspejler et tydeligt forarbejde og velovervejede rationaler. Det tyder på, at gerningspersonerne har en klar interesse i at opretholde en høj succesrate, hvorfor de målretter deres ressourcer mod personer, som de vurderer, er realistiske og sårbare mål.

6.2.3 Ældre som svindlernes foretrukne mål

Et yderligere karakteristika, der bør betragtes i sammenhæng med de ovenstående, køn og navn, er alder. På baggrund af indledende research troede vi på, at det primært var den ældre del af befolkningsgruppen, som blev udsat for denne svindeltype. Vores faktiske tal af ofrenes aldersfordeling, har vi illustreret i nedenstående:

Tabel 5 – Aldersfordeling blandt ofre



Kilde: Bilag 14a; 14d.

Blandt de 174 totale ofre, hvor der foreligger oplysninger om alder, er den gennemsnitlige alder 81 år. Dette bekræfter, at den primære offergruppe for denne særlige form for bedrageri overvejende tilhører den ældre generation, hvor 85,6 pct. af den samlede offergruppe er over 70 år gamle. Om *legitime ofre* ved vi, at særligt ældre borgere i højere grad betragtes som ideelle ofre, da denne persongruppe anses som værende mere værdige ofre end andre. På den baggrund ser vi, at samfundet (bl.a. bestående af politi, medier, domstole og al anden offentlighed), er tilbøjelig til at udvise medfølelse, retfærdighed og tildeler ressourcer til dem, der passer bedst på denne skabelon (Christie, 1986:18-19). Vi ser denne forestilling som forankret i en opfattelse af ældre som svage, svækkede og uskyldige, da de ofte er afhængige af andres hjælp, f.eks. ved at deres voksne børn er behjælpelige med at administrere deres økonomi. Deres opfattede sårbarhed fremstår i vores øjne som et tegn på, at de hverken har haft del i handlingerne eller haft mulighed for at provokere en eventuel gerningsperson. Netop derfor vækker de ofte sympati blandt offentligheden, da de opfattes som uden ansvar for at de udvælges, hvorfor de uretmæssigt er blevet udsat for noget kynisk kriminalitet.

Som de fleste ved, kommer alderen sjældent alene, men det indebærer også en gradvis svækkelse af visse funktioner, i form af kognitive og fysiske aldersrelaterede forandringer. En informant beskriver, at han oplever at en væsentlig del af ofrene lider af demens: *"Mange af dem er blinde, døve og demente og sådan noget […] ældre, demente, svagelige mennesker bliver snydt, ribbet for alt, hvad de har* (Bilag 10:linje 76-77). Denne iagttagelse er i overensstemmelse med den forskning vi har fundet på området (jf. afsnit 4.2), og viser deres søgen efter de svageste ofre.

6.2.4 Ofrenes adfærdsmønstre - rutineaktiviteters betydning for viktimisering

På baggrund af de foregående afsnit, hvor vi har identificeret de objektive karakteristika for offergruppen, rettes fokus nu mod en mere dybdegående forståelse af ældre menneskers vaner, rutiner og adfærdsmønstre. Vi har på nuværende tidspunkt kortlagt, at det typiske offer BBB ofte er en ældre kvinde. Derfor vil det følgende afsnit i højere grad beskæftige sig med netop denne gruppes daglige praksisser og handlemønstre.

I den følgende del vil vi derudover undersøge de bagvedliggende forklaringsfaktorer og mekanismer, som kan belyse, hvordan visse vaner og rutiner, ofte forbundet med alder og livsfase,

kan medføre en adfærdsmæssig sårbarhed. Dette vil bidrage til at forklare, hvorfor ældre i særlig grad udgør en risikogruppe.

Et adfærdsmæssigt kendetegn ved vores gruppe af ofre, kan identificeres gennem de hændelser, de udsættes for. Disse hændelser vidner om konkrete mønstre og vaner, som er særligt fremtrædende. Baseret på de handlinger, vi observerer i forbindelse med ofrene, ser vi at der er tale om en gruppe med særlige adfærdstræk. Med en gennemsnitsalder på 81 år adskiller de sig især fra den yngre og midaldrende befolkning ved oftere at være i fysisk besiddelse af kontanter - en faktor, vi ser, der kan øge deres risiko for udsathed. Hertil udtaler SparNord:

> *"Den svage kundegruppe er de meget ældre. Når der går pension ind, så er der altså nogen, der bare måned efter måned, og går op og hæver alle pengene, fordi de føler, at de kan styre dem, og sådan har det altid været. Der kan være mange grunde, men der er altså en gruppe af borgere, der styrer det med kontant."* (Bilag 11:linje 645-649)

Vi udleder, at nogle netværk har haft stor succes med at springe et led over og allerede ved det første møde, direkte på offerets bopæl, få udleveret kontanter. Gennem retsdokumenter har vi kunnet kortlægge omfanget af disse direkte kontantafhentninger, hvor pengene går direkte fra offerets hånd til svindlerne. Ud over betalingskort lykkedes det i 29 tilfælde gerningspersonerne også at få udleveret kontanter ved ofrenes adresse. Det svarer til, at der i cirka hver femte svindelsag indgår en kontantafhentning (Bilag 14b). De direkte kontantoverleveringer fylder således en relativt væsentlig del af den samlede gevinst. På baggrund af, hvad ofrene udsættes for, klassificerer vi denne adfærd som *predatory crime*. Det skyldes, at bankbudenes endelige mål er at redistribuere værdi via bedrag, på den mindst ressourcekrævende og komplicerede måde for dem selv.

Vi mener, at mængden af kontanter, afspejler en gennemgående praksis blandt ældre generationer, hvor det at have kontanter til rådighed skaber tryghed, giver visuelt overblik og gør det nemmere at håndtere økonomien. Ud af den samlede gruppe på 363 totale ofre, har vi ingen dokumentation for, at en person under 85 år har udleveret kontanter direkte til gerningspersonerne. Endvidere kan en vis usikkerhed eller manglende færdigheder inden for digitale løsninger resultere i, at de enten bevidst undgår at være afhængige af digitale tjenester eller ikke finder overskud til at tilegne sig nye teknologiske kompetencer.

Ofrenes daglige vaner og rutineaktiviteter påvirker både frekvensen og sandsynligheden for, at de bliver udsat for svindel (Cohen & Felson, 1979:589). Med frekvens og sandsynlighed refererer vi til, antallet af berørte ofre og hvor ofte det faktisk lykkes for bankbudene at gennemføre svindlen mod disse personer. Faste rutiner i hverdagen kan gøre nogle personer mere sårbare, hvilket øger chancen for, at de bliver kontaktet og narret af bankbude. Den rutinebaserede tilgang, hvor ældre benytter kontanter til at administrere deres økonomi, gør dem særligt sårbare, netop på grund af deres vaner. Vi finder, at kontantbeløbene der opbevares i de ældres hjem, sjældent er i den lave ende. Som højeste kontantafhentning, sker der en direkte fysisk overlevering på 270.000 kr. med netværk 1 i spidsen (Bilag 14b).

Ikke alene opbevarer mange ældre kontanter i hjemmet, de adskiller sig også ved i højere grad end yngre aldersgrupper ved at opholde sig hjemme i dagtimerne. Hvor størstedelen af befolkningen typisk er ude af huset beskæftiget med arbejde, uddannelse eller andre aktiviteter, er mange ældre oftere hjemme, hvilket øger risikoen for, at svindlere kan få adgang til dem direkte i deres eget hjem. Vi ved, at visse personer i offentlighedens øjne, kan anskues som værende oplagte ofre, når de bliver angrebet i en situation, der anses som legitim (Christie, 1986:18-19), specifikt som her, når ofrene opholder sig, i sit eget private hjem. Dette er endnu en udpræget hverdagsaktivitet blandt offergruppen, og vi ser i den forbindelse, hvordan denne metode tydeligt afslører svindlernes kynisme, for det er svært at forestille sig en mere grænseoverskridende udnyttelse, end en udnyttelse der foregår gennem indtrængen i menneskers privatsfære. Vi forstår, at bankbudene har indsigt i de ældres rutiner, hvorfor de har et stærkt incitament for at udnytte netop denne målgruppe som en *'nem vej til hurtige kontanter'.*

6.2.5 Neutralisering

De fysiske kontantafhentninger afspejler at svindlerne er kyniske og følelseskolde. I forlængelse heraf, ser vi hos svindlerne et behov for at retfærdiggøre denne målrettede udnyttelse af ofre, når de stilles til ansvar. Retsdokumentet fra Retten i Viborg, at en af gerningspersonerne under afhøringen forsøgte at fralægge sig ansvaret for hans gerninger. Dette gjorde han ved, i strid med sandheden, at hævde, at de ældre ofre ikke led et egentligt økonomisk tab, og at alvoren derfor kunne nedtones. I dokumentet fremgår beskrivelsen at: *"Han har fået oplyst, at de gamle mennesker ikke mistede penge, da staten betalte, og det troede han på."* (Bilag 20a:33-34). Vi tolker, at dette er et konkret og tydeligt eksempel på at anvende en neutraliseringsteknik. Neutraliseringsteknikker er en psykologisk taktik, som først blev beskrevet af

Matza og Sykes (1957), hvor personer foretager en ansvarsfralæggelser og forsøger at retfærdiggøre deres kriminelle aktiviteter, både for dem selv og andre.

Det, vi ser som gældende i dette tilfælde, er brugen af teknikken *fornægtelse af skade* (*denial of injury*) (Matza & Sykes, 1957:667). I udtalelser som disse, ser vi en erkendelse af selve handlingen, men at den forsøges at blive retfærdiggjort ved at minimere ansvar og skyld, idet gerningspersonen hævder, at der ikke er sket nogen reel skade. Formålet bliver dermed at eliminere at den alvor, der ligger i, at man har forvoldt offeret skade, på det personlige plan.

Vi ser også i mindre omfang tilstedeværelsen af en sekundær teknik, nemlig *fornægtelse af ansvar* (*denial of responsibility*) (Ibid). Denne teknik bygger på en forestilling om, at gerningspersonen handlede i god tro, fordi andre havde forklaret, at handlingen ikke ville få konsekvenser. Denne teknik fungerer som en understøttende strategi til den første og tjener til at flytte det personlige ansvar væk fra gerningspersonen og over på de 'omstændigheder', han handlede under.

Vi vurderer, at teknikkerne bliver et redskab for gerningspersonerne til at håndtere den moralske konflikt, der opstår, når de har accepteret, men handler imod samfundets grundlæggende normer. Det betyder, ikke at normerne helt forkastes, men at de ved et skyldsspørgsmål midlertidigt neutraliseres.

