rijksuniversiteit groningen

Noord-Nederland

“Hello, to future millionaires!”:

Een inhoudsanalyse van het gebruik van neutralisatietechnieken in advertenties van Cybercrime-as-a-Service-aanbieders op illegale online marktplaatsen

Kris Roemer

Juli 2025

Sociologie van de Criminaliteit en Veiligheid
Faculteit Gedrags- en Maatschappijwetenschappen
Rijksuniversiteit Groningen

Begeleider: Zoltán Lippényi
Referent: Marinus Spreen

Voorwoord

Voor u ligt mijn masterscriptie die is geschreven ter afronding van de master Sociologie van Criminaliteit en Veiligheid aan de Rijksuniversiteit Groningen. In dit onderzoek is gekeken naar de manier waarop aanbieders van Cybercrime-as-a-Service gebruikmaken van neutralisatietechnieken op illegale online marktplaatsen. Hiervoor zijn advertenties van het dark web en Telegram verzameld, om deze vervolgens zowel kwantitatief als kwalitatief te analyseren op neutralisatietechnieken en andere advertentiekenmerken. Het doel van dit onderzoek is om bij te dragen aan de huidige inzichten over online criminaliteit en om inzichtelijk te maken hoe neutralisatietechnieken kunnen worden gebruikt in de interactionele context van online criminaliteit en Cybercrime-as-a-Service in het bijzonder.

Tijdens het schrijven van deze scriptie heb ik stage mogen lopen bij het RIEC Noord-Nederland. Het RIEC speelt een ondersteunende rol voor samenwerkingspartners, zoals gemeenten en politie, in het bestrijden van ondermijnende criminaliteit. Hieronder valt ook kennisdeling en het signaleren van criminele patronen. Tijdens deze stage heb ik nieuwe inzichten verkregen over de verschijningsvormen van ondermijnende criminaliteit en over hoe integrale aanpak kan bijdragen aan de bestrijding hiervan. Ik wil graag mijn begeleider, Arjen de Boer, bedanken voor de nuttige sparringsessies en het vertrouwen in mijn afstudeerproces. Ook wil ik graag alle andere collega's bij RIEC Noord-Nederland bedanken voor het meedenken met mijn onderzoek en de leuke, leerzame tijd die ik hier heb beleefd.

Daarnaast wil ik graag Zoltán Lippényi bedanken voor de begeleiding vanuit de Rijksuniversiteit Groningen. Dankzij de ontvangen feedback en fijne samenwerking heb ik mijzelf verder kunnen ontwikkelen op het gebied van onderzoek doen. Ook wil ik mijn referent, Marinus Spreen, bedanken voor de geleverde input op dit onderzoek.

Tot slot wil ik graag mijn tweede codeur bedanken voor de tijd en moeite die erin zijn gestoken om bij te dragen aan dit onderzoek.

Kris Roemer

Groningen

11-07-2025

Abstract

De opkomst van Cybercrime-as-a-Service (CaaS) heeft geleid tot een professionalisering van online criminaliteit. Criminele diensten zoals DDoS-aanvallen, phishing en ransomware worden op een laagdrempelige wijze aangeboden op illegale marktplaatsen, waaronder het dark web en Telegram. Deze ontwikkeling heeft als resultaat dat de morele en technische drempel voor deelname aan online criminaliteit is verlaagd. Ook gebruikers zonder criminele achtergrond of gespecialiseerde kennis kunnen hiermee eenvoudig instappen. In dit onderzoek wordt gekeken of aanbieders ook morele bezwaren bij potentiële kopers weg proberen te nemen aan de hand van neutralisatietechnieken. Neutralisatietechnieken fungeren hierbij als overtuigingsstrategie, waarbij deviant gedrag wordt gepresenteerd als moreel acceptabel of onschuldig. Dit wordt gedaan aan de hand van de volgende onderzoeksvraag: “Op welke manier gebruiken aanbieders van Cybercrime-as-a-Service op illegale online marktplaatsen neutralisatietechnieken in hun advertenties?”.

Om deze vraag te kunnen beantwoorden is er een inhoudsanalyse van 369 advertenties uitgevoerd met zowel een kwantitatief als kwalitatief component. Er is onderzocht hoe vaak, in welke context en op welke manieren neutralisatietechnieken worden gebruikt. Hierbij is gebruikgemaakt van het model van Kaptein & Van Helvoort (2019), waarbij twaalf neutralisatietechnieken zijn onderscheiden. De resultaten laten zien dat neutralisatietechnieken in bijna één op de drie advertenties voorkomen en vaak worden gecombineerd met andere kenmerken. Aanbieders die neutralisatietechnieken toepassen hanteren voornamelijk een zakelijke toon en creëren vaker een groepsgevoel in advertenties door naar de online gemeenschap te verwijzen. Opvallend is dat advertenties op het dark web significant vaker neutralisatietechnieken bevatten dan op Telegram. Ook maakten veel aanbieders gebruik van alternatieve overtuigingsstrategieën, zoals positieve reputatieverwijzingen en het bieden van een klantenservice. Dit hing echter niet significant samen met het gebruik van neutralisatietechnieken. Deze bevindingen suggereren dat neutralisatietechnieken strategisch worden ingezet om de morele weerstand bij potentiële kopers te verlagen.

Verder bleken de advertenties ingebed te zijn in een bredere online subcultuur, waarin mannelijkheid, status en normvervaging centraal staan. Doelwitten werden in de advertenties vaak ontmenselijkt of als legitiem slachtoffer voorgesteld. Veel aanbieders benadrukten ook het verdienen van geld en het nemen van wraak als redenen om een aankoop te doen. Daarnaast waren er verschillende typen aanbieders te herkennen aan hun zelfpresentatie. Sommige aanbieders presenteerden zichzelf als legitieme aanbieders en hanteerden daarbij een zakelijke toon, terwijl andere aanbieders het criminele karakter duidelijk naar voren lieten komen en zich meer informeel opstelden.

Dit onderzoek laat zien dat CaaS-aanbieders niet alleen producten en diensten ter verkoop aanbieden, maar ook morele rechtvaardigingen bieden om het aanbod aantrekkelijker te maken. Daarmee levert dit onderzoek een bijdrage aan de literatuur over neutralisatietechnieken en hoe zij ook op interactioneel niveau een rol kunnen spelen.

Inhoudsopgave

Hoofdstuk 1: Inleiding

In december 2024 haalden internationale opsporingsdiensten in het kader van ‘Operation PowerOFF’ 27 websites offline die DDoS-aanvallen als dienst aanboden. Via deze websites konden gebruikers tegen betaling websites van bijvoorbeeld bedrijven of overheidsinstanties tijdelijk platleggen, zonder daarvoor zelf computerkennis nodig te hebben. Bij deze operatie van onder andere de FBI, Europol en de Nederlandse Politie, werden drie personen gearresteerd. Zij boden deze diensten aan als onderdeel van een professioneel opgezet verdienmodel. Meer dan 300 gebruikers van hun diensten werden geïdentificeerd (Europol, 2024). Deze casus laat zien dat online criminaliteit zich steeds meer verplaatst naar een digitale markt waar criminelen hun diensten te koop aanbieden.

Deze ontwikkeling maakt deel uit van een bredere verschuiving waarbij illegale online marktplaatsen voor meer mensen beschikbaar worden. Dit zijn digitale omgevingen waarin illegale goederen en diensten grootschalig worden verhandeld, zoals software, drugs en persoonsgegevens. Potentiële kopers kunnen in contact komen met aanbieders en ronden de transacties af met de cryptovaluta’s die op dat moment populair zijn (Leukfeldt et al., 2017). Een populaire marktplaats is het dark web, dit is een gedeelte van het verborgen internet dat vaak voor illegale doeleinden wordt gebruikt. Alhoewel het dark web voor iedereen toegankelijk is, is het een aantrekkelijke plek voor criminele doeleinden vanwege de anonimiteit van de gebruikers. De locatie en het IP-adres van gebruikers kunnen niet worden achterhaald en dus kunnen criminele handelingen die hier worden uitgevoerd niet makkelijk worden teruggeleid naar de dader (Saleem et al., 2022). Ook de app Telegram is populair onder online criminelen (Roks & Monshouwer, 2020). Mensen kunnen hier berichten met elkaar uitwisselen in privégesprekken of in groepen met tot wel tienduizenden leden tegelijkertijd. De gegevens van gebruikers worden beschermd door Telegram en worden niet toegankelijk gemaakt voor derden, waaronder overheidspartijen en opsporingsinstanties (Telegram, z.d.).

In 2024 werden 2,4 miljoen Nederlanders van 15 jaar of ouder slachtoffer van een vorm van online criminaliteit, wat een toename is in vergelijking met 2022 (Centraal Bureau voor de Statistiek, 2025). Tegenwoordig wordt bijna de helft van alle criminaliteitsslachtoffers in Nederland veroorzaakt door online criminaliteit (Openbaar Ministerie, z.d.). Deze toename van online criminaliteit hangt samen met de toegankelijkheid van illegale online marktplaatsen, waar je relatief eenvoudig veel geld kunt verdienen met weinig investeringen en technische kennis. Vergeleken met traditionele criminele markten is de pakkans online lager, mede doordat online criminaliteit zich zo snel ontwikkelt dat opsporingsinstanties moeite hebben om deze veranderingen bij te houden (Ablon et al., 2014). De drempel van deze illegale online marktplaatsen is tegenwoordig lager omdat er steeds meer karakteristieken van legitieme online markten over worden genomen. Websites die online illegale goederen en diensten aanbieden, gebruiken vergelijkbare technieken als legitieme websites. In de

advertenties van aanbieders wordt duidelijke communicatie over veiligheidsmaatregelen opgemerkt, maar ook het bieden van kortingen en gratis verzending, de mogelijkheid voor klanten om reviews achter te laten en in sommige gevallen zelfs een klantenservice om problemen op te lossen (Fisher et al., 2025; Holt et al., 2022). Er worden uiteenlopende tactieken toegepast door concurrerende aanbieders om zoveel mogelijk potentiële kopers te overtuigen. Deze manier van aanbieden draagt bij aan een gevoel van professionaliteit en betrouwbaarheid voor potentiële kopers.

Onder online criminaliteit vallen alle delicten waarbij gebruik wordt gemaakt van ICT. Dit kunnen delicten zijn die volledig afhankelijk zijn van ICT, zoals DDoS-aanvallen of hacken, maar ook traditionele delicten die door ICT worden gedigitaliseerd zoals online fraude (Furnell, 2020). Hoe online criminaliteit zich zo snel heeft kunnen verspreiden over de jaren heen, kan worden verklaard aan de hand van de ‘Routine Activities Theory’. Volgens deze theorie ontstaat criminaliteit als de volgende drie elementen samenkomen: een gemotiveerde dader, een geschikt doelwit en de afwezigheid van toezicht (Cohen & Felson, 1979). Op het internet kunnen mensen zich anoniem en flexibel bewegen, waardoor normen die in de offline wereld gelden niet altijd doorwerken in de online context. Er is minder toezicht op online handelingen. Dit maakt het makkelijker voor individuen om gedragingen te vertonen die zij offline wellicht niet als acceptabel zouden beschouwen (Goldsmith & Brewer, 2015). De digitale omgeving kan de grens tussen legaal en illegaal gedrag doen vervagen, wat het aantal gemotiveerde daders vergroot. Onderzoek laat verder zien dat bepaalde digitale gewoonten sterk samenhangen met het risico om slachtoffer te worden van online criminaliteit. Er zijn bepaalde apparaten en handelingen die aantrekkelijk zijn voor criminelen, maar ook het gebrek aan directe bescherming van gebruikers en het regelmatig online zijn maakt specifieke doelwitten extra geschikt (Junger et al., 2017).

Binnen deze digitale onderwereld speelt Cybercrime-as-a-Service (CaaS) een grote rol. Dit is een vorm van dienstverlening waarbij de software die nodig is om delicten te plegen ter verkoop wordt aangeboden door ervaren criminelen met geavanceerde computervaardigheden (Ablon et al., 2014). Het is mogelijk om iemand in te huren om een bepaalde online aanval voor je uit te voeren, maar je kunt ook kant-en-klare software of andere tools aanschaffen voor permanent gebruik of gedurende een bepaalde tijdsperiode (Manky, 2013). Mensen met onvoldoende computervaardigheden kunnen met behulp van CaaS toch online delicten plegen. Aanbieders van CaaS voorzien hun klanten daarnaast niet alleen van software, maar geven ook specifieke instructies over het toepassen ervan en bieden de mogelijkheid tot gepersonaliseerde aanpassingen om het gebruik zoveel mogelijk te vereenvoudigen (Kshetri & Chauhan, 2023). Het Openbaar Ministerie noemde dit soort software eerder een “Zwitsers zakmes voor cybercrime”, omdat het zo gemakkelijk wordt gemaakt om op grote schaal slachtoffers te maken (NOS, 2024a). Ook de Nederlandse Politie (2024) merkt op dat digitale hulpmiddelen voor online fraude al enige jaren worden aangeboden via het dark web en sociale media.

Naast de laagdrempeligheid en professionalisering van CaaS, kunnen aanbieders ook neutralisatietechnieken gebruiken om het aanbod op een overtuigende manier te presenteren. Dit zijn

rechtvaardigingen voor deviant gedrag (Kaptein & Van Helvoort, 2019). Sociale normen die mensen er normaliter van weerhouden om een delict te plegen, kunnen met behulp van neutralisatietechnieken tijdelijk worden omzeild. Morele implicaties zoals schuldgevoelens over het gepleegde delict kunnen hiermee voorkomen worden. Als aanbieders deze technieken toepassen, kan het morele besef van kopers dus op interactioneel niveau worden beïnvloed om diegene te overtuigen om een illegale aankoop te doen.

Er is nog weinig onderzoek gedaan naar hoe criminele aanbieders gebruikmaken van neutralisatietechnieken om potentiële kopers te overtuigen. In verschillende onderzoeken naar het gebruik van neutralisatietechnieken in de online criminaliteit worden uiteenlopende definities van de technieken gehanteerd, wat het lastig maakt om vast te stellen welke technieken het meest worden gebruikt door online criminelen (Brewer et al., 2020). Zo toont onderzoek van Bossler (2021) bijvoorbeeld aan dat sommige neutralisatietechnieken bijdragen aan een verhoogde bereidheid tot online criminaliteit, terwijl andere geen significant effect hebben. Dit kan samenhangen met de specifieke context waarin de technieken worden toegepast. Kaptein & Van Helvoort (2019) hebben vanwege de grote variëteit een model ontwikkeld met 60 individuele neutralisatietechnieken, waarmee in beeld wordt gebracht welke technieken er zijn en hoe deze herkend kunnen worden. Er ontbreekt echter nog wel kennis over welke neutralisatietechnieken worden gebruikt bij verschillende vormen van online criminaliteit, evenals hoe deze technieken gebruikt kunnen worden binnen de interactionele context. Er is ook nog geen onderzoek gedaan naar de toepassing ervan in Nederlandstalige advertenties, bij verschillende platforms en verschijningsvormen van CaaS. In eerdere onderzoeken lag de focus voornamelijk bij de motivatie van online criminelen zelf en niet bij de rol van aanbieders in het proces van morele rechtvaardiging.

Met dit onderzoek wordt in kaart gebracht hoe aanbieders van CaaS gebruikmaken van neutralisatietechnieken om potentiële kopers te overtuigen. Volgens sociologische theorieën worden houdingen ten opzichte van criminaliteit gevormd via sociale interactie. De theorie over ‘Techniques of Neutralization’ van Sykes & Matza (1957) laat zien hoe morele bezwaren kunnen worden geneutraliseerd om deviant gedrag mogelijk te maken. Aanbieders van CaaS kunnen potentiële kopers overtuigen door illegale diensten niet te presenteren als deviant gedrag, maar als een legitieme handeling. Bijvoorbeeld door zichzelf niet te presenteren als crimineel maar als technologisch expert of ondernemer, of door criminele handelingen te presenteren als zakelijke transacties of een vorm van rechtvaardige rebellie. Daarmee beïnvloeden zij hoe het aanbod van online criminaliteit wordt waargenomen door potentiële kopers.

Dit onderzoek legt specifiek de focus bij aanbieders van Caas omdat zij met hun advertenties mensen op interactioneel niveau kunnen overhalen om criminele diensten aan te schaffen. Door deze processen in kaart te brengen, ontstaan waardevolle inzichten over de rol van communicatie van aanbieders in de sociale mechanismen die online criminaliteit aantrekkelijk en toegankelijk maken. Dit

leidt tot de volgende onderzoeksvraag: “Op welke manier gebruiken aanbieders van Cybercrime-as-a-Service op illegale online marktplaatsen neutralisatietechnieken in hun advertenties?”

Hoofdstuk 2: Theoretisch kader

In dit hoofdstuk wordt allereerst ingegaan op de definitie van neutralisatietechnieken en de manier waarop deze kunnen worden toegepast binnen de context van Cybercrime-as-a-Service. Vervolgens wordt er aandacht besteed aan de verschillende doelgroepen en hoe deze terug zijn te zien in verschillende online marktplaatsen en soorten delicten. Tot slot wordt er stilgestaan bij de afstand die bestaat tussen het doelwit en de aanbieders en kopers van CaaS.