6.2.6 Skyld og skam

Et gennemgående tema er den retorik, der placerer ansvaret hos ofrene selv og fokuserer på deres formodede manglende dømmekraft som forklaring på, hvorfor de blev udsat for svindel. De ældre bliver ofte mødt med foragt og skuffelse, både fra deres nærmeste pårørende og fra offentligheden, hvorfor de ikke altid tør dele, det de har været udsat for. Vores data viser, at flere ofre oplever psykiske konsekvenser, herunder selvbebrejdelse og skyldfølelse. De føler sig krænket og manipuleret (Bilag 11-12). Vi ser, at dette særligt styrkes ved, at de har haft direkte kontakt til gerningspersonen, og har set dem i øjnene, som de valgte at stole på. En informant, der qua sit faglige virke, har hjulpet ofre fortæller:

> *"Det er jo et overgreb. [...] De er blevet svindlet i telefonen, de er hoppet på den, men de har faktisk også set det, de opfatter som gerningsmanden i øjnene. Det er jo et moderne bankrøveri. Vi ved jo, hvor hårdt det tog på nogle af dem der sad i kasserne i gamle dage, og nu står de ude ved den ældre. Det er ret indgribende.*

> *Pengene er én ting, men der er så meget skyld og skam i det. Det bliver ikke bedre, når sønnen siger, at mor, 'du hopper da ikke på den'. Det hjælper ikke noget, men det er bare det, vi tit hører, at det er den reaktion de bliver mødt med at omverden, altså: 'jeg troede du var klogere' "* (Bilag 11:linje 338-346).

Den ovenstående beretning fra banken illustrerer, hvor psykisk belastende og grænseoverskridende denne form for svindel er, idet man både rammes økonomisk og emotionelt. Det er væsentligt at understrege, at det ikke kun er sårbare, ældre eller godtroende, der kan blive ofre.

Når selv bankerne, som består af specialiserede fagfolk netop med særlig opmærksomhed på svindel, kan blive snydt gennem spoofing, hvor svindlere mundtligt manipulerer dem til at genåbne ofrenes spærrede konti, vidner det om, at en motiveret gerningsperson er en dygtig svindler, som kan opnå succes uafhængigt af offerets alder eller faglige position.

På den baggrund kan vi udlede, at det faktum, at en ældre kvinde er blevet udsat for svindel og har lidt et økonomisk tab, ikke nødvendigvis er ensbetydende med, at hun har handlet uansvarligt eller hensynsløst. Snarere ser vi, at SE-teknikkerne har en væsentlig gennemslagskraft, samtidigt med at systematikken og predatory-elementerne er afgørende. Særligt når disse mekanismer kommer til udtryk i de profitdrevne netværk. En anden bank supplerer:

> *"Det er ikke nogen skam at være blevet snydt. Man er blevet manipuleret, de siger de rigtige ting rent psykologisk til en, indtil man bliver fanget i det. De er bare hammergode, sprogligt"* (Bilag 12:linje 774-776).

Ofrene erkender ofte, i bagklogskabens lys, at de burde have forholdt sig mere kritisk og reflekterende. I vores data udleder vi tydelige eksempler på, hvordan det at være under et akut pres, såsom tidspres, kan påvirke ofre til at reagerer impulsivt og irrationelt, fordi de psykiske pres overtager deres normale dømmekraft. I sådan en situation gør disse triggere at ofrene handler i panik og træffer hurtige beslutninger. Beslutninger, som de med stor sandsynlighed ikke havde truffet i en mere rolig tilstand under kontrollerede omstændigheder. Vi ser, at processer som disse under en svindelakt, fra offereret perspektiv, gør at deres egne handlinger kolliderer med deres selvbillede som værende ansvarlige og fornuftige individer. Dette skaber kognitiv dissonans, som udmønter sig i skyld og skam og et *"jeg burde have vidst bedre"* tankemønster.

6.2.7 Sammenfatning - offerprofilen

Vores analyse af offerprofilen for BBB viser tydeligt en markant kønsmæssig skævhed. Ældre udgør en risikogruppe grundet deres daglige vaner og rutiner. Især kvinder i alderen omkring 81 år, har ofte kontanter fysisk til rådighed, hvorfor deres sårbarhed øges. Derudover opholder de sig i højere grad i hjemmet i dagtimerne, hvor svindlerne kan få direkte adgang til dem. Denne praksis understøttes af strategisk udnyttelse af ofrenes tryghed ved kontanter og deres ofte begrænsede digitale færdigheder.

Svindlerne systematiserer deres selektering af ofre, baseret på fornavne, som tilhører den ældre generation. Dette indikerer, at visse navne i sig selv kan fungere som indikatorer for udsathed. Denne strategi understøttes af brugen af både ulovligt indkøbte fullz og offentligt tilgængelige databaser, hvilket vidner om grundigt forarbejde og en profitoptimerende tilgang, hvor ingen kræfter spildes på uopnåelige ofre. Fremgangsmåderne bekræfter, at der er tale om kriminalitet med høj grad af planlægning og teknologisk understøttelse.

Det er væsentligt at understrege, at ofrene ikke nødvendigvis er godtroende eller hensynsløse. Tværtimod viser vores analyse, at selv bankmedarbejdere, som har ekspertise i at opdage svindel, kan blive narret gennem avancerede manipulationsmetoder. Dette indikerer, at netværkene er yderst dygtige manipulatorer, som kan omgå selv professionelle, hvorfor det er ukorrekt at placere ansvaret entydigt hos de ældre kvindelige ofre.

Gerningspersonernes brug af neutraliseringsteknikker, såsom fornægtelse af skade og ansvar, illustrerer deres forsøg på at retfærdiggøre deres kynisme, samtidig med at de håndterer den moralske konflikt ved at forflytte og minimere ansvar. Ofrene oplever psykiske konsekvenser, herunder skyld, skam og selvbebrejdelse, hvilket forstærkes af samfundets og pårørende negative reaktioner.

Samlet set peger analysen på, at svindlerne udnytter både de objektive forhold og psykologiske mekanismer hos ofre for at maksimere udbyttet, hvilket nødvendiggør forebyggende tiltag, som tager højde for både ældres adfærdsmønstre og svindlernes professionelle manipulationsmetoder.

6.3 Delanalyse 3 – Step-by-step guide til succesfuldt bankbudsbedrageri

6.3.1 Modustyper og fremgangsmåde

Gennem vores kodning af retsdokumenterne har vi identificeret en række manuskripter og modustyper, som gerningspersonerne anvender i forbindelse med BBB. Formålet med dette afsnit er ikke at foretage en udtømmende gennemgang af hver enkelt modus, men snarere at beskrive og sammenligne centrale mønstre i fremgangsmåderne. Ved at analysere, hvordan svindlen udføres, opnår vi en dybere forståelse af gerningspersonernes handlinger og rationaler. En sådan indsigt er afgørende, da den ikke blot bidrager til en kortlægning af fænomenet, men også styrker mulighederne for at udvikle målrettede og effektive forebyggelsesstrategier, hvilket vi belyser i diskussionen.

Vi fandt frem til ti manuskripter (Bilag 15:11-12), som anvendes af de kriminelle netværk. Manuskripterne er en række replikker, som svindleren anvender til at manipulere ofrene. Vores manuskripter består ikke af længere sammenhængende talestrømme, men udgøres derimod af korte sætninger, som gentagne gange optræder i de forskellige sager, som f.eks., ”*Dit kort er blevet misbrugt*” og ”*vi sender en medarbejder ud for at afhente kortet*”. Det betyder, at der ofte indgår manuskripter i forskellige konstellationer i samme sag, som aktiveres sekventielt i takt med, at samtalen skrider frem.

Vi identificerede ligeledes ti anvendte modus (Bilag 15:1-3). Forekomsten af disse kan aflæses af nedenstående tabel.

Tabel 6 - Hyppighed af anvendte modus (baseret på direkte ofre)

Modustype	**Antal gange anvendt modus**
Modus 1	1
Modus 2	2
Modus 3	1
Modus 4	3
Modus 5	2
Modus 6	123
Modus 7	1
Modus 8	1
Modus 9	16
Modus 10	18

Ovenstående tabel viser, at modus 6 anvendes i hele 73 pct. af tilfældene. *Modus 6* er karakteriseret ved, at gerningspersonen kontakter offeret telefonisk og udgiver sig for at være fra offerets bank. Gerningspersonen fortæller en falsk historie om, at der foregår mistænkelig aktivitet på vedkommendes konto, og under denne falske præmis overtales offeret til at udlevere kontanter, kort og pinkode til en person, som fysisk møder op på vedkommendes bopæl. Kortet anvendes derefter til at foretage kontanthævninger, hvilket medfører et økonomisk tab for offeret. Flere af de identificerede fremgangsmåder deler centrale elementer med modus 6. I det følgende foretager vi en systematisk sammenligning af de forskellige fremgangsmåder på tværs.

6.3.2 Det er "banken" der ringer

I ni ud af ti identificerede fremgangsmåder indledes bedrageriet med telefonisk kontakt, hvor gerningspersonerne, under dække af at repræsentere eksempelvis banken, politiet eller Nets, fremkalder en vildfarelse hos offeret. På baggrund af retsdokumenterne tyder det på, at det ikke hovedsageligt er de dømte bankbude, der foretager disse opkald, men snarere andre medgerningspersoner, såkaldte *'callere'*, som befinder sig enten i køretøjet de transporterer sig i eller på en ukendt lokalitet. Eftersom bankbudene ikke selv står for den første kontakt til offeret, vurderes deres rolle ikke at være central i svindelens indledende fase. Ikke desto mindre vurderer vi, at det er relevant at foretage en nærmere analyse af de fortællinger, som callerne anvender i deres kommunikation med ofrene, da disse udgør et centralt element i svindelens succes. Det er netop gennem denne fortælling, at gerningspersonerne formår at manipulere og opbygge den nødvendige tillid, som muliggør det videre bedrageri.

Dataene viser, at når den indledende fase af svindlen mislykkes, f.eks. ved at offeret gennemskuer gerningspersonens skumle agenda, falder det hele til jorden. I de tilfælde, hvor forsøget ikke er lykkedes, ses en markant lavere andel af callere, der udgiver sig for at være fra banken. Kun i 31 pct. af de 196 mislykkede forsøg påstår svindlerne, at opkaldet kommer fra banken, mens de i 69 pct. af tilfældene i stedet angiver at ringe fra Nets, Rigspolitiet eller Politiet. I hele 87 pct. af de 168 succesfulde bedragerier udgiver callerne sig for at være repræsentanter fra den forurettedes bank. Strategien er særligt effektiv, og anvendes derfor i langt størstedelen af de gennemførte bedragerier. En forklaring herpå kan være, at banker opfattes som autoriteter, fordi de forvalter befolkningens, og dermed også ofrenes formuer. I praksis betyder det, at

bankerne både har kontrol over og adgang til borgernes opsparinger og økonomiske forsørgelsesgrundlag. Med den magt følger også en autoritet, som bliver særlig tydelig når 'bankmanden' hævder, at privatpersoners penge er i fare grundet mistænkelig aktivitet på kontoen. Derfor ser vi, at de loyale ofre typisk responderer ved at følge de anvisninger de instrueres i.

Den gennemgående taktik i bedrageriforsøgene indebærer at svindlerne påtager sig en autoritativ identitet. Ved 50 pct. af de direkte ofre, fremgår det eksplicit, at callerne enten har fortalt, at der er tegn på mistænkelig aktivitet på ofrenes konto, der er hævet penge i udlandet, eller at nogen er i færd med at bryde ind på deres konto. Formålet at skabe en følelse af utryghed, forvirring og stress hos ofret, hvilket øger sandsynligheden for, at de accepterer callerens "hjælp" og anvisninger. Dette må ligeledes anses som en central del af svindelens manipulationsteknik, hvor følelsesmæssigt pres og afledning anvendes til at fremkalde tillid og samarbejdsvillighed.

I den eksisterende forskning omhandlende SE-teknikker, viste denne at særligt *autoritet*, *afledning* og *social bekræftelse* var de mest hyppigt anvendte manipulationsstrategier. Vores data bekræfter i høj grad at svindlerne anvender autoritet og afledning til at svindle ofrene. Ved alle direkte ofre anvender gerningspersonerne autoritet, og i 127 tilfælde, svarende til 75 pct., indgår begge elementer. Derimod ses strategien om *social bekræftelse*, ikke anvendt i det foreliggende datamateriale. Dette fravær kan indikere, at netop denne form for svindel, som vi undersøger, adskiller sig fra de digitale svindeltyper, som undersøges i Jones et al.'s studie. *Social bekræftelse* bygger på idéen om, at individer lader sig påvirke af, hvad de opfatter som konsensus eller norm i en gruppe. I denne svindel består interaktionen imidlertid ved en isoleret en-til-en-relation mellem offer og svindler. Der eksisterer således ikke et synligt 'fællesskab', offeret kan spejle sig i.

Ved 125 direkte ofre fremgår det, at gerningspersonerne oplyser, at en medarbejder vil blive sendt ud for at assistere, og afhente værdigenstande med det formål om at bringe dem i sikkerhed. I 115 tilfælde instrueres ofrene specifikt i at udlevere deres betalingskort for at forhindre yderligere misbrug. Det kan ikke udelukkes, at denne instruktion forekommer i flere sager, men blot ikke er blevet inddraget i retsdokumenterne. Sammenfattende virker gerningspersonerne både professionelle og hjælpsomme i røret, samtidig med at de intimiderer ofrene.

6.3.3 Længden på samtale

Der foreligger begrænset information om varigheden af de telefoniske samtaler mellem callerne og de forurettede. I enkelte tilfælde er ofret 'hoppet i fælden' efter få minutter (Bilag 19). I flere tilfælde beskrives dog længerevarende samtaler, hvor kommunikationen har varet flere timer (Bilag 10; 12; 19). Informanten fra politiets EAE-afdeling fortæller:

> *"Nogle forurettede har gerningspersonerne jo siddet og bearbejdet i op til 6 timer. I mange, mange timer har de siddet og bearbejdet dem. Holder dem fast. Det gælder for dem alle sammen. Du må ikke lægge på, fordi det gælder om, at du ikke bliver ringet op af din familie eller banken eller pårørende"* (Bilag 10: linje 541-544).

Informanten fremhæver samtalernes længde som et centralt element i svindlernes strategi for at fastholde kontrollen over ofrene. Ligeledes fortæller informanten fra Sydbank, at *"... 2 timer er ret langt tid, og man kan virkelig blive manipuleret og 'rundforvirret', ikke? [...] Og så er det typisk at den der har hentet kortet, når i automaten inden de lægger på hos ofre"* (Bilag 12: linje 182-183). På baggrund af informanternes udsagn tyder meget på, at jo længere tid svindlerne formår at holde ofrene i røret, desto mere tilbøjelige bliver ofrene til at acceptere fortællingen, og i sidste ende falde i 'svindel-fælden'. Når ofre manipuleres og presses af professionelle svindlere over længere tid, er det ikke overraskende, at det kan ende med sådan et resultat. Samtalernes varighed er således ikke tilfældig. Tværtimod fremstår den som en bevidst strategi, der i væsentlig grad bidrager til bedrageriets succes.

6.3.4 Dine værdier er i "trygge hænder"

For 196 personer stopper svindlen efter den indledende kontakt, men for 168 personer fortsætter denne *'rovdyrs-kriminalitet'*, og gerningspersonerne går i gang med næste fase af svindlen. I denne del kommer bankbudene ind i billedet. De skal ud på ofrenes adresser og afhente værdier, i form af betalingskort, smykker og kontanter. I ni ud af de ti identificerede modustyper møder bankbuddet op på adressen, og i tre sager (modus 4) foregår kontakten uden direkte fysisk kontakt, men udelukkende via opkald og bankoverførsler direkte til gerningspersonens konto.

Herudover ses det i flere netværk, at gerningspersonerne bevidst forsøger at få ofrene til selv at foretage bankoverførsler frem for at tilegne sig deres fysiske betalingskort. Denne fremgangsmåde kan potentielt generere en højere økonomisk gevinst, idet netbanks-transaktioner ikke er underlagt de samme beløbsgrænser som kontanthævninger, og samtidig reduceres risikoen for identifikation, da gerningspersonerne undgår videoovervågning ved hæveautomaterne. Særligt Netværk 1 gør systematisk brug af metoden med overførsler, og har en gennemsnitlig indtjening pr. offer på 150.000 kr., hvilket er markant højere end det gennemsnitlige tab i de øvrige netværk. Imidlertid er fremgangsmåden ikke problemfri. Bankoverførsler efterlader et digitalt spor, som kan følges af efterforskere, og der er derfor en øget sandsynlighed for, at transaktionerne kan tilbageføres eller stoppes. Det samme gør sig ikke gældende ved kontanter, da disse udbetales med det samme.

Set ud fra RCT er denne fremgangsmåde et udtryk for gerningspersonernes bevidste afvejning mellem opdagelsesrisiko og den potentielle økonomiske gevinst. Denne strategiske tilpasning af fremgangsmåden fremstår som særligt attraktiv i et kortsigtet perspektiv, idet den muliggør høje transaktionsbeløb og hurtig økonomisk gevinst med en umiddelbar lav opdagelsesrisiko. Dog viser praksis, at de langsigtede konsekvenser ikke nødvendigvis følger samme logik. Konkret i Netværk 1 blev gerningspersonen anholdt efter blot ni gennemførte bedragerier. Dette indikerer, at den reelle opdagelsesrisiko kan være væsentligt højere end gerningspersonen har kalkuleret.

I de resterende modustyper, udleverer ofrene deres værdier til bankbuddet. Denne direkte kontakt øger umiddelbart risikoen for identifikation, idet ofrene har mulighed for at beskrive bankbudenes udseende. Samtidig udsætter gerningspersonerne sig selv for risikoen for at blive videoovervåget, når de efterfølgende anvender kortene ved hæveautomater. Det fysiske møde mellem offer og gerningsperson udgør således ikke blot en opdagelsesrisiko i sig selv, men fungerer også som overgang til svindlens næste fase, nemlig det systematiske misbrug af de udleverede betalingskort.

6.3.5 Nu skal der tjenes 'lapper'

Ved fem ud af de ti typer af modus (modus 2, 3, 6, 9,10) har bankbuddet fået udleveret ofrenes betalingskort og pinkode, for derefter at tage direkte ud til enten hæveautomater, tankstationer eller forretninger. Herefter begynder næste fase af bankbudsbedrageriet, selve misbruget af

kortet, hvor der skal handle hurtigt og effektivt, for at få størst mulig indtjening. Blandt hæveautomater, forretninger og tankstationer, viser dataene, at svindlerne hyppigst anvender og opnår størst økonomisk udbytte ved brug af hæveautomaterne. Derfor retter vi hovedfokus mod brugen af disse samt svindlernes hævningsmønstre. Indledningsvis kommenterer vi dog kort på svindlernes forbrugsmønstre i forretninger og på tankstationer.

Når svindlerne anvender de stjålne kort i forretninger, viser dataene, at det især er iPhones, der bliver købt (Bilag 14b). Vi postulerer, at svindlerne målrettet går efter telefoner, da disse hurtigt kan omsættes til kontanter ved videresalg, hvormed dette er en effektiv måde at tjene hurtige penge på.

Når svindlerne anvender de stjålne kort på tankstationer, ved vi med sikkerhed ud fra retsdokumenterne, at noget af det de køber er kartoner af cigaretter (Bilag 14b). Det er uklart, om de købte varer primært er til eget forbrug, videresalg eller andre kriminelle formål, da dataene ikke giver indsigt i dette. Derfor vil vi ikke gå yderligere i dybden med dette aspekt. Vi formoder desuden, at der også foretages køb af benzin, hvilket sandsynligvis sker for at sikre, at de forsat kan komme fra 'a til b' under svindlen.

Som nævnt tidligere, anvender svindlerne hyppigst hæveautomater. Så snart de er kommet i besiddelse af både kort og pinkode, bevæger de sig hurtigst muligt mod en hæveautomat, ofte en, der tilhører det pengeinstitut, kortet er udstedt af, med det formål at hæve så store beløb som muligt. Målet er at maksimere det økonomiske udbytte, før ofret bliver opmærksom på svindlen, og når at få kortet spærret. Tid er således en kritisk faktor for gerningsperson i denne fase, hvor vi ser en effektiv og målrettet udnyttelse af det korte vindue, hvor kortet stadig er aktivt.

Når bankbudene er kommet frem til hæveautomaterne, er de nået til tidspunktet i processen, hvor de skal hæve penge, og hertil tegner der sig et klart hævningsmønster. En række konkrete beløb går systematisk igen ved alle netværkenes hævningsaktiviteter. Beløbene på henholdsvis 2.000 kr., 6000 kr., 10.000 kr., 14.804 kr.[4] og 15.000 kr., er de fem hyppigst forekomne, samtidigt ser vi en kobling mellem specifikke beløb og banken hvori hævningerne foretages.

[4] Beløbet på de 14.000 veksler mellem 14.804 kr., 14.806 kr. og 14.804 kr. Vi formoder, at de 'skæve' beløb skyldes, at der foretages hævninger i euro-valuta. Vi ser mindre udsving på et par kroner som stammer fra den vekslende valutakurs på euroen.

At gerningspersonerne oftest hæver disse beløb, indikerer at de har en bevidsthed om kontanthævningsgrænser hos forskellige pengeinstitutter, de såkaldte *limits* (Bilag 11-13). Limits refererer til de beløbsgrænser, der er fastsat for, hvor meget en kunde kan hæve kontant i en hæveautomat inden for et givent tidsrum. Disse grænser varierer afhængigt af en række faktorer, herunder korttypen, den pågældende bankinstitution samt eventuelle individuelle aftaler mellem kunden og bankrådgiveren. F.eks. kan en kunde i SparNord, som har et VISA eller Mastercard, hæve 15.000 kr. i kontanter i samtlige automater uanset hvilken bank de tilhører (Bilag 11:linje 610-611). I modsætning hertil, kan en kunde med et betalingskort udstedt af Sydbank hæve 10.000 kr. i en Sydbank automat, og mere konservativt blot hæve 2.000 kr. i eksterne hæveautomater (Bilag 12:linje 636-637).
I vores data optræder 55 tilfælde af kontanthævninger på mellem 14.000 og 15.000 kr. Der optræder tilmed 93 kontanthævninger af beløbet 2.000 kr. Sidstnævnte beløb synes at være en slags "bundgrænse" for, hvad svindlerne med sikkerhed kan opnå, da ingen banker, så vidt vides, har lavere limits end det. Denne grænse udgør derfor en slags kalkuleret minimumsgevinst, som bankbudene kan forvente, forudsat at der er dækning på kortet. Dette afspejler igen den rationelle vurdering af risiko og udbytte, der præger svindlens fremgangsmåde.