2.1 Neutralisatietechnieken

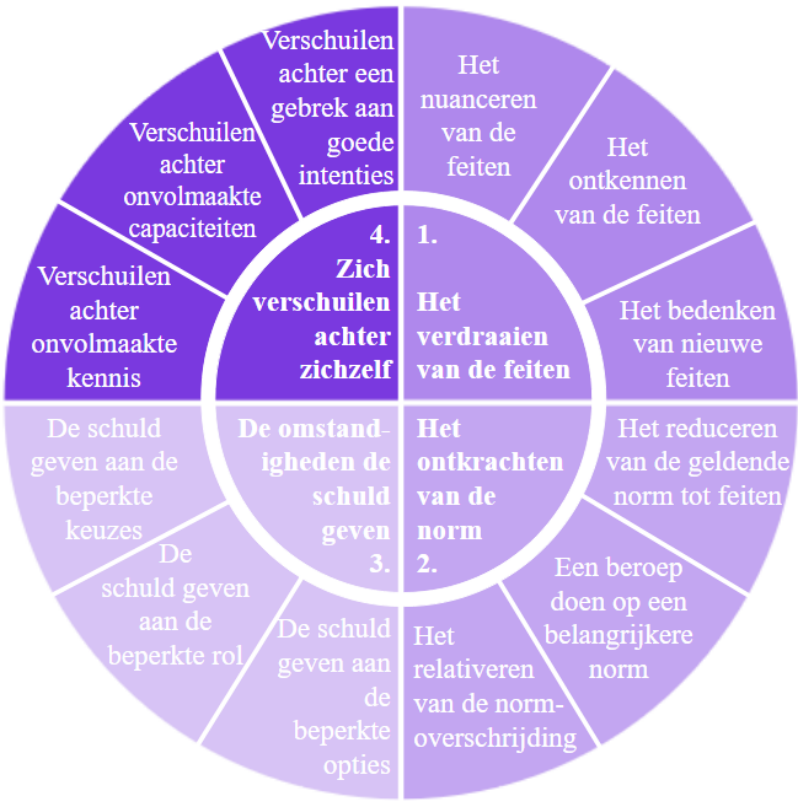
De samenleving ziet online criminaliteit als bedreiging. Dit blijkt uit de manier waarop overheden, media en opsporingsinstanties online criminaliteit presenteren: als een groeiend probleem dat actief moet worden bestreden. Zo wordt er bijvoorbeeld meer geld beschikbaar gesteld voor de aanpak van online criminaliteit en gelden er in Nederland hoge straffen voor daders (Rijksoverheid, z.d.). Er is ook onderzoek gedaan naar de percepties van mensen tegenover verschillende vormen van online criminaliteit. Hieruit blijkt dat boosheid de meest voorkomende emotie is, voornamelijk als de privacy en het vertrouwensgevoel van individuen wordt aangetast (Achuthan et al, 2025). Deze manier van straffen en de percepties tegenover online criminaliteit laten zien dat het plegen van online criminaliteit wordt afgekeurd door de samenleving, waardoor er morele, sociale en juridische consequenties aan verbonden zijn voor daders.

Ondanks deze morele implicaties en geldende wetten, blijft online criminaliteit groeien (Centraal Bureau voor de Statistiek, 2025). Veel delinquenten zien hun eigen deviante gedrag namelijk wel als rechtvaardig of onschuldig, ook al wordt dit niet zo gezien door het rechtssysteem of de maatschappij (Kaptein & Van Helvoort, 2019). Met behulp van neutralisatietechnieken kunnen delinquenten hun deviante gedrag moreel rechtvaardigen. Dit hoeft niet altijd een onderdeel te zijn van een interne afweging die wordt gemaakt door de delinquent zelf, want neutralisatietechnieken kunnen ook tijdens het communiceren worden ingezet om het deviante gedrag anders over te laten komen op een ander. Zo zouden aanbieders van CaaS ze ook kunnen gebruiken om het aanbod als minder deviant te presenteren. Sykes en Matza (1957) hebben als eerste een vijftal neutralisatietechnieken geïdentificeerd die individuen kunnen toepassen om morele bezwaren en schuldgevoelens te omzeilen voorafgaand aan het plegen van een delict. Deze technieken vormen de basis voor latere onderzoeken naar neutralisatietechnieken en worden daarom ook wel de ‘famous five’ genoemd (Kaptein & Van Helvoort, 2019). Hieronder vallen bijvoorbeeld het ontkennen van verantwoordelijkheid en het ontkennen van het slachtoffer (Sykes & Matza, 1957).

Sindsdien hebben onderzoekers aanvullende technieken geïdentificeerd. Kaptein & Van Helvoort (2019) hebben deze samengevoegd in één overkoepelend model dat in totaal zestig verschillende neutralisatietechnieken bevat. Het model is opgedeeld in vier hoofdcategorieën, die ieder drie bredere neutralisatietechnieken bevatten. Dit onderzoek maakt gebruik van deze twaalf

neutralisatietechnieken. In figuur 1 is een visuele weergave opgenomen van de vier hoofdcategorieën en de bijbehorende neutralisatietechnieken.

Figuur 1: Visuele weergave van de vier hoofdcategorieën en bijbehorende neutralisatietechnieken volgens het model van Kaptein & Van Helvoort (2019)



De eerste hoofdcategorie is het verdraaien van de feiten. De feiten over het delict worden hier anders voorgedaan aan zichzelf of aan anderen zodat er geen sprake meer lijkt te zijn van een normoverschrijding. Deze categorie bevat de volgende neutralisatietechnieken: het nuanceren van de feiten, het ontkennen van de feiten en het bedenken van nieuwe feiten. Bij het nuanceren van de feiten wordt de waarheid die het gedrag deviant maakt ontkend. De waarheid kan volledig ontkend worden, of er kan worden beweerd dat de waarheid niet bewezen is of dat mensen niet op de hoogte kunnen zijn van deze waarheid (Kaptein & Van Helvoort, 2019). Aanbieders van CaaS zouden hier op kunnen inspelen door twijfel te zaaien over wat moreel en crimineel is. Bijvoorbeeld door te stellen dat de regels over het delict die gelden in het ene land, niet gelden in het andere land; dit ondermijnt het idee dat er een objectieve waarheid over het delict bestaat. Bij de tweede neutralisatietechniek in deze categorie, het ontkennen van de feiten, wordt de waarheid over het gedrag wel erkend. Echter, deze waarheid wordt vermeden door één of meer feiten over het delict te ontkennen. Mensen kunnen wel accepteren dat zij deviant gedrag hebben vertoond, maar zwakken dit af door feiten te ontkennen zoals

de toegedane schade of het bestaan van een slachtoffer (Kaptein & Van Helvoort, 2019). Door te stellen dat er geen echte schade is toegedaan, hoeft de dader zichzelf niet als crimineel te zien (Ridley & Selck-Paulsson, 2022). Aanbieders zouden deze neutralisatietechniek kunnen gebruiken door bijvoorbeeld de toegedane schade te bagatelliseren, te stellen dat er helemaal geen sprake is van een slachtoffer, of door het strafbare karakter te minimaliseren. Bij het bedenken van nieuwe feiten wordt er een nieuwe realiteit gecreëerd waarin het gedrag niet of in mindere mate deviant is. Het onderscheid tussen wat een feit is en wat fictie wordt bewust vervaagd (Kaptein & Van Helvoort, 2019). Aanbieders zouden hierop in kunnen spelen door scenario's in advertenties te schetsen waarin het gedrag rechtvaardig of onschuldig oogt. Een concreet voorbeeld van deze techniek komt uit het onderzoek van Connelly et al. (2025) waarin de volgende rechtvaardiging wordt gebruikt: *"There are no companies without money [that cannot pay a ransom]."* Er wordt een fictief scenario gecreëerd waarin de toegedane schade aan het slachtoffer wordt geneutraliseerd. Aanbieders zouden soortgelijke scenario's kunnen schetsen.

De tweede hoofdcategorie is het ontkrachten van de norm. Dit heeft betrekking op de norm die stelt dat het gedrag afwijkend is, die met behulp van de neutralisatietechnieken wordt weerlegd. Deze categorie bestaat uit de volgende neutralisatietechnieken: het reduceren van de geldende norm tot feiten, een beroep doen op een belangrijkere norm en het relativeren van de normoverschrijding. Bij het reduceren van de geldende norm tot feiten wordt de geldende norm niet inhoudelijk ontkracht, maar weggezet als irrelevant. In plaats van in te gaan op de inhoud van de norm, wordt deze gepresenteerd als iets subjectiefs of willekeurigs. Zo kan morele afkeuring worden afgedaan als een kwestie van persoonlijke smaak, waarmee de afwijzing van het gedrag door anderen haar overtuiging verliest. Ook wordt de norm soms omzeild door het gebruiken van alternatieve bewoordingen, zoals eufemismen of metaforen, die het gedrag minder immoreel doen lijken (Kaptein & Van Helvoort, 2019). Ook deze neutralisatietechniek zouden aanbieders kunnen gebruiken door in de advertentie de norm af te doen als een persoonlijke voorkeur. Voorbeelden die hieronder vallen zijn uitspraken als *"That is just the way the world works"* of het verwijzen naar autodiefstal als een *"joyride"* (Kaptein & Van Helvoort, 2019). Deze uitspraken kunnen een koper het idee geven dat er geen geldende norm wordt geschonden. Bij een beroep doen op een belangrijkere norm wordt een andere norm belangrijker geacht dan de norm die wordt overschreden. De overschrijdende norm kan worden gezien als een nobel of maatschappelijk doel, zoals verzet, waardoor het deviante gedrag op een positieve manier wordt gepresenteerd. De belangrijkere norm kan ook voortkomen uit het conformeren aan anderen en hun verwachtingen; bijvoorbeeld een norm die wordt gehanteerd door een rolmodel of in de eigen sociale groep. Vergelding en overlevingsdrang vallen ook onder de overschrijdende normen, omdat dit onder het hogere doel van zelfbescherming en persoonlijke rechtvaardigheid geschaald kan worden (Kaptein & Van Helvoort, 2019). Aanbieders zouden hiervan gebruik kunnen maken door hun aanbod te koppelen aan een hoger doel als technologische innovatie (Connelly et al., 2025). Aanbieders zouden het product ook kunnen omschrijven als een populaire keuze bij andere klanten. Producten die

op deze manier worden gepresenteerd worden vaker gekocht, omdat mensen graag conformeren aan het gedrag dat door anderen wordt vertoond (Cialdini, 2021). Bij het relativeren van de normoverschrijding wordt erkend dat de norm is overtreden, maar gesteld dat dit niet erg is. De redenatie kan zijn dat er anderen zijn die nog erger gedrag vertonen, of dat het gedrag niet erg is zo lang het niet te frequent plaatsvindt (Kaptein & Van Helvoort, 2019). Aanbieders zouden hiervan gebruik kunnen maken door te verwijzen naar andere criminelen of delicten die nog immoreler zijn, zodat het eigen aanbod mild lijkt in vergelijking.

Bij de derde hoofdcategorie wordt de schuld gegeven aan de omstandigheden. Er wordt erkend dat het gedrag deviant is, maar hier wordt geen of minder verantwoordelijkheid voor gedragen vanwege de omstandigheden. Hieronder vallen de neutralisatietechnieken om de schuld te geven aan beperkte opties, aan de beperkte rol in het delict of aan beperkte keuzes. Als de schuld wordt gegeven aan beperkte opties, wordt het vertonen van het deviante gedrag goedgepraat door te beweren dat er geen betere, realistische alternatieven waren voor het deviante gedrag. De delinquent meent dus dat hij in deze situatie niet anders kon (Kaptein & Van Helvoort, 2019). Aanbieders zouden kunnen inspelen op deze neutralisatietechniek door andere opties als niet haalbaar te presenteren, bijvoorbeeld omdat alternatieven te duur, te langzaam of te ineffectief zijn. Een ander voorbeeld is dat diefstal wordt omschreven als een eenmalige, unieke kans om spullen te verkrijgen die anders niet verkrijgbaar zijn (Kaptein & Van Helvoort, 2019). Als de schuld wordt gegeven aan de beperkte rol in het deviante gedrag, wordt verantwoordelijkheid voor het gedrag ontkend. Bijvoorbeeld omdat de eigen rol in het delict maar een kleine rol was van het geheel. De verantwoordelijkheid kan op iemand anders worden afgeschoven om de eigen verantwoordelijkheid te minimaliseren (Kaptein & Van Helvoort, 2019). Aanbieders zouden dit kunnen gebruiken om te stellen dat de koper slechts degene is die de aankoop doet, maar niet degene die het delict daadwerkelijk uitvoert. Als de schuld wordt gegeven aan beperkte keuzes wordt er erkend dat er wel alternatieve opties zijn, maar dat enkel de keuze voor deviant gedrag over blijft vanwege externe druk en grote verleidingen. Bijvoorbeeld als dit de keuze is waarmee het meeste indruk op anderen kan worden gemaakt (Kaptein & Van Helvoort, 2019). Hier zouden aanbieders op kunnen inspelen door bewust verleidingen te creëren in hun advertenties, zoals het leggen van de nadruk op financiële vrijheid, snel geld verdienen en status.

De vierde hoofdcategorie is het verschuilen achter zichzelf. Door dit te doen wordt ook het idee gecreëerd dat de delinquent minder verantwoordelijkheid draagt voor het gedrag. Dit kan op drie verschillende manieren: beweren dat er sprake is van onvolmaakte kennis, onvolmaakte capaciteiten, of een gebrek aan goede intenties. Bij het verschuilen achter onvolmaakte kennis wordt beweerd dat de delinquent niet had kunnen weten dat het gedrag deviant was; daarom draagt diegene geen (volledige) verantwoordelijkheid voor het gedrag (Kaptein & Van Helvoort, 2019). Deze neutralisatietechniek leent zich minder goed voor aanbieders om te gebruiken. De techniek draait vooral om het verontschuldigen van het eigen gedrag door onwetendheid te claimen. Voor aanbieders is het niet gunstig om de koper als onwetend neer te zetten, omdat potentiële kopers dit als negatief

kunnen ervaren en omdat dit kan afnemen van de positieve presentatie van de aanbieder zelf. Bij het verschuilen achter onvolmaakte capaciteiten beweert de delinquent dat het deviante gedrag voortkomt uit onbekwaamheid en een gebrek aan zelfcontrole (Kaptein & Van Helvoort, 2019). Ook deze techniek is minder toepasbaar voor aanbieders in een interactionele context. Het suggereren dat kopers hun gedrag niet onder controle hebben, zou wederom een tegenovergesteld effect kunnen hebben. Bij het verschuilen achter een gebrek aan goede intenties beweren delinquenten niet verantwoordelijk te zijn voor het gedrag, omdat ze niet beschikken over de neiging om zich te conformeren aan de norm. Het delict wordt gepleegd zonder daar schaamte of schuldgevoelens bij te ervaren (Kaptein & Van Helvoort, 2019). Dit is een risicovolle neutralisatietechniek voor aanbieders om te gebruiken, omdat er wordt erkend dat er sprake is van immoreel gedrag. Dit kan echter wel toegepast worden door een beeld van normloosheid te creëren, waarin plezier beleven bij het delict centraal staat. Morele onverschilligheid kan worden gepresenteerd als een aantrekkelijke houding. Tegelijkertijd zou de aanbieder dit ook kunnen gebruiken om duidelijk te maken dat je met elk verzoek bij diegene terecht kunt, omdat diegene niet door morele grenzen tegen wordt gehouden. In criminele sferen zou dit een positieve reputatie kunnen opleveren.

2.1.1 Neutralisatietechnieken in de context van Cybercrime-as-a-Service

Oorspronkelijk worden neutralisatietechnieken omschreven als manieren voor delinquenten om het delict intern te rechtvaardigen (Kaptein & Van Helvoort, 2019). In de context van Cybercrime-as-a-Service zouden ze echter ook strategisch kunnen worden ingezet om anderen te beïnvloeden. CaaS-aanbieders verkopen hun diensten en producten om hiermee geld te verdienen. De advertenties moeten dan ook zo aantrekkelijk mogelijk zijn. Om dit te bereiken kunnen aanbieders proberen om de morele weerstand bij potentiële kopers te verlagen door twijfels en schuldgevoelens te neutraliseren, voordat de transactie plaatsvindt.

Neutralisatietechnieken kunnen expliciet worden ingezet als een overtuigingsmiddel in de interactie tussen aanbieder en koper. Aanbieders presenteren hun motivatie bijvoorbeeld niet als financieel gewin, maar als persoonlijke ontwikkeling of maatschappelijke bijdrage. Een ransomware-gebruiker beschreef de eigen motivatie als volgt: *“The money is not the target – the process is the important thing… The one of self-realisation”* (Connely et al., 2025). Door online criminaliteit te presenteren als een vorm van zelfontplooiing, wordt het beeld gecreëerd dat de activiteit moreel verdedigbaar is. Op deze manier wordt niet alleen de dienst van de aanbieder gepresenteerd als acceptabel, maar ook het gedrag van de koper. Het onderliggende doel is om kopers gerust te stellen door te pretenderen dat zij geen onderdeel zijn van een criminele praktijk, maar van iets belangrijkers wat de geldende normen overstijgt (Kaptein & Van Helvoort, 2019).

Neutralisatietechnieken zijn specifiek gericht op het rechtvaardigen van deviant gedrag, maar aanbieders kunnen ook aanvullende strategieën gebruiken om hun aanbod zo aantrekkelijk mogelijk te

maken. Aanbieders kunnen bijvoorbeeld proberen om een groepsgevoel te creëren in hun advertenties door bepaalde aanspreekvormen richting potentiële kopers te gebruiken. Door te verwijzen naar bepaalde groepsnormen of door de koper bij de hand te nemen in het uitvoeren van het delict, wordt het gepresenteerd als normaal binnen de groep. Kopers voldoen dan aan de verwachtingen van deze groep als zij een aankoop doen, of hebben het idee dat ze doen wat anderen in dezelfde situatie ook zouden doen (Cialdini, 2021; Kaptein & Van Helvoort, 2019). Aanbieders kunnen ook een beeld van legitimiteit proberen te schetsen, door hun eigen diensten aan te bieden op een manier die overeenkomt met advertenties van legitieme bedrijven: er worden kortingen geboden en er is een klantenservice beschikbaar als er problemen worden ervaren (Fisher et al., 2025). Door zichzelf voor te doen als een legitieme aanbieder richting potentiële klanten, wordt de aanschaf van deze diensten en producten afgebeeld als iets dat niet deviant is (Ridley & Selck-Paulsson, 2022). Het taalgebruik en de presentatie kunnen dus bewust worden gekozen om hun handeling als acceptabel voor te doen.