En korrespondance mellem bankbud og bagmand, viser en klar bevidsthed om limits': "*Du skal først til den nærmeste Danske bank automat og hæve det maksimale du kan, ville tro det er 6000 kr. Efterfølgende tager du til en ny hæveautomat som ikke er Danske bank hvor du hæver 2000 kr."* (Bilag 19:34). Gerningspersonernes viden om limits synes at gå langt ud over almindelig forbrugerbevidsthed og fremstår i stedet som en vigtig del af den kriminelle strategi. I nogle af retsdokumenterne fremgår det, at svindlernes interne kommunikation indeholder direkte instruktioner til bankbudene, om hvor store beløb de må hæve, for ikke at overskride disse grænser. På Snapchat ses bl.a. følgende korrespondance mellem et bankbud og en anden person i netværket, som har en mere koordinerende rolle:

> *"Husk bror du skal hæve 15 lapper fra begge kort i SparNord bank hæveautomat, og to lapper fra en anden bank"* (Bilag 19:50).

Korrespondancen om fremgangsmåden ved hævningerne fortsættes senere ved et andet offer:

> *Du skal tage til nærmeste KONTANTEN hæveautomat og hæve i de to Sparekassen Kronjylland. Der kan du hæve 15.000 hver, og så til Arbejdernes Landsbank og hæve 10.000"* (Bilag 19:32).

Ovenstående citater viser tydeligt, at netværkene udviser en høj grad af bevidsthed og strategiske i deres overvejelser om, hvordan de bedst muligt kan operere for hurtigt at maksimere deres profit.

Der er nogle banker, som anvendes hyppigere end andre. Der foretages samlet set 27 hævninger á 6.000 kr., hvoraf de stort set alle foretages i Danske Banks hæveautomater. Koblingen mellem specifikke beløb og den bank hvori kontanthævningerne foretages, indikerer at det typiske mønster, som vi gennemgående ser ved bankbudene er, at der hæves 2.000 kr. i Sydbanks automater, at der hæves 6.000 kr. i Danske Banks automat og at der hæves mellem 14.000 og 15.000 kr., i SparNord og Nordeas hæveautomater. Dette mønster påviser, at gerningspersonerne ikke foretager tilfældige og impulsive hævninger, men at der snarere er tale om, at de forinden grundigt har orienteret sig i bankernes procedurer. Det tydeliggør at netværkene er både velovervejet og strategiske i deres hævninger. Frekvensen af hævninger fordelt på bankerne, fremgår af nedenstående tabel:

Tabel 7 – hævninger ved konkrete banker

Bank eller hæveautomat	**Hyppighed**
Ukendt hæveautomat[5]	103 hævninger
Nordea	48 hævninger
Danske Bank	46 hævninger
KONTANTEN ATM	36 hævninger
Jyske Bank	15 hævninger

[5] De 103 hævninger foretaget i de 'ikke-oplyste' hæveautomater er primært kendetegnet ved høje beløb i intervallet 10.000–15.000 kr. På den baggrund formoder vi, at disse ukendte automater tilhører banker med høje beløbsgrænser.

Sydbank	13 hævninger
Djursland Bank	7 hævninger
Arbejdernes Landsbank	6 hævninger
SparNord	2 hævninger
Nordjyske Bank	2 hævninger
Vestjysk Bank	1 hævning
Handelsbanken	1 hævning

Der ses markante forskelle i praksis mellem bankerne, både hvad angår svindlernes hævemønstre ved de forskellige bankers hæveautomater og bankernes egne fastsættelser af limits. Limits fremstår som et omdiskuteret emne blandt de medvirkende informanter, hvor særligt eksperterne fra bankerne udtrykker bevidsthed om, at høje beløbsgrænser kan skabe incitament for økonomisk motiveret kriminalitet. Netop høje limits kan gøre det mere attraktivt for gerningspersoner at give sig i kast med at være bankbud, idet de potentielle gevinster kan opveje risikoen for straf. Samtidig italesætter bankerne, at de navigerer i en hårfin balance mellem sikkerhedsforanstaltninger på den ene side, og brugervenlighed for deres kunder for den anden side. Denne balancegang kan utilsigtet skabe sårbarheder, der systematisk kan udnyttes af svindelnetværkene. Problematikken vil blive behandlet i diskussionen (jf. afsnit 7.2).

6.3.6 Svindel i højt tempo

Nu hvor vi har klarlagt, at gerningspersonerne har indsigt i, hvor meget de kan hæve i de forskellige banker, og at de agerer strategisk ud fra denne viden, retter vi nu opmærksomheden mod deres tempo i gennemførelsen af hævningerne og geografiske mobilitet. Ønsket om at maksimere udbyttet på kortest muligst tid gør det relevant at klarlægge, hvorhenne, og hvor

hurtigt de opererer, når kort og pinkode først er i deres varetægt. Ved kortlægningen af netværkenes hævningsmønstre har vi kunnet identificere præcise placeringer og klokkeslæt for, hvornår aktiviteterne finder sted. Det giver os indsigt i, hvor hurtigt svindlerne bevæger sig, hvor lang tid de enkelte trin i forløbet tager, og hvor aktive bankbudene formår at være inden for blot én time eller en enkelt dag. Samtidig ser vi, hvordan deres aktivitet afspejler sig i størrelsen af deres udbytte.

I mange tilfælde er reaktionstiden ekstremt kort fra det øjeblik, hvor bankbuddet får udleveret kortet, til at det anvendes ved en hæveautomat. I nogle tilfælde drejer det sig blot om et par minutter, før det økonomiske udbytte er i deres besiddelse. Et udklip af et netværks hændelsesforløb ses i nedenstående figur.

Figur 3 - Aktivitetsmønster (Bilag 14b)

D. 21. APRIL 2023			
KL. 11:30	**OFFER 166**	RINGER TIL OFFER, MØDER PÅ ADRESSE, AFHENTER KORT	HERNING
KL. 11:30	**OFFER 166**	AFHENTER SMYKKER FOR EN VÆRDI AF 9.875 KR.	HERNING
KL. 11:30	**OFFER 166**	AFHENTER 10.000 KR. KONTANT	HERNING
KL. 12:01	**OFFER 166**	HÆVER 15.000 KR. UKENDT AUTOMAT	-
KL. 12:04	**OFFER 166**	HÆVER 2.000 KR. UKENDT AUTOMAT	-
KL. 13:20	**OFFER 167**	RINGER TIL OFFER, MØDER PÅ ADRESSE, AFHENTER KORT	HERNING
KL. 13:30	**X OFFER 168**	MISLYKKEDES SVINDELFORSØG	HERNING
KL. 13:43	**OFFER 167**	HÆVER 10.000 KR. UKENDT AUTOMAT	-
KL. 13:56	**OFFER 167**	HÆVER 2.000 KR. UKENDT AUTOMAT	-
KL. 15:37	**OFFER 167**	KØBER IPHONE FOR 6.609 KR. I FØTEX	IKAST
KL. 17:00	**OFFER 169**	RINGER TIL OFFER, MØDER PÅ ADRESSE, AFHENTER KORT	HOLSTEBRO
KL. 17:38	**OFFER 169**	HÆVER 15.000 KR. UKENDT AUTOMAT	-

Ved denne dags aktivitet åbner svindlernes 'kontor' kl. 11.30, hvilket er et tidspunkt, der falder inden for bankens almindelige åbningstider. Allerede i løbet af de første 34 minutter af deres "arbejdsdag" har svindlerne haft kontakt med *offer 166*, afhentet værdigenstande, foretaget kontanthævninger og dermed opnået en økonomisk gevinst på 36.875 kr. Fremgangsmåden vidner om en høj grad af målrettethed, for blot en time senere er de allerede i færd med at svindle *offer 167.* Her går der kun 23 minutter fra første kontakt, til de første 10.000 kr. har forladt offerets konto, og indenfor de næste par timer har offeret mistet yderligere 9.000 kr. Parallelt hermed forsøger gerningspersonerne at svindle *offer 168,* hvilket mislykkes. Det forhindrer dem dog ikke i at fortsætte bedrageriet, og inden dagen er omme, har de franarret *offer*

169 for 15.000 kr. Kl. 17.38 markerer afslutningen på svindlernes aktiviteter for dagen, sideløbende med, at de fleste banker også lukker. Dette tidsmæssige sammenfald antyder, at svindlen i nogen grad følger en struktureret og arbejdsdagslignende rytme, hvilket kan være et forsøg på at få svindlen til at virke så troværdig som mulig. Dette vidner om en velovervejet tilrettelæggelse af svindlen. På trods af, at dette eksempel blot repræsenterer et enkelt udsnit fra en tilfældigt udvalgt dag, indikerer de observerede aktiviteter en tydelig og gentagende tendens i gerningspersonernes fremgangsmåde.

6.3.7 Den geografiske mobilitet

Dataene indikerer at der ligger strategiske overvejelser bag udvælgelsen af ofre i forhold til deres geografiske placering. Som det fremgår af figur 3, er samtlige fem ofre for svindlen på denne dag bosat i Midt- og Vestjylland. Dette vidner om en geografisk målretning, hvor ofre udvælges inden for et afgrænset område. En sådan fremgangsmåde kan tolkes som en strategisk optimering af deres kriminalitetsudøvelse, hvor målet er ramme flere ofre indenfor en kortere periode, for at maksimere udbyttet inden for kortest mulig tid og afstand. Dette peger på en opportunistisk kriminalitet, hvor valget af ofre i højere grad er styret af logistiske hensyn end af f.eks. formodninger om stor økonomisk gevinst eller personlig agenda. De logiske hensyn udelukker dog ikke, at netværkene udviser en høj grad af mobilitet, og kan bevæge sig nye steder hen, ved f.eks. at operere i Herning én dag og i Nørresundby den næste (Bilag 14b). I forlængelse heraf understreges det, at svindlen er rationelt organiseret og drevet af et ønske om profitmaksimering, hvor gerningspersonerne flytter sig efter pengene. Endvidere understøtter denne form for fleksibel og opportunistisk mobilitet, billedet af en velorganiseret svindelpraksis, hvor logistiske og tidsmæssige faktorer indgår som centrale elementer i svindelstrategien.

Med afsæt i ovenstående, finder vi det relevant at undersøge, hvorvidt BBB primært er koncentreret i specifikke geografiske områder, eller om der snarere er tale om et landsdækkende fænomen, der ikke er begrænset af lokale forhold. De syv retssager i datamaterialet er fordelt på domstole i hele landet. Dette indikerer umiddelbart, at BBB ikke er et lokalt afgrænset fænomen, men snarere en kriminalitetsform, der forekommer nationalt. Dog viser dataene, at 51 pct. af de direkte ofre, hvor vi kender til deres geografiske placering, er forankret i Midtjylland (Bilag 25). Dette indikerer at der må være et særligt geografisk hotspot for BBB i denne landsdel.

Ved en nærmere analyse af de 76 ofre fra Midtjylland, ser vi, at nogle byer er mere udsatte for BBB end andre. Især Herning adskiller sig som den by med flest registrerede tilfælde, idet 16 pct. af ofrene i Midtjylland er bosat her (Bilag 25). De resterende 64 ofre er fordelt på 32 forskellige byer, hvilket indikerer, at mens Herning udgør et særlig hotspot, forekommer kriminaliteten også spredt over et større geografisk område i landsdelen.

6.3.8 Hierarki og gruppedynamik – hver mand for sig selv

Bankbudene pålægger ikke alene deres ofre et tidspres, men udsættes tillige selv for et internt pres, der udøves af aktører højere oppe i netværkets hierarki. Dette pres manifesterer sig i krav om hurtighed og effektivitet i forbindelse med gennemførelse af hævninger. Hertil fortæller informanten fra Politiet:

> *"de [red: bagmændene] skynder på de der bankbude. De siger "se så for helvede at komme afsted. Nu har vi ventet et kvarter. Kom afsted. Hvornår er du der?" Når vi anholder bankbuddet, så får vi jo deres telefoner og kan se de beskeder de har fået. De lyder sådan "Hvornår er du fremme? Idiot. Det var Nørregade 1". Så de er meget aggressive når de kommunikerer med hinanden"* (Bilag 10:linje 544-548).

Denne interne kommunikation som ovenstående citat, og de efterfølgende citater viser, giver indsigt i, at der en klar hierarkisk struktur i netværket, hvor bagmændene udøver betydeligt pres på de udførende gerningspersoner, bankbudene. Denne organisering bærer præg af en kommandostruktur, hvor de øvre led i hierarkiet både instruerer, uddelegerer, overvåger og kontrollerer de lavere rangerede aktører for at sikre, at svindlen gennemføres så hurtigt og effektivt som muligt. Bankbudene har dermed en operativ rolle med lav grad af autonomi og handler som udgangspunkt under tidspres og ved at parerer ordrer.

Udtryk som "*idiot*" og ordrer som "*kom så for helvede afsted*" afslører en aggressiv og truende kommunikationsform, som ikke blot afspejler en effektiviseringslogik, men også peger på en intern kultur præget af trusler, dominans og kontrol. Ligeledes fremstår det tydeligt i dataene, at netværkenes interne dynamikker og dagsordener præges af en udtalt mistillid mellem aktørerne. De stoler ikke på hinanden og agerer i høj grad ud fra en indbyrdes skepsis. Det bygger vi på, at vi har dokumentation for, hvordan medlemmerne i netværket indbyrdes stiller høje

krav til, at de skal kunne dokumentere deres handlinger overfor hinanden. Det fremgår eksempelvis af Netværk 5's vidneforklaringer, hvor det beskrives at:

> "*Når han hævede penge, facetimede han med [red: gerningsperson], og det gjorde han også med de andre. Det var også for hans egen sikkerhed, så de kunne se, hvad der blev hævet og de ikke snød hinanden. Han kendte (gerningsperson), men de facetimede, så de ikke blev uvenner over det."* (Bilag 20a:45)

Selvsamme mangel på tillid og det tilhørende behov for intern dokumentation og kontrol afspejler sig også i politiets udsagn, hvor det fortælles:

> "*400.000 kr. står gerningspersonen og filmer til bagmændene. […] Alle bankbudene skal tænde for deres telefon, sådan at bagmændene, der sidder på callcenteret, kan følge med i, hvad ofret siger. […] Fordi ellers så, […] kunne de jo godt finde på at sige, der var ingen smykker, og der var ingen penge. Der var kun hævekortet, og så bare stikke de 400.000 kr. i lommen. Så de optager hele samtalen med den gamle. Og når de så kører ned til hæveautomaten, så skal de stå og filme hæveautomaten, fordi dem, der sidder på callcenter, skal se om der står 15.000. Fordi ellers så kan de jo bare hæve 15.000 og sige, der stod kun 1.500 kr."* (Bilag 10:linje 306-315).

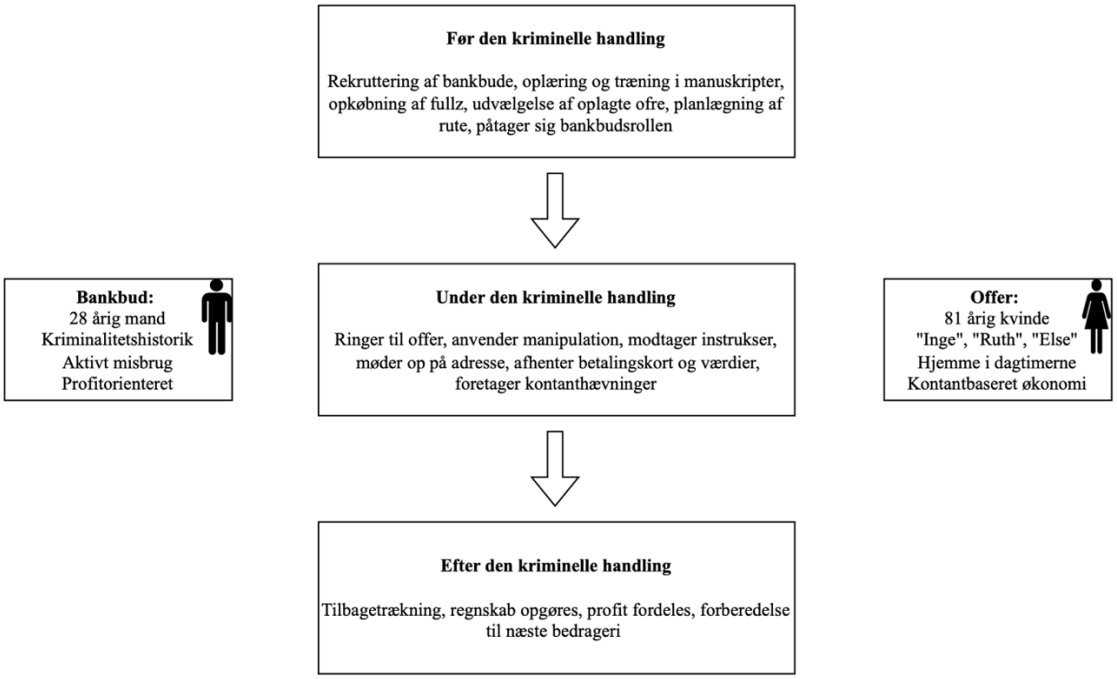
I forlængelse heraf, betragter vi, at denne udprægede mistillid udgør et specielt karakteristika, hvad angår gruppedynamikkerne i kriminelle netværk, som netop vores. Det skyldes, at strukturen og agendaen i samarbejdet adskiller sig markant fra andre former for organiseret kriminalitet, da kriminelle netværk sædvanligt har mere tungtvejende elementer af loyalitet og "broderskab" som grundlag for den hierarkiske opbygning. Manglen herpå belyser, at fællesskabet ikke tager afsæt i faktorer såsom loyalitet, men snarere at fællesskabet stort set består i at bruge hinanden til økonomisk vinding. Gerningspersonerne arbejder altså sammen, om at opnå det samme mål, og de har kompetencer og ressourcer, der kan gavne dette mål.

Ikke alene er medlemmerne underlagt intern kontrol, men de er også konstant i forhandling om deres individuelle procentmæssig andel i udbyttet (Tjek det, 2025). Her ved vi, at de personer, fysisk eksponerer sig selv, og således bærer en højere risiko for at blive straffet, langt fra er dem, der går derfra med den højeste gevinst. Vi vurderer, som tidligere nævnt, at dette i realiteten afspejler, at bankbude ofte udgør det svageste led i netværket.

Denne svage gruppetilknytning kommer konkret til udtryk i, at svindlerne ikke lader sig påvirke det fjerneste af, at deres med-gerningspersoner bliver opdaget eller anholdt, og således ryger ud af fællesskabet. I vores retsdokument fremgår det, at et bankbud bliver anholdt i forbindelse med svindlen, hvorefter de øvrige aktører fortsætter deres svindelnummer, som om intet var hændt. Dagen efter, er dette medlem erstattet af et nyt (Bilag 22:40). Netværkenes medlemmer er således i vidt omfang udskiftelige. På baggrund heraf, definerer vi denne tendens, ved at begrebsliggøre BBB som en *svingdørskriminalitet.* Denne udskiftelighed og manglende interne interesse for den, vidner om, at disse netværk er fællesskab præget af svage tilhørsforhold, hvor den enkelte primært kæmper for egne interesser. Dette indikerer for os, at de mennesker der indgår i specifikt netværk af BBB, er mennesker der enten befinder sig i en form for krise, eller er præget af en form for desperation, formentligt grundet pengemangel. Mange af de involverede aktører må formodes at være belastet af enten narkogæld eller ubetalte bøder til mere magtfulde, og ofte usynlige, bagmænd. Vi har tidligere postuleret at bankbudene er kyniske, men det tyder på, at alternativet er værre for dem, hvis de ikke er. De vil altså hellere snyde "Inge", som alligevel ikke "mister penge" end at stå i gæld til de "grimme og farlige" bagmænd.

6.4 Crime script – visualisering af bankbudsbedrageri

Med afsæt i vores kortlægning af bankbudsbedrageriers operationelle fremgangsmåde, præsenteres i det følgende et crime script, der systematisk visualiserer de centrale trin i svindlen – *før, under* og *efter* den kriminelle handling. Trinene indgår som en cirkulær proces, hvor afslutningen på ét bedrageri danner grundlag for planlægningen af det næste.



7. Diskussion

I denne del af specialet diskuteres det, hvordan BBB bedst kan forebygges med afsæt i vores kortlægning af fænomenet. Vi tager udgangspunkt i den situationsbestemte kriminalitetsforebyggelsesmodel, som har til formål at reducere mulighederne for kriminalitet ved at gøre det mindre rationelt og mere besværligt at gennemføre en given kriminel handling (Bjørgo, 2016:12). Vi ønsker således at diskutere, hvordan man konkret kan gøre BBB mindre attraktivt, og mere besværligt for svindleren på flere niveauer.

Vi tager afsæt i de tre overordnede faser fra vores crime script, og anvender disse som strukturerende ramme for diskussionen.

7.1 Før - Forebyggelse forinden skaden sker

I denne del af diskussionen rettes fokus mod 'før'-fasen, hvor vi undersøger, hvordan sårbare personer kan gøres mere resiliente overfor BBB. Derudover diskuteres det, i hvilket omfang en forebyggende indsats rettet mod denne fase kan have præventiv effekt.

Vores data har indikeret, at én af metoderne til udvælgelse af ofre sker via hjemmesiden 'Krak.dk'. En mulig situationel forebyggelsesstrategi kunne være at indføre adgangsbegrænsninger, f.eks. gennem profilordninger koblet til brugernes CPR-nummer, så dem der foretager søgningerne, sætter et digitalt aftryk. Et sådan tiltag vil øge mulighed for at spore gerningspersonerne, samtidig med at anonymiteten reduceres. Dette kan potentielt gøre det mindre attraktivt at anvende platformen som redskab til at identificere ofre. Dog er det klarlagt, at svindlerne er tilpasningsdygtige, hvilket betyder, at de sandsynligvis vil kunne omgå nye barrierer eller blot skifte til alternative platforme, hvor tilsvarende information kan være tilgængelig. På baggrund heraf, vurderes det, at det mest effektive sted at sætte ind med forebyggelse, kan være hos de potentielle ofre snarere end hos gerningspersonerne. Dette skyldes, at ofrene, om end ufrivilligt og ubevidst, i praksis medvirker til, at svindlen lykkes, idet de selv overdrager værdier og informationer til gerningspersonerne. Øget oplysning om BBB kan potentielt styrke ofrenes modstandskraft og mindske deres sårbarhed over for manipulation. Selvom det fortsat er relevant at opstille barrierer for gerningspersonerne, peger dataene som nævnt på, at de er særdeles tilpasningsdygtige og hurtigt formår at omgå forhindringer. På den baggrund må sådanne barrierer primært anses for at have en forsinkende snarere end varig effekt på gerningspersonernes færden. I modsætning hertil fremstår oplysningskampagner, der sigter mod at øge befolkningens bevidsthed om digital svindel, som et mere langsigtet forebyggelsesredskab.