Een andere strategie is door vertrouwen op te bouwen met de potentiële koper door de eigen expertise en relevante kennis te benadrukken. Mensen laten zich sneller overtuigen door iemand die zichzelf presenteert als iemand met expertise, omdat dit betrouwbaarheid en geloofwaardigheid uitstraalt (Klucharev et al., 2008). Dit komt concreet naar voren in het gebruiken van online reputaties. Op het dark web kunnen kopers op sommige websites beoordelingen achterlaten over de dienst/het product en de aanbieder zelf. Aanbieders met een betrouwbare reputatie hebben meer kopers en kunnen hogere prijzen vragen dan aanbieders zonder reputatie (Przepiorka et al., 2017). Aanbieders hebben dus een financieel voordeel bij een positieve reputatie. Naast de reviews die door klanten worden achtergelaten, kunnen aanbieders ook zelf actief verwijzen naar hun eigen reputatie en betrouwbaarheid. Om betrouwbaarheid uit te stralen verwijzen aanbieders vaak naar scherpe prijzen en de hoge kwaliteit van hun eigen aanbod, maar bieden ook transparantie door informatie te geven over zaken als betaalmethoden en levering. Andere signalen die verkopers kunnen afgeven zijn de periode waarin een aanbieder al actief is op een platform en de toegankelijkheid voor contact met (potentiële) kopers (Laferrière & Décary-Hétu, 2023). Door deze verschillende strategieën met neutralisatietechnieken te combineren kunnen aanbieders hun advertenties zo aantrekkelijk mogelijk maken en de nadruk op morele implicaties meer naar de achtergrond verplaatsen.

2.2 Doelgroepen

De mate waarin neutralisatietechnieken worden toegepast door aanbieders kan verschillen afhankelijk van de doelgroep die zij voor ogen hebben. Een belangrijk onderscheid hierbij is dat tussen beginnende criminelen (‘drifters’) en consistente criminelen. Maruna & Copes (2005) stellen dat delinquenten neutralisatietechnieken gebruiken voorafgaand aan het delict, om zichzelf moreel in staat te stellen tot deviant gedrag over te gaan. Dit geldt in het bijzonder voor de groep die door Matza (1964) wordt omschreven als ‘drifters’: dit zijn individuen die wel belang hechten aan de

maatschappelijke normen, maar hier op sommige momenten van afwijken om deviant gedrag te vertonen. Het gebruik van neutralisatietechnieken zorgt ervoor dat zij zichzelf kunnen verplaatsen tussen conformerend en deviant gedrag zonder de morele implicaties hiervan te ervaren. Neutralisatietechnieken zijn belangrijk voor deze groep delinquenten omdat zij sociale relaties hebben die normafwijkend gedrag afkeuren en het deviante gedrag dus niet als gangbaar zien (Walters et al., 2023). De innerlijke spanning bij het plegen van deviant gedrag is daardoor voor deze groep het grootst. De toepassing van neutralisatietechnieken wordt ook wel gezien als een teken van zwakke criminele binding: hoe meer afstand iemand houdt tot een criminele identiteit, hoe sterker de behoefte aan morele rechtvaardiging (Maruna & Copes, 2005).

De komst van het internet heeft het voor deze groep nog makkelijker gemaakt om zich te verplaatsen tussen conformerend en deviant gedrag. Met behulp van technologie kunnen delicten worden gepleegd vanuit de privésfeer en is er minder binding vereist tussen criminelen onderling. Dit stelt gebruikers in staat om hun betrokkenheid flexibel te houden; ze bepalen zelf in hoeverre ze zich emotioneel en sociaal verbinden met hun online handelen. Hierdoor kan er gemakkelijk geëxperimenteerd worden met deviant gedrag, zonder directe morele consequenties daarvan te ervaren (Goldsmith & Brewer, 2015). De anonimiteit tussen de dader en slachtoffer zorgt er ook voor dat de daders de gevolgen van hun gedrag minder sterk ervaren (Weulen Kranenbarg & Leukfeldt, 2021). Dit maakt het makkelijker om hun criminele handelingen los te koppelen van hun identiteit. Omdat de drempel om criminaliteit te plegen lager is in de online wereld, kan de toepassing van neutralisatietechnieken hier nog effectiever zijn om beginnende criminelen te overtuigen.

Bij consistente of ervaren criminelen speelt deze verplaatsing tussen deviant en conformerend gedrag in mindere mate. Zij hebben meer criminele relaties en maken deel uit van de subculturen waarin deviant gedrag genormaliseerd is (Walters et al., 2023). Sociale groepen creëren hun eigen regels over wat acceptabel is en niet, waarbij wordt vastgesteld wat wel of niet deviant is binnen de groep. Het vertonen van wat voor anderen deviant gedrag is, kan dus voortkomen uit de subcultuur waarvan de persoon onderdeel uitmaakt waarin dit gedrag wel is genormaliseerd. Dit geldt ook voor online subculturen. Online criminelen kunnen handelen volgens de sociale normen van hun groep, terwijl het gedrag wel de algemeen geldende (sociale) regels overtreedt (Holt, 2019). Naarmate een individu dieper in de criminaliteit raakt, verliezen conventionele morele waarden hun grip en neemt de behoefte aan neutralisatietechnieken ook af (Maruna & Copes, 2005).

Digitale platforms, zoals het dark web en Telegram, vervullen ook een sociale en educatieve functie. Criminelen kunnen elkaar hier online ontmoeten en netwerken vormen, of elkaar anoniem om hulp en advies vragen over het plegen van een delict. Op veel online forums worden tutorials geplaatst om beginnende criminelen op weg te helpen (Leukfeldt et al., 2017). Dit versterkt de normalisering van online criminaliteit binnen online subculturen, waardoor er in eerste instantie al minder morele complicaties worden ervaren. De verschillen tussen deze groepen komen ook tot uiting in de platforms die zij gebruiken en de moeilijkheidsgraad van de delicten die zij plegen.

2.2.1 Online marktplaatsen

Hoewel het aanbod van Cybercrime-as-a-Service in zijn geheel wordt gekenmerkt door anonimiteit en een relatief laagdrempelig karakter, zijn er specifieke platforms die hierin een centrale rol spelen. Met name Telegram en illegale marktplaatsen op het dark web zijn belangrijke omgevingen voor het aanbieden en afnemen van Cybercrime-as-a-Service. Deze platforms verschillen echter wel in hun technische toegankelijkheid en complexiteit, waardoor ze mogelijk verschillende soorten gebruikers aantrekken.

De benodigde software om op het dark web te kunnen komen is voor iedereen beschikbaar, maar het gebruik ervan vereist wel enige kennis over hoe dark web browsers en websites precies werken (Saleem et al., 2022; United Nations, z.d.). Deze complexiteit vormt een barrière voor mensen die niet beschikken over deze kennis, wat het platform minder toegankelijk maakt. Het gebruik van Telegram brengt daarentegen minder barrières met zich mee. Dit is een reguliere mobiele applicatie en daarom voor iedereen met een smartphone te downloaden. Binnen enkele minuten kunnen gebruikers criminele groepen vinden met behulp van eenvoudige zoektermen, wat de toenadering toegankelijk maakt voor iedereen. Zo stellen aanbieders van drugs op Telegram zelf dat dit een laagdrempelige manier is om nieuwe klanten te werven, waarbij eenvoudige taal en emoji's worden gebruikt in hun advertenties (NOS, 2024b). Dit maakt Telegram laagdrempeliger dan het dark web, waar advertenties op een professionele manier worden ingericht (Fisher et al., 2025). De informele toon en de laagdrempeligheid van Telegram maken het beter afgestemd op beginnende criminelen met beperktere computervaardigheden (Tidy, 2024).

Telegram lijkt dus toegankelijker en aantrekkelijker voor de groep beginnende criminelen, die een grotere behoefte hebben aan morele rechtvaardiging dan consistente criminelen. Op basis van deze verschillen luidt de eerste hypothese als volgt: Telegram-advertenties bevatten meer neutralisatietechnieken dan dark web-advertenties.

2.2.2 Soorten delicten en moeilijkheidsgraad

Er bestaan veel verschillende soorten diensten en producten die via Cybercrime-as-a-Service worden aangeboden, waarmee uiteenlopende delicten kunnen worden gepleegd. Dit brede aanbod maakt CaaS aantrekkelijk voor een diverse groep daders. De moeilijkheidsgraad verschilt per aangeboden dienst of product. Sommige tools zijn vrijwel direct inzetbaar en vereisen minimale computervaardigheden, terwijl andere wel meer computervaardigheden of ervaring vragen om effectief gebruikt te kunnen worden. Er is dus een onderscheid tussen meer eenvoudige en gecompliceerde delicten. In bijlage 1 wordt een overzicht gegeven van de verschillende CaaS-vormen met hun moeilijkheidsgraad.