Flere banker informerer allerede deres kunder om digital svindel, samt at de aldrig vil kontakte dem telefonisk og anmode om personfølsomme oplysninger, hvilket må anses som et skridt i den rigtige retning. Endvidere har Finans Danmark nedsat en *Svindel Task Force*, vis opgave er at finde løsninger, der kan bremse digital svindel (Finans Danmark, 2024). Her indgår 'oplysning om svindel' som et vigtigt element i forebyggelsen af digital svindel. Dette kan altså indikere at oplysning som forebyggelsesstrategi, kan øge befolkningens modstandsdygtighed over for svindelrelaterede trusler.

På trods af de igangsatte informationskampagner er det nødvendigt at forholde sig kritisk til, hvorvidt budskaberne i tilstrækkelig grad når ud til de rigtige målgrupper, da antallet af anmeldelser af digital svindel fortsat stiger. Dette peger på, at oplysningsstrategien bør revurderes og målrettes mere specifikt mod ældre aldersgrupper, som muligvis har en begrænset digital tilstedeværelse. Det er derfor afgørende, at relevante aktører som f.eks. banker og politi anvender mere traditionelle og tilgængelige informationskanaler som tekst-tv, aviser og lignende til at formidle *klare* og *simple* råd om, hvordan man kan beskytte sig mod digital svindel, og hvordan man bør reagere, hvis man kommer i 'klørene' på en svindler. Det er dog væsentligt ikke at overinformere, således at disse råd ikke bliver for omfattende eller komplicerede, da det kan føre til at modtageren bliver for 'mættet' af information, og derfor ikke forholder sig til dem. Endvidere bør fokus ikke udelukkende kun være på at oplyse og forebygge ved de ældre selv, men også ved deres nærmeste familie. De kan fungere som en vigtig støtte ved at informere og vejlede de ældre i, hvordan de håndterer potentielle svindelsituationer. Samtidig skaber denne støtte et trygt rum, hvor de ældre kan tale åbent om eventuelle oplevelser med svindel, hvilket kan bidrage til at reducere den skyld og skam, som ofte er forbundet med BBB. Denne sociale støtte kan dermed ikke blot forebygge svindel, men også hjælpe med at bryde tabuet omkring det at blive offer.

Med denne oplysningsbaserede tilgang, og med afsæt i situationel forebyggelse, kan der skabes bedre forudsætninger for at reducere mulighederne for at begå BBB. Dette opnås ved at mindske antallet af potentielle ofre gennem øget opmærksomhed på svindel og styrket modstandsdygtighed blandt de mest sårbare befolkningsgrupper.

7.2 Under - brugervenlighed vs. sikkerhedsforanstaltninger

I dialogen med bankerne er beløbsgrænserne, de såkaldte *limits,* et omdiskuteret emne. Dette åbner for forskellige perspektiver for, hvordan bankerne differentierer sig mellem hinanden

samt de følgevirkninger limits har for økonomisk kriminalitet og svindlernes muligheder – både i forhold til hvad der frister potentielle svindlere, og tilsvarende hvad der afholder dem. Bankerne bekræfter, at deres limits varierer væsentligt og en informant giver udtryk for, at det er et generelt opgør, som de vil komme til at tage i hele sektoren (Bilag 11, linje 622-623). Dog har bankerne til ansvar at indfri kundernes behov for kontanter, som til vores overraskelse, aldrig har været så stort, som det er netop nu (Bilag 11, linje 624-625).

Fra et forebyggende perspektiv kan vi, på den ene side, stille spørgsmålstegn, til hvorvidt det simple tiltag med at nedsætte beløbsgrænserne, ville have en præventiv effekt på BBB. En tese er, at den reducerede udsigt til profit vil have en afskrækkende effekt, her med afsæt i, at vi har konkretiseret hvor velovervejet aktiviteten hos gerningspersonerne er, når det kommer til profitmaksimering. I samme ombæring, er BBB på den anden side, et unikt fænomen der blot har været en aktuel problemstilling de seneste 2 – 3 år i Danmark (Bilag 10). Derfor, kan der også herske tvivl om, hvorledes svindlerne blot tilpasser sig og opfinder nyere metoder med nyt modus. Dette lægger sig i tråd med, at vi i øvrige har identificeret at agendaen i at *'snyde gamle mennesker for deres penge'* har eksisteret siden tidernes morgen. Bankerne oplever en løbende opblomstring af nye svindelfænomener, hvilket tyder på, at den motiverede svindler kontinuerligt vil videreudvikle svindeltaktikker med henblik på at narre penge fra deres ofre. Helt aktuelt, er der en tendens i svindel med *Wallet*, hvor svindlere lykkedes med at koble ofrenes betalingskort op på deres egen Wallet app, hvilket åbner op for en helt nye muligheder for kortmisbrug, end de, de nuværende bankbude har, når de har borgernes fysiske kort i hånden. Samtidigt med det, elimineres alle geografiske udfordringer. Dette er et eksempel på, omstillingsparatheden hos de motiverede svindlere er unik, hvorfor de ikke må formodes at opgive grundet et par benspænd, så længe der er penge i sigte. Når det kommer til limits giver dette genklang hos vores informanter, idet der er forskellige opfattelse af, hvad den rette løsning er. Det skyldes at bankerne både skal sikre brugervenligheden for deres kunder, men samtidig forsøge at minimere uberettiget misbrug og formuetab for både banken selv og ofrene. Balancen mellem, hvornår svindlerne har et åbent ta'-selv-bord, og hvornår sikkerhedsforanstaltninger, begrænsninger og dobbeltgodkendelser bliver et begrænsende element i kundernes dagligdag, er vanskelig.

Som et helt andet alternativ finder vi, gennem et perspektiv med fokus på situationel forebyggelse, potentiale i, at man kunne styrke sikkerheden, ikke nødvendigvis blot ved betalingskortet, men også ved de fysiske hæveautomater. I stedet for kun at fokusere på betalingskortet, ser

vi et potentiale i at udnytte de teknologiske muligheder, der i dag er tilgængelige, til at øge beskyttelsen ved selve kontanthævningen. Konkret kunne der med fordel implementeres biometriske sikkerhedsforanstaltninger som ansigtsgenkendelse eller fingeraftryksidentifikation. Sådanne tiltag vil kunne gøre det markant sværere for uvedkommende at misbruge andres adgange og dermed bidrage til en mere tryg og modstandsdygtig infrastruktur omkring kontanthævninger. Vi ser de biometriske sikkerhedstiltag oplagte for fremtidens situationelle forebyggelse, da det skaber et problem for svindlerne, der ikke umiddelbart lader sig løse, ved blot at tænke 'ud af boksen'. Dog forholder vi os kritisk til, om omkostningerne ved etableringen og implementeringen af dette tiltag vil opveje omkostningerne ved BBB.

7.3 Efter – hensynsløs eller offer? - i juridisk forstand

Denne del af diskussionen forholder sig til det afsluttende element, *efter,* som forekommer, '*når skaden er sket*' og retter sig mod ofre, skadevirkningerne og den værdi, der både i fysisk og psykisk forstand, er gået tabt.

Når skaden er sket og ofre har lidt et økonomisk tab, gør det sig gældende, at pengeinstitutterne er underlagt en række retningslinjer, med udgangspunkt i, at de som organisation bærer et ansvar for at varetage kundernes, eller rettere sagt, nu ofrenes, interesser. I forlængelse heraf, er samtlige danske banker og pengeinstitutter omfattet af Betalingslovens § 100 (Bekendtgørelse af Lov om Betalinger). Konkret fremgår det i bestemmelsen;

> *Betalerens udbyder af betalingstjenester hæfter i forhold til betaleren for tab som følge af andres uberettigede anvendelse af en betalingstjeneste, medmindre andet følger af stk. 2-5 […].*

For så vidt angår specifikt BBB, findes reglerne i bestemmelsen *stk. 4,* hvortil der følger en konkret betingelse i *stk. 4 nr. 2;*

> *Stk. 4) Medmindre videregående hæftelse følger af stk. 5, hæfter betaleren med op til 8.000 kr. for tab som følge af andres uberettigede anvendelse af betalingstjenesten, hvis betalerens udbyder godtgør, at den til betalingstjenesten hørende personlige sikkerhedsforanstaltning har været anvendt, og*

> *Stk. 4, nr. 2) at betaleren med forsæt har overgivet den personlige sikkerhedsforanstaltning til den, der har foretaget den uberettigede anvendelse, uden at forholdet er omfattet af stk. 5, eller*

Dog lyder *stk. 3*;

> *Stk. 3. Medmindre videregående hæftelse følger af stk. 4 og 5, hæfter betaleren med op til 375 kr. for tab som følge af andres uberettigede anvendelse af betalingstjenesten, hvis den til betalingstjenesten hørende personlige sikkerhedsforanstaltning har været anvendt.*

Med egne ord, forholder det sig således, at hvis et betalingskort bliver stjålet ved alment tyveri, hæfter forurettede for at betale en selvrisiko på 375 kr., hvis der derimod er foregået et bankbudsbedrageri som beskrevet i specialet, så hæfter forurettede for at betale den væsentligt højere selvrisiko på 8.000 kr., hvilket er et for os, bemærkelsesværdigt regelsæt, hvortil der bør knyttes en række overvejelser. Det skal dog kommenteres, at der i retsdokumenterne påstande vedrørende erstatningskrav både forekommer, beløb á 375 kr., og 8.000 kr., hvorfor vi formoder, at der i nogle tilfælde er foretaget individuelle vurderinger i overensstemmelse med Betalingslovens § 100.

En af vores medvirkende banker bekræfter: *"Man har en egenbetaling på 8.000kr., hvis du selv udleverer dine kort og din PIN-kode"* (Bilag 12, linje 270-271), samt *"Det er typisk maks. 12.000kr., de kan få fat i. Så hæfter kunden altså for de 8 af dem selv, og så hjælper banken med de resterende".* (Bilag 12, linje 285-286).

På den ene side kan vi ikke negligere, at ofrene fysisk selv har overdraget deres betalingskort og pinkoder, direkte i hænderne på svindlerne. Dette er særligt væsentligt, da vi netop har gennemgået og identificeret 164 konkrete personer, som har gjort præcis dette. På den anden side finder vi det dog diskutabelt, om denne forbrydelse er mindre alvorlig og indgribende end det almene tyveri af betalingskort, som f.eks. kan ske for de fleste af os, når vi handler i supermarkedet, eller når vores taske kortvarigt er uden opsyn, og kortet forsvinder fra vores pung. Efter vores overbevisning er alvoren og ansvarsfordelingen i disse tilfælde ikke så skævt fordelt, som

det fremgår i juridisk forstand. Vi anser det nemlig som afgørende, at overdragelsen af betalingskortet i tilfælde af BBB er foregået under falske forudsætninger, og at dette bør tillægges en betydelig vægt.

Stk. 4, nr. 2 forudsætter *"at der har været fortsæt",* hvilken i alment sprog kan oversættes til, at en handling udføres bevidst eller ved at vedkommende er velvidende om, hvad handlingen kan medføre. Vi fremhæver denne ordlyd, fordi vi ikke mener, at det er tilfældet ved vores ofre. Ofre for BBB, er på trods heraf, ikke omfattet af de samme erstatningsrettigheder, som dem, der ikke får *narret*, men i stedet *stjålet* deres betalingskort fra dem.

Vi påstår ikke, at et offer for svindel aldrig kan handle hensynsløst eller altid kan undgå ethvert ansvar for det, de udsættes for. Der kan i visse tilfælde være elementer af personlig uagtsomhed eller mangel på kritisk dømmekraft. Dog det er vigtigt at anerkende, at denne problemstilling er kompleks og præget af dilemmaer. Balancen mellem individets ansvar og gerningspersonens skyld er sjældent entydig, og det kræver en nuanceret tilgang at forstå, hvornår og hvordan et offer kan siges at have medvirket til sin egen situation, uden at det fjerner fokus fra den egentlige uret, som er blevet begået. Vi ser derfor, at hensynsløshed kan forekomme, men at balancen heri er dilemmafyldt. *For hvordan opgør man dette ansvar?* særligt når flere kriminalitetstyper har en tydelig fællesnævner i, at udefrakommende uberettiget kommer i besiddelse af et betalingskort, og gør brug af det, på offerets bekostning.

Vi ser, at der gennem beløbene er en signalværdi i, hvorvidt ofrene bærer et medansvar, og i tilfælde heraf, i hvor stort et omfang. På den ene side, forholder vi os derfor undrende overfor, hvordan en forbrydelse (tyveri af betalingskort), er mindre alvorlig og rejser et lavere fokus på skyldsspørgsmålet, da det som udgangspunkt er en forbrydelse, der ikke også inkluderer en direkte psykisk belastning, i modsætning til BBB.

Vi kan ud fra vores overvejelser i ovenstående rejse en bekymring for, at der ved netop dette fænomen, BBB, kan forekomme en *samfundsmæssig* og/eller *retslig 'victimblaming'.* Vi begrebsliggør ovenstående, med *indirekte victimblaming.* Samlet set, kan vi dog ikke komme med et entydigt svar på, hvad der er rigtigt og forkert at gøre, hverken i juridisk eller moralsk forstand.

8. Konklusion

Formålet med nærværende speciale har været at undersøge, hvordan bankbudsbedrageri organiseres fra start til slut. Med afsæt i et stigende antal anmeldelser af kontaktbedrageri og en stor mængde potentielle ofre for it-relateret økonomisk kriminalitet undersøges en innovativ, omkostningstung og særlig form for bedrageri, der ikke tidligere er belyst fra en dansk akademisk vinkel. Alle kan i princippet blive ofre for denne form for svindel, men analysen viser, ofrene hovedsageligt er ældre kvinder omkring 81 år, som udvælges systematisk på baggrund af navnelister og livsomstændigheder. Deres rutiner, lette tilgængelighed ved ophold i hjemmet og besiddelse af fysiske kontanter udgør centrale risikofaktorer, der gør ældre kvinder til "oplagte ofre". Ofrene manipuleres systematisk gennem SE-teknikker, hvor svindlerne, der udgiver sig for at være repræsentanter fra banken, påtager sig autoritetsroller, skaber tidspres og hindrer kontakt til omverdenen.

Bagmændene rekrutterer udsatte mænd, typisk omkring 28 år, med aktivt misbrug og kriminel baggrund, til at agere bankbude. Disse fungerer som udskiftelige brikker i en svingdørskriminalitet, hvor rollefordelingen er klart defineret, mens den interne tillid er lav. Dette kommer til udtryk gennem trusler, dokumentationskrav og kontrol indbyrdes i de organiserede netværk, som vidner om en svag gruppetilknytning, der adskiller sig fra anden organiseret kriminalitet. Netværkene er organiseret i en hierarkisk struktur, hvor rekrutteringen foregår via sociale relationer, gældsforhold og krypterede platforme.

Bagmændene indtager en skjult, men central og styrende position, mens bankbudene befinder sig nederst i hierarkiet, og udfører det mest risikofyldte arbejde. Parallelt hermed foregår et tæt samarbejde med callere, der opererer fra forskellige lokationer, i form af callcentre og rullekontorer. Som fjerde og sidste led i netværket, er de eksterne aktører, vis funktion består i at købe og indsamle ulovlige datapakker, med personfølsomme oplysninger, i form af fullz. Vi finder, at kriminaliteten effektiviseres i stigende grad via cyber-aktiverede metoder, hvor svindel understøttes og faciliteres gennem brug af datapakker og telefoniske opkald. På baggrund heraf konkluderer vi, at BBB er en cyber-aktiveret kriminalitetsform, hvor teknologien, gennem et rationelt valg, anvendes til at understøtte og udvide svindlens udbytte og rækkevidde.

Ydermere er BBB ikke kun begrænset til én kriminalitetsform, men betragtes også som profitdrevet kriminalitet. Dette udleder vi, på baggrund af gerningspersonernes aktivitetsmønstre, der kendetegnes ved profit- og nyttemaksimering. I den forbindelse afslører de dokumenterede

hævningsmønstre, hurtige kontanthævninger, en bevidst udvælgelse af banker og beløbsstørrelser, en veludviklet forståelse af bankernes procedurer og limits. Der svindles for omfattende pengebeløb, hvor vi samlet set har identificeret svindel for 5,6 mio. kr. fordelt på netværkene. Vi konkluderer, at fænomenet er en kriminalitetsform styret af strategisk planlægning, systematik og professionalisme målrettet økonomisk vinding fra start til slut.

Svindelnetværkene er præget af høj mobilitet og omskiftelighed, hvor aktørerne flytter sig rundt, afhængigt af opgaver, og er således ikke geografisk forankret. De opererer landsdækkende, dog med særlig aktivitet i visse landsdele.

Bankbudsbedrageri er altså en kriminalitetsform, der kombinerer cyber- og kontaktbaserede elementer. Vi kan, ud fra et kriminologisk perspektiv, pege på mulige indsatser gennem situationel forebyggelse. Ved at ændre fastlagte procedurer, styrke ofres modstandsdygtighed gennem målrettede oplysningskampagner samt fysiske benspænd i forbindelse med kontanthævninger, besværliggøres de rationelle svindlers muligheder for succes.

På baggrund af ovenstående kortlægning, konkluderer vi at bankbudsbedrageri er organiseret ved en klar rollefordeling og hierarki, velovervejede hævning- og aktivitetsmønstre med fokus på profitmaksimering samt strategisk offerudvælgelse. Endvidere opereres der med høj mobilitet, tilpasningsdygtighed samt manipulationsteknikker.

Endeligt, konkluderer vi at bankbudsbedrageri er et komplekst fænomen med omfattende konsekvenser for både ofre og samfundet som helhed.

9. Litteraturliste

Aalborg Universitet (2025). Generativ AI på AAU. https://www.studerende.aau.dk/regler-ogpraktisk/it/generativ-ai-pa-aau (Besøgt d. 01/06/2025).

Bjørgo, T. (2016). Introduction: A Comprehensive Model for Preventing Crime. In *Preventing Crime. Crime Prevention and Security Management*. Palgrave Macmillan, London. https://doi.org/10.1057/9781137560483_1London

Braun, T. (2024). The Evolution Of Fraud: New Platforms, Old Tricks. Forbes. https://www.forbes.com/councils/forbesbusinesscouncil/2024/08/26/the-evolution-of-fraud-new-platforms-old-tricks/ (Besøgt d. 01/04/2025).

Bryman, A., Clark, T., Foster, L. & Sloan, L. (2021). Bryman's social research methods (Sixth edition.). Oxford University Press.

Choi, K., Lee, J., & Chun, Y. (2017). Voice phishing fraud and its modus operandi. Security Journal, 30(2), 454–466. https://doi.org/10.1057/sj.2014.49

Christie, N. (1986). The Ideal Victim. In Ezzat A. Fattah (red), *From Crime to Policy to Victim Policy – Reorientering the Justice System.* (pp. 17-30). London: MacMillan Press.

Cialdini, R. B. (2007). Influence: The psychology of persuasion. Collins. New York. (Vol. 55, p. 339).

Cornish, D. B. & Clarke, R. V. (2021). Crime as a Rational Choice. In Cullen, F. T., Agnew, R., & Wilcox, P. (red), *Criminological Theory, Past to Present* (pp. 425-430). Oxford University Press.

Cornish, D. B. (1994). The procedural analysis of offending and its relevance for situational prevention. Crime prevention studies, 3(1), (pp. 151-196).

Creswell, J. W. & Creswell, D. J. (2023). Research design: qualitative, quantitative and mixed methods approaches.

Cullen, F. T., Agnew, R., & Wilcox, P. (2021). Reviving Classical Theory: Deterrence and Rational Choice Theories. In Cullen, F. T., Agnew, R., & Wilcox, P. (red), *Criminological Theory, Past to Present* (pp. 399-418). Oxford University Press.

Danielsen, N. F. (2024). Mand varetægtsfængslet for at være falsk bankbud. TV Midtvest. https://www.tvmidtvest.dk/viborg/mand-varetaegtsfaengslet-for-at-vaere-falskbankbud (Besøgt d. 21/03/2025).

Danmarks Statistik (2023). Smartphone i ni ud af ti hjem. https://www.dst.dk/da/Statistik/nyheder-analyser-publ/nyt/NytHtml?cid=37848 (Besøgt d. 05/03/2025).

Danmarks Statistik (2025). Hvor mange hedder?... https://www.dst.dk/da/Statistik/emner/borgere/navne/hvor-mange-hedder (Besøgt d. 20/05/2025)

Danske Bank (2025). Digital innovation ændrer danskernes hverdag 1960-2021. https://danskebank.com/da/om-os/vores-historie/digital-innovation-aendrer-danskernes-hverdag-1960-2021 (Besøgt d. 21/04-2025).

DKR (2025). It-kriminalitet i tal. Det kriminalpræventive råd. https://dkr.dk/it/it-kriminalitet-i-tal (Besøgt d. 21/04/2025).

Eguchi, Y., Bun, S., Niimura, H., Shikimoto, R., Kida, H., Nishida, H., Suzuki, T., Takayama, M. & Mimura, M. (2024). P50: Fraud Victimization and Scam Vulnerability in the Arakawa Cohort Study Conducted in an Urban Area of Japan. International Psychogeriatrics, *36*(S1), 150–151. doi:10.1017/S1041610224002813

Finans Danmark (2025). Netbankssvindel. Finans Danmark. https://finansdanmark.dk/tal-og-data/institutter-filialer-ansatte/kriminalitet/svindel-med-netbank-og-betaling er/netbanksvindel/ (Besøgt d. 05/03/2025).

Finans Danmark (2024). Styrket bekæmpelse af digital svindel - Svindel Task Forcens 18 anbefalinger. Finans Danmark.