Bij de eenvoudige delicten wordt er weinig gevraagd van de koper. De koper betaalt voor het uitvoeren van de dienst of de installatie van software en hoeft verder niets te doen of minimale handelingen te verrichten (Ablon et al., 2014). Hieronder valt bijvoorbeeld phishing. De phishing kits

die worden aangeboden zijn erg compleet. Bij de kits zijn al templates voor e-mails inbegrepen om naar potentiële slachtoffers te sturen, maar ook de neppe websites waar ze naartoe worden geleid en formulieren waarin vervolgens de persoonsgegevens worden verzameld (Ganguli, 2024). De koper hoeft de phishing-berichten dus alleen nog maar te versturen, waarna op grote schaal toegang tot bankrekeningen wordt verkregen. Het uitvoeren van een DDoS-aanval, waarbij een website tijdelijk offline wordt gehaald door er enorm veel dataverkeer op af te sturen, heeft een vergelijkbare moeilijkheidsgraad. De koper hoeft enkel aan te geven om welke website het gaat en voor hoe lang deze offline moet blijven (Ganguli, 2024). Dit vereist dus verder geen computervaardigheden van de koper, de koper hoeft alleen de advertentie te vinden en te betalen. Ook ransomware is door de opkomst van CaaS een eenvoudig delict geworden. Bij een ransomware-aanval worden de bestanden of de computer van het slachtoffer geblokkeerd en wordt er losgeld geëist om de toegang terug te krijgen. De benodigde software die wordt aangeboden is ook gebruiksklaar en vereist weinig handelingen van de koper. Voor de enkele handelingen die wel verricht moeten worden, wordt in de meeste gevallen een klantenservice aangeboden voor vragen en problemen (Fisher et al., 2025).

Waar eenvoudige delicten weinig computervaardigheden vereisen, zijn bij gecompliceerde delicten wel kennis en handelingen van de koper noodzakelijk na aanschaf. Sommige aanbieders zijn dan ook meer gericht op het bijstaan van ervaren criminelen (Akyazi et al., 2021). Bij deze complexere delicten wordt meer gevraagd van de koper: ze vereisen diepgaandere computervaardigheden, strategisch inzicht en soms langdurige voorbereiding. Bij het gebruik van ‘exploit kits’ moet de koper bijvoorbeeld nog zelf de kwetsbaarheden in het systeem van een doelwit identificeren en de software daar handmatig op aanpassen (Huang et al., 2018). Een ander voorbeeld is het gebruik van een ‘remote access trojan’ waarbij langdurige toegang wordt verkregen tot het systeem van een slachtoffer. Het kan als kant-en-klaar product worden aangeschaft, maar het gebruik ervan is gecompliceerd omdat het beheren van het systeem van het slachtoffer zelf uitgevoerd moet worden en onopgemerkt moet blijven (Huang et al., 2018).

De variërende moeilijkheidsgraad trekt uiteenlopende groepen kopers aan. Eenvoudigere delicten richten zich op beginnende criminelen met beperkte computervaardigheden, terwijl gecompliceerde delicten aantrekkelijker zijn voor ervaren criminelen met geavanceerde computervaardigheden. Aanbieders zijn zich bewust van deze doelgroepsverschillen (Akyazi et al., 2021). Op basis hiervan luidt de tweede hypothese als volgt: bij het aanbieden van eenvoudige delicten worden meer neutralisatietechnieken gebruikt dan bij het aanbieden van gecompliceerde delicten.

2.3 Afstand tot het doelwit

De sociale en emotionele afstand tot het beoogde doelwit kan ook het gebruik van neutralisatietechnieken beïnvloeden. Hoe anoniemer en onpersoonlijker het doelwit voelt, hoe gemakkelijker het is voor de dader om de morele implicaties van het delict te negeren. Deze afstand

maakt het eenvoudiger om het slachtofferschap te ontkennen of om de ernst van de schade te bagatelliseren (Brewer et al., 2020). Deze afstand kan ook gecreëerd worden door nieuwe feiten te verzinnen die de realiteit zodoende aanpassen dat het delict niet langer als deviant wordt gezien. Een voorbeeld hiervan is stellen dat ransomware-betalingen weinig tot geen consequenties zullen hebben voor het doelwit, omdat het een bedrijf betreft dat het geld zou kunnen missen (Connolly et al., 2025). Daders zijn ervan op de hoogte dat hun acties negatieve consequenties hebben voor slachtoffers en creëren een nieuwe realiteit waarin dit niet langer het geval is. Door sociale en emotionele afstand tot het beoogde doelwit te creëren, kunnen de morele implicaties die met het delict gepaard gaan geneutraliseerd worden. Een ander voorbeeld is om een ander label aan het slachtoffer te hangen, zoals “kapitalist”, wat het idee geeft dat het acceptabel is om dit bedrijf als slachtoffer te nemen (Connolly et al., 2025).

Binnen online criminaliteit is de afstand tussen dader en doelwit vaak al groot. Veel vormen van online criminaliteit, zoals DDoS-aanvallen en ransomware, richten zich voornamelijk op doelwitten zoals bedrijven of andere instanties (Centraal Bureau voor de Statistiek, 2023). Doelwitten staan niet dichtbij de dader, waardoor zij kunnen worden gereduceerd tot een administratief gegeven zoals een bankrekeningnummer of IP-adres. Vaak gaat het delict ook nog landsgrenzen over, wat de sociale en emotionele afstand nog verder vergroot. Deze anonimiteit en afstand verlagen de drempel voor deviant gedrag, omdat de emotionele impact op het doelwit onzichtbaar blijft voor de dader (Weulen Kranenbarg & Leukfeldt, 2021).

Aanbieders van Cybercrime-as-a-Service kunnen hierop inspelen in hun advertenties. Door te benoemen dat het product/de dienst kan worden toegepast op bedrijven en andere instanties, in plaats van personen, wordt het delict meer gerechtvaardigd en zijn de advertenties dus aantrekkelijker voor potentiële kopers. Dit leidt tot de derde hypothese: er worden meer neutralisatietechnieken gebruikt als het type doelwit een persoon is, dan wanneer het doelwit een bedrijf of instantie betreft.

Hoofdstuk 3: Methoden

Het doel van dit onderzoek is om inzicht te krijgen in de wijze waarop aanbieders van Cybercrime-as-a-Service neutralisatietechnieken gebruiken in hun advertenties, door te analyseren hoe zij in advertenties op het dark web en Telegram communiceren naar potentiële kopers. Er wordt gepoogd antwoord te geven op de volgende onderzoeksvraag: “Op welke manier gebruiken aanbieders van Cybercrime-as-a-Service op illegale online marktplaatsen neutralisatietechnieken in hun advertenties?”.

In dit hoofdstuk wordt toegelicht wat de opzet van dit onderzoek is om deze onderzoeksvraag te kunnen beantwoorden. Daarnaast wordt er besproken welke methoden er zijn gebruikt voor de dataverzameling en hoe de data is gecodeerd en geanalyseerd. Ook wordt er toelichting gegeven over de operationalisatie van de variabelen en de ethische overwegingen die zijn gemaakt over de onderzoeksopzet, de dataverzameling en de data-analyse.

3.1 Onderzoeksopzet

Er is een inhoudsanalyse uitgevoerd met zowel een kwantitatief als een kwalitatief component. In een inhoudsanalyse kunnen onderwerpen gekwantificeerd worden door deze te tellen, zoals het aantal keren dat een specifieke neutralisatietechniek wordt gebruikt of het aantal advertenties dat op een specifiek platform wordt aangeboden. Tegelijkertijd kan de tekst ook kwalitatief geanalyseerd worden door kwalitatieve componenten uit de teksten te verzamelen. Tijdens het coderen werden citaten verzameld over onder andere de gebruikte neutralisatietechnieken en de toon van de tekst. Deze werden achteraf geanalyseerd om exploratief te kunnen kijken naar de vormgeving van de taal en de context waarbinnen neutralisatietechnieken worden gebruikt. Door beide benaderingen te combineren, ontstaat er een vollediger beeld van hoe aanbieders hun diensten presenteren. Het kwantitatieve deel van het onderzoek is gebruikt om de drie gestelde hypothesen mee te toetsen, maar heeft ook een exploratieve functie. Er is gekeken welke neutralisatietechnieken het vaakst worden gebruikt en of er patronen zichtbaar zijn in relatie tot onder andere het platform, de taal of de aangeboden dienst/het product. Omdat neutralisatietechnieken afhankelijk van de context en het taalgebruik zijn, is het belangrijk om aan de hand van de kwalitatieve analyse te begrijpen hoe deze technieken worden vormgegeven.

Een inhoudsanalyse is een veelgebruikte methode voor berichten vanuit de massamedia, die de intentie hebben om een groot, heterogeen publiek te bereiken (Neuendorf et al., 2017). CaaS-advertenties kunnen ook beschouwd worden als berichten uit de massamedia omdat ze geplaatst worden op openbare marktplaatsen met als doel om zoveel mogelijk potentiële kopers te bereiken. Een inhoudsanalyse maakt het ook mogelijk om grotere hoeveelheden kwalitatieve data, in dit geval de

teksten uit de CaaS-advertenties, te analyseren (Mogaji, 2017). Met deze methode kan worden achterhaald wat het doel en de boodschap zijn van de bestudeerde communicatie (Krippendorff, 2019).

Dit onderzoek kan het best gekarakteriseerd worden als een descriptieve inhoudsanalyse, waarbij de focus ligt op het systematisch beschrijven en interpreteren van elementen binnen de tekst zelf (Neuendorf et al., 2017). Het onderzoek heeft dus gedeeltelijk een verklarend karakter, omdat er achterhaald wordt welke neutralisatietechnieken worden toegepast om potentiële kopers te overtuigen. De hypothesen die zijn gesteld op basis van de literatuur zijn getoetst. Tegelijkertijd is het onderzoek grotendeels exploratief, omdat er nog weinig bekend is over neutralisatietechnieken in CaaS-advertenties. Er wordt daarom gekeken naar mogelijke nieuwe patronen en verbanden tussen neutralisatietechnieken en andere advertentiekenmerken. Het exploratieve gedeelte is zowel kwantitatief als kwalitatief uitgevoerd. Zo is er gekeken naar welke neutralisatietechnieken het meest en minst worden gebruikt en hoeveel er worden gebruikt per platform. Ook is er gekeken naar de samenhang tussen bijvoorbeeld het gebruik van neutralisatietechnieken en het type aanbieder en met de aanwezigheid van andere technieken zoals reputatie, klantenservice en kortingen/promoties.

3.2 Dataverzameling

De CaaS-advertenties zijn van twee verschillende platforms gehaald waarop illegale online marktplaatsen plaatsvinden: het dark web en Telegram. De verzamelde advertenties waren openbaar beschikbaar voor alle gebruikers van het platform. In totaal zijn er 369 advertenties verzameld, waarvan 262 van het dark web en 107 van Telegram. De dark web-advertenties zijn afkomstig van twaalf verschillende websites en de Telegram-advertenties uit twaalf verschillende groepen. In bijlage 2 staat een volledig overzicht van deze groepen en websites.

De totale omvang van de populatie bestaat uit alle Engels- en Nederlandstalige, openbare CaaS-advertenties die op het dark web en Telegram zijn aangeboden in de periode van dataverzameling. Deze worden geplaatst in verschillende groepen en op verschillende websites. Het werkelijke aantal hiervan is niet vast te stellen, omdat het gaat om criminele praktijken in dynamische online omgevingen. Er worden continu nieuwe groepen en websites gestart, terwijl andere weer offline gehaald worden. Zo zijn er tijdens de periode van dataverzameling ook twee groepen op Telegram verdwenen en was één van de websites op het dark web enkele dagen uit de lucht. Er zijn geen statistieken (openbaar) beschikbaar die laten zien om welke aantallen aanbieders en advertenties dit in totaal gaat. Om dit probleem op te lossen is gebruikgemaakt van een operationele populatie, wat een bruikbare momentopname is van de populatie en geen weergave van de gehele realiteit (Neuendorf et al., 2017). De operationele populatie bestaat uit alle Engels- en Nederlandstalige CaaS-advertenties die gedurende de periode van dataverzameling van drie weken zijn geplaatst op specifieke websites en in groepen.

Alle advertenties die zijn geplaatst op het dark web en Telegram gedurende deze drie weken zijn opgeslagen, mits zij voldeden aan drie criteria. Ten eerste moesten de advertenties expliciet een CaaS-dienst aanbieden, zoals DDoS-aanvallen of phishing kits. Het maakt verder niet uit welke dienst er specifiek wordt aangeboden, alle verschijningsvormen van CaaS worden inbegrepen bij het onderzoek. Ten tweede moeten de advertenties afkomstig zijn van websites en groepen die actief zijn tijdens de dataverzameling om een actueel beeld te geven van hoe aanbieders op dit moment hun diensten presenteren. De advertenties moeten dus tijdens deze tijdsperiode beschikbaar zijn voor afnemers. Als laatste worden er zowel Engelstalige als Nederlandstalige advertenties meegenomen, maar geen andere talen. Een visuele weergave van een aantal geanalyseerde advertenties is opgenomen in bijlage 3, om inzichtelijk te maken hoe de advertenties er in de oorspronkelijke context uitzagen.

Op Telegram maakten aanbieders gebruik van bots die dezelfde advertentie herhaaldelijk in een groep bleven sturen, soms tientallen keren per minuut. Hierdoor was er sprake van veel dubbele advertenties. Alle individuele advertenties die zijn geplaatst in de periode van dataverzameling zijn opgeslagen, maar konden dus niet allemaal worden gebruikt. Alle advertenties met dezelfde inhoud zijn er na afloop van de dataverzameling uitgefilterd. Alle advertenties die na deze stap zijn overgebleven, vormen het aantal advertenties van de operationele populatie.

Op het dark web waren er verschillende aanbieders actief die meerdere advertenties plaatsten voor verschillende diensten en producten. Van sommige aanbieders waren er tientallen verschillende advertenties te vinden. Deze advertenties hadden dezelfde structuur, opmaak en taalgebruik. Het enige verschil tussen deze advertenties per aanbieder was het aangeboden product. Om oververtegenwoordiging van de communicatiestijl van deze aanbieders in de data te voorkomen, is ervoor gekozen om maximaal vijf advertenties te verzamelen per individuele aanbieder.

In de advertenties werd door de aanbieders met regelmaat gebruikgemaakt van straattaal en afkortingen. Om er zeker van te zijn dat de betekenissen van deze woorden goed werden geïnterpreteerd tijdens het verzamelen van de advertenties en het coderen, werden deze woorden tijdens de dataverzameling opgezocht in een online straattaal woordenboek.

Het vaststellen van de operationele populatie liep gelijktijdig aan de dataverzameling zelf. Dit was wederom noodzakelijk vanwege de vluchtige aard van de advertenties. Alle advertenties die in deze tijdsperiode werden geplaatst en voldeden aan de criteria, werden opgeslagen per platform en kregen een nummer. Alle opgeslagen advertenties vormen uiteindelijk de operationele populatie (Neuendorf et al., 2017). Vanwege het haalbare aantal advertenties van 369 dat uiteindelijk is verzameld, is de gehele operationele populatie gebruikt voor de data-analyse.

3.3 Codering van de data

Het coderen is handmatig uitgevoerd aan de hand van een codeboek en bijbehorend codeerformulier. Deze zijn van tevoren ontworpen om tijdens het coderen zo objectief mogelijk te kunnen werken (Neuendorf et al., 2017). De variabelen en categorieën uit het codeboek zijn overgenomen in het codeerformulier, dat voor iedere individuele advertentie werd ingevuld. Zo werd er stapsgewijs een bruikbare dataset opgebouwd (Mogaji, 2017). In het codeboek zijn alle variabelen en antwoordmogelijkheden uitgebreid toegelicht, met per categorie duidelijke definities en voorbeelden. Dit verhoogt de betrouwbaarheid van de codering en vergemakkelijkt een consistente interpretatie tussen codeurs (Neuendorf et al., 2017).

Bij de inhoudsanalyse zijn de kwantitatieve en kwalitatieve componenten gelijktijdig uitgevoerd in het codeerformulier. Er is gekozen voor deze aanpak omdat de combinatie van beide methoden leidt tot een beter begrip van de uitkomsten. Zowel de frequentie als het taalgebruik van de variabelen konden worden onderzocht van alle advertenties in de steekproef. Door beide componenten gelijktijdig toe te passen en niet op verschillende momenten, konden de neutralisatietechnieken en andere variabelen het beste in de context van de advertentie worden geplaatst door de codeurs. Het was ook praktisch haalbaar om een kwalitatieve analyse uit te voeren voor alle advertenties in de steekproef omdat de advertenties over het algemeen vrij kort zijn en daarom weinig analysetijd vereisten.

Alle advertenties zijn gecodeerd door één codeur, namelijk de uitvoerder van het onderzoek. Omdat de codeur op de hoogte is van het doel van het onderzoek en de gestelde hypothesen, kan er sprake zijn geweest van bepaalde vooroordelen tijdens het coderen. Dit kan invloed hebben op de validiteit en betrouwbaarheid van de uitkomsten (Neuendorf et al., 2017). Daarom zijn vijftig van de advertenties ook gecodeerd door een tweede codeur. De tweede codeur had alleen toegang tot de advertenties, het codeboek en het codeerformulier. Er werden willekeurige nummers van advertenties geselecteerd voor de tweede codeur. Ieder nummer kon maar één keer geselecteerd worden. De achtergrond van de tweede codeur is niet relevant, omdat deze persoon verder niet betrokken is geweest in het onderzoek. Beide codeurs beheersen het Nederlands en Engels vloeiend, zodat advertenties in beide talen zorgvuldig beoordeeld konden worden.

Met het codeboek en het codeerformulier is eerst een testronde uitgevoerd. De eerste codeur heeft 35 proefadvertenties gecodeerd met het oorspronkelijke codeboek en op basis hiervan nodige aanpassingen gedaan. Nadat deze aanpassingen zijn doorgevoerd, heeft de tweede codeur het codeboek doorgenomen en 10 proefadvertenties hiermee gecodeerd. De eerste en tweede codeur hebben hierna een overleg gevoerd over hun bevindingen. Aan de hand van dit overleg zijn eventuele onduidelijkheden in het codeboek verhelderd. De proefadvertenties zijn willekeurig verzameld voorafgaand aan de periode van dataverzameling. Met het definitieve codeboek (bijlage 5) en codeerformulier (bijlage 6) zijn de advertenties uit de operationele populatie gecodeerd. De eerste codeur heeft alle 369 advertenties gecodeerd en de tweede codeur heeft 50 advertenties gecodeerd.

De coderingen van beide codeurs op de overeenkomende advertenties zijn samengevoegd in één bestand. Met dit bestand zijn per kwantitatieve variabele betrouwbaarheidscoëfficiënten berekend in SPSS. Het betrouwbaarheidscoëfficiënt vergelijkt de antwoorden van beide codeurs met elkaar. Er is gekozen voor Cohen's Kappa, omdat alle kwantitatieve variabelen die worden getoetst nominaal van aard zijn. Een coëfficiënt van boven de 0,8 is altijd acceptabel, boven de 0,6 is in sommige gevallen acceptabel en beneden de 0,6 is onacceptabel (Neuendorf et al., 2017). De resultaten van de betrouwbaarheidsanalyse zijn weergegeven in bijlage 4. De intercodeurbetrouwbaarheid was over het algemeen hoog. De laagste Cohen's Kappa werd gevonden voor de variabele "toon" ($\kappa = 0{,}662$), wat nog steeds boven de grens van acceptabele betrouwbaarheid valt. Voor alle andere variabelen was sprake van een substantiële tot uitstekende overeenkomst tussen de eerste en tweede codeur. In twee gevallen was zelfs sprake van volledige overeenstemming ($\kappa = 1{,}000$), namelijk bij de tweede en derde neutralisatietechniek. Bij deze volledige overeenstemming moet wel de kanttekening worden geplaatst dat het hier om weinig voorkomende coderingen ging; zes advertenties bevatten een tweede neutralisatietechniek en één advertentie bevatte een derde neutralisatietechniek. De uitkomsten van de betrouwbaarheidsanalyse geven weer dat de coderingen met hoge onderlinge overeenstemming zijn uitgevoerd.

In het codeerformulier zijn de advertentienummers van de advertenties uit de steekproef toegevoegd. Er zijn zowel kwantitatieve als kwalitatieve invulvelden toegevoegd aan het codeerformulier (bijlage 6). In de open tekstvelden voor het kwalitatieve onderzoek is of een citaat of een eigen interpretatie gegeven. Bij iedere gebruikte neutralisatietechniek is alle tekst genoteerd die is toe te schrijven aan het gebruiken van de techniek. Bij de framing van de aanbieder en het doelwit is een eigen interpretatie gegeven. Hierbij geeft de codeur in eigen woorden een korte beschrijving van hoe de aanbieder zichzelf presenteert en hoe het doelwit van de advertentie werd afgebeeld of gelegitimeerd. Omdat framing impliciet en verspreid in de tekst aanwezig kan zijn, werd hier niet om een citaat, maar om een interpretatie gevraagd. Als in de advertentie geen specifiek doelwit werd benoemd, worden de velden over type doelwit en framing van het doelwit overgeslagen. Deze citaten en interpretaties werden later gebruikt in de kwalitatieve analyse om inzicht te krijgen in hoe neutralisatietechnieken worden vormgegeven en om theoretische patronen toe te lichten met voorbeelden uit de data.

3.4 Operationalisatie van de variabelen

Om het kwantitatieve gedeelte van het onderzoek uit te voeren, zijn de theoretische concepten omgezet naar meetbare variabelen. Alle handmatig gecodeerde variabelen en hun definities, categorieën en voorbeeldquotes zijn vastgelegd in het codeboek in bijlage 5. Een kleiner gedeelte van de variabelen is na afloop toegevoegd op basis van de ingevulde waarden tijdens het codeerproces. Hoe deze bewerkingen zijn uitgevoerd in SPSS wordt weergegeven in bijlage 9. Bij iedere vraag zijn ook de

opties “Anders” en “Niet mogelijk om te bepalen” beschikbaar, zodat ook bij afwijkende en onduidelijke gevallen een passende antwoordmogelijkheid gegeven kon worden (Neuendorf et al., 2017).

In het onderzoek is ten eerste vastgesteld of bepaalde advertentiekenmerken wel of niet aanwezig waren in de advertenties. De beschikbare categorieën zijn gekozen op basis van de afbakeningen van het onderzoek en de kenmerken die in de literatuur zijn gevonden. Er is vastgesteld op welk platform de advertentie is geplaatst, waarbij kon worden gekozen tussen het dark web en Telegram. Dit zijn ook de enige platforms waarvan data is verzameld in dit onderzoek. Ook is de taal vastgesteld, waarbij kon worden gekozen voor een hoofzakelijk Nederlandse of hoofdzakelijk Engelse tekst. Omdat sommige Nederlandse advertenties bijvoorbeeld ook Engelse termen kunnen bevatten, is ervoor gekozen om de hoofdzakelijke taal van de advertentie te coderen. Er is ook een variabele toegevoegd die het aantal woorden per advertentie weergeeft, dit werd automatisch berekend aan de hand van de originele advertentietekst.

Verder is er gekeken naar het gebruiken van aanvullende strategieën in de advertenties, te beginnen met de toon. Hierbij werd onderscheid gemaakt tussen een zakelijke of informele toon, wat laat zien of de aanbieder via de toon poogt om het aanbod op een legitieme manier over te brengen (Ridley & Selck-Paulsson, 2022). Er is ook ingevuld welke aanspreekvorm de aanbieder heeft gebruikt in de advertentie, waarbij gekozen kon worden tussen de “jij-vorm”, de “wij-vorm” of een combinatie van beide vormen. Hiermee kon met een nieuwe variabele worden vastgesteld of de aanbieder een groepsgevoel probeert te creëren in de advertentie. Hierbij zijn de advertenties waarin de “wij-vorm” als aanspreekvorm wordt gebruikt afgezet tegen de advertenties die de “jij-vorm” als aanspreekvorm gebruiken. Volgens de literatuur kan het creëren van een groepsgevoel namelijk het delict als normaal presenteren, waardoor kopers het gevoel hebben dat zij conformeren aan de geldende groepsnormen (Cialdini, 2021).

Vervolgens zijn er drie verschillende variabelen die vaststellen of er sprake was van alternatieve overtuigingsstrategieën in een advertentie: de aanwezigheid van reputatie, de aanwezigheid van een klantenservice en de aanwezigheid van kortingen en/of promoties. Deze overtuigingsstrategieën zijn vastgesteld aan de hand van eerder onderzoek. Deze drie technieken zijn eerder geïdentificeerd in advertenties op het dark web als manieren waarmee de aanbieder de eigen positie probeert te versterken ten opzichte van concurrentie (Fisher et al., 2025; Przepiorka et al., 2017).

Bij het vaststellen van de neutralisatietechnieken waren er twaalf categorieën, gebaseerd op de technieken van Kaptein & Van Helvoort (2019). De aanwezigheid van de neutralisatietechnieken is tijdens het coderen geïdentificeerd aan de hand van de gegeven definities en voorbeelden in het codeboek. Er konden tot maximaal vijf verschillende neutralisatietechnieken worden geïdentificeerd per advertentie. Aan de hand van het aantal neutralisatietechnieken dat werd ingevuld, is achteraf een nieuwe variabele gemaakt die weergeeft of er wel of geen neutralisatietechnieken zijn toegepast per

advertentie. Ook is er nog een variabele toegevoegd die per advertentie telt hoeveel verschillende overtuigingsstrategieën er zijn toegepast. Dit omvat de optelsom van het gebruik van neutralisatietechnieken, reputatieverwijzingen, klantenservices en kortingen/promoties.

Er is ook voor iedere advertentie vastgesteld of er werd verwezen naar een specifiek type doelwit. Indien er wel werd verwezen naar en specifiek type doelwit, is ook vastgesteld welk type doelwit dit betrof. Dit is onderverdeeld in de categorieën particulier, bedrijf of overheidsinstantie en de combinaties hiertussen. Deze verschillende typen weerspiegelen de vermeende afstand tussen de aanbieder en koper tot het doelwit. Bij een particulier doelwit is deze afstand klein en bij bedrijven en overheidsinstanties is de afstand groter (Brewer et al., 2020). Op basis hiervan is uiteindelijk nog een variabele toegevoegd die de advertenties met particuliere doelwitten afzet tegen advertenties met niet-particuliere doelwitten en advertenties zonder doelwitverwijzing.

Bij het type aanbieder is vastgesteld in welke categorie de aanbieder valt op basis van diens zelfpresentatie. In totaal zijn tien typen vastgesteld, waaronder enkelvoudige categorieën als “crimineel” of “expert” en gecombineerde vormen als “crimineel en ondernemer” of “expert en mentor”. Deze typen zijn vastgesteld aan de hand van de bestaande literatuur, die bijvoorbeeld liet zien dat sommige aanbieders zoveel mogelijk legitieme aanbieders proberen te imiteren (Ridley & Selck-Paulsson, 2022) en dat aanbieders soms verwijzen naar hun eigen expertise om betrouwbaarheid uit te stralen (Laferrière & Décary-Hétu, 2023). Zo vielen