Finanstilsynet (2022). Kreditinstitutternes størrelsesgruppering - Pengeinstitutterne fordelt efter størrelse 2022. Finanstilsynet. https://www.finanstilsynet.dk/tal-og-fakta/statistik/kreditinstitutternes-stoerrelsesgruppering (Besøgt d. 04/04/2025).

Folketinget. (2017). Lov om betalinger *(Betalingsloven), LBK nr. 652 af 08/06/2017*. https://www.retsinformation.dk/eli/lta/2017/652

Gragg, D. (2003). A multi-level defense against social engineering. SANS Reading Room, 13, (pp. 1-21).

Griffin, S. E., & Rackley, C. C. (2008). *Vishing*. Proceedings of the 5th Annual Conference on Information Security Curriculum Development, InfoSecCD '08, 33–35. https://doi.org/10.1145/1456625.1456635

Grubb, T. (2010). The Five A's that Make Cybercrime so Attractive. Security Week. https://www.securityweek.com/five-as-make-cybercrime-so-attractive/ (Besøgt d. 31/03/2025).

Hameed, Z., Petersen, A.S., Hansen, D. G., Fabienke, J. B. & Jensen, S. (2025). Hackede optagelser afslører svindel indefra: Lyt med her trin for trin. Tjek Det. https://www.tjekdet.dk/indsigt/hackede-optagelser-afsloerer-svindel-indefra-lyt-med-her-trin-trin

Haselhuhn, M. P., Kennedy, J. A., Kray, L. J., Van Zant, A. B., & Schweitzer, M. E. (2015). Gender differences in trust dynamics: Women trust more than men following a trust violation. Journal of Experimental Social Psychology, *56,* (pp. 104–109). https://doi.org/10.1016/j.jesp.2014.09.007

Herfeld, C. (2022). Revisiting the criticisms of rational choice theories. Philosophy Compass, 17(1), e12774. https://doi.org/10.1111/phc3.12774doi.org

Holt, T., & Bossler, A. (2015). Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge.

Holt, T., Bossler, A., & Seigfried-Spellar, K. (2022). Cybercrime and digital forensics: An introduction. Routledge.

Ienca, M. & Vayena, E. (2021). Ethical requirements for responsible research with hacked data. *Nature Machine Intelligence, 3*(9), (pp. 744-748). doi: https://doi.org/10.1038/s42256-021-00389-w

Ingemann, J. H., Kjeldsen, L., Nørup, I., & Rasmussen, S. (2019). Kvalitative undersøgelser i praksis - viden om mennesker og samfund. Samfundslitteratur. 1 udgave, 2 oplag.

Jacobsen, A. V., Hummelmose, A. S. & Erenbjerg, A. (2024). It-anvendelse i befolkningen 2024. Danmarks Statistik.

Jacobsen, M. H. & Jensen, S. Q. (2012). Kvalitative udfordringer. København: Hans Reitzel Forlag.

Jakobsen, M. N. (2015). Bekæmpelse af særlig økonomisk kriminalitet – nogle karakteristika. Juristen, (3), (s. 89-97).

Jansen, J., & Leukfeldt, R. (2015). How people help fraudsters steal their money: an analysis of 600 online banking fraud cases. Workshop on Socio-Technical Aspects in Security and Trust, (pp. 24–31). https://doi.org/10.1109/STAST.2015.12

Jones, K. S., Armstrong, M. E., Tornblad, M. K., & Siami Namin, A. (2021). How social engineers use persuasion principles during vishing attacks. Information and Computer Security, 29(2), 314–331. https://doi.org/10.1108/ICS-07-2020-0113

Kripos (2023). Cyberkriminalitet 2023 - Politiets årlige temarapport om kriminalitet mot datasystemer og kriminalitet støttet av datasystemer. Politiet. https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2023.pdf

Kristiansen, K. (2025). Falske bankbude dømt i retten. TV Midtvest. https://www.tvmidtvest.dk/kort-nyt/falske-bankbude-doemt-i-retten (Besøgt d. 21/03/2025).

Kvale, S. & Brinkmann, S. (2015): Interview. København: Hans Reitzels Forlag.

Leclerc, B. (2017). Crime scripts. In Environmental Criminology and Crime Analysis. Taylor and Francis, (2nd edition), (pp. 119-141).

LII (2000). Modus operandi. Cornell Law School. https://www.law.cornell.edu/wex/modus_operandi (Besøgt d. 03/04/2025).

Loggen, J. & Leukfeldt, R. (2022). Unraveling the crime scripts of phishing networks: an analysis of 45 court cases in the Netherlands. *Trends Organ Crim* 25, 205–225. https://doi.org/10.1007/s12117-022-09448-z

Lusthaus, J. (2012). Trust in the world of cybercrime. Global crime, 13(2),(pp. 71-94).

Lusthaus, J. (2024). Reconsidering Crime and Technology: What Is This Thing We Call Cybercrime? Annual Review of Law and Social Science, 20(1), pp. 369–385. https://doi.org/10.1146/annurev-lawsocsci-041822-044042.

Lusthaus, J., Kleemans, E., Leukfeldt, R. & Holt, T. (2024). Cybercriminal networks in the UK and Beyond: Network structure, criminal cooperation and external interactions.

Trends Organ Crim 27, (pp. 364–387). https://doi.org/10.1007/s12117-022-09476-9

Lynggaard, K. (2020). Dokumentanalyse. I S. Brinkmann, & L. Tanggaard (red.), *Kvalitative metoder: En grundbog* (3 udgave.). Hans Reitzels Forlag.

McGuire, M. & Dowling, S. (2013). Cybercrime: a review of the evidence. Res. Rep. 75, Home Off., London.

Midt- og Vestjyllands Politi (2024). 24-årig dømt for bankbuds-bedragerier til 700.000 kroner. Politi. https://politi.dk/midt-og-vestjyllands-politi/nyhedsliste/24aarig-doemt-for-bankbudsbedragerier-til-700000-kroner/2024/12/16 (Besøgt d. 21/03/2025).

Moos-Bjerre A/S (2024). Ansvars- og rollefordelingen i forebyggelsen af IT-relateret økonomisk kriminalitet rettet mod voksne borgere. Det kriminalpræventive råd.

Moffitt, T. E. (2022). Pathways in the life course to crime. In Criminological Theory: Past to Present. Cullen, F. T., Agnew, R. & Wilcox, P. Oxford University Press.

NCIK (2024). NCIK Årsrapport 2023 - En rapport om it-relateret økonomisk kriminalitet anmeldt i 2023. Nationalt Center for IT-kriminalitet.

NCIK (2025). NCIK Årsrapport 2024 - En rapport om it-relateret økonomisk kriminalitet anmeldt i 2024. National Enhed for Særlig Kriminalitet.

NSK (2025). Svindlere manipulerer i højere grad borgere til at overføre penge. National Enhed for Særlig Kriminalitet. https://politi.dk/national-enhed-for-saerlig-kriminalitet/nyhedsliste/svindlere-manipulerer-i-hoejere-grad-borgere-til-at-overfoere-penge/2025/02/24 (Besøgt d. 02/05/2025).

Ordnet.dk (2025). Bankbud. https://ordnet.dk/ddo/ordbog?query=bankbud&tab=for (Besøgt d.21/04/2025).

Pedersen, M. L. & Balvig, F. (2024). Udsathed for vold og andre former for kriminalitet - Offerundersøgelserne 2005-2023. Justitsministeriet.

Petersen, C. M. (2025). Falske bankbude på spil i Østjylland. Odder Avis. https://ugeavisen.dk/odderavis/falske-bankbude-paa-spil-i-oestjylland (Besøgt d. 21/03/2025).

PET (2025). Freya er OSINT-specialist. https://pet.dk/du-kan-ogsaa-arbejde-i-pet/hvem-arbejder-i-pet/freya-er-osint-specialist (Besøgt d. 31/05/2025).

Prior, L. (2003). Basic themes: use, production and content. In *Basic themes: Use, production and content* (pp. 2-29). SAGE Publications Ltd, https://doi.org/10.4135/9780857020222.n1

Racina, K. (2024). Falske bankbude har svindlet sig til over 20 mio. kroner i år. Finans Danmark. https://finansdanmark.dk/nyheder/2024/december/falske-bankbude-har-svindlet-sig-til-over-20-mio-kroner-i-aar/ (Besøgt d. 10/03/2025).

Regeringen (2021). National strategi for cyber- og informationssikkerhed. Finansministeriet.

Riis, O. (2005). Samfundsvidenskab i praksis: introduktion til anvendt metode. 1. udgave, 1. oplag. Kbh. Hans Reitzel.

Yin, R. K. (2014). Case study research: design and methods (Fifth edition.). SAGE.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future internet, 11(4), 89.

Sikker Digital (2025). Falske mails og sms'er - phishing og smishing. Sikker Digital. https://www.sikkerdigital.dk/borger/digital-svindel/phishing-og-smishing (Besøgt d. 27/04/2025)

Smith, R. G. (2000). Fraud and financial abuse of older persons. Current issues in criminal justice, 11(3), (pp. 273-291).

Stajano, F., & Wilson, P. (2011). Understanding scam victims: seven principles for systems security. Communications of the ACM, *54*(3), (pp. 70-75).

Straffeloven (LBK nr. 976 af 26/09/2019 med senere ændringer). Retsinformation.dk: https://www.retsinformation.dk/eli/lta/2019/976

Song, J., Kim, H., & Gkelias, A. (2014). iVisher: Real-Time Detection of Caller ID Spoofing. *ETRI Journal*, *36*(5), (pp.) 865–875. https://doi.org/10.4218/etrij.14.0113.0798

Sykes, G. M., & Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. American Sociological Review, 22(6), (pp. 664–670). https://doi.org/10.2307/2089195

Thorning, C. (2025). Stor anti-svindel kampagne fortsætter i 2025. Finans Danmark. https://finansdanmark.dk/nyheder/2025/januar/stor-anti-svindelkampagn efortsaetter-i-2025/ (Besøgt d. 10/03/2025).

Tjek det (2025). Spoofing-svindlerne. https://www.tjekdet.dk/spoof (Besøgt d. 3/04/2025).

Ueno, D., Arakawa, M., Fujii, Y., Amano, S., Kato, Y., Matsouka, T. & Narumoto, J. (2022). Psychosocial characteristics of victims of special fraud among Japanese older adults: A cross-sectional study using scam vulnerability scale. Frontiers in Psychology, doi: 10.3389/fpsyg.2022.960442.

van't Hoff-de Goede, M. S., van de Weijer, S., & Leukfeldt, R. (2024). Explaining cybercrime victimization using a longitudinal population-based survey experiment. Are personal characteristics, online routine activities, and actual self-protective online behavior related to future cybercrime victimization? *Journal of Crime & Justice*, *47*(4),(pp. 472–491). https://doi.org/10.1080/0735648X.2023.2222719

Viano, E. C. (2017). Cybercrime, organized crime, and societal responses. Int. approaches, Basel.

Wall, D. S. (1998). Catching cybercriminals: policing the Internet. International Review of Law, Computers & Technology, 12(2), (pp. 201-218).

Winchester, N. (2021). Financial fraud and vulnerable people. UK Parliament. https://lordslibrary.parliament.uk/financial-fraud-and-vulnerable-people/ (Besøgt d. 01/04/2025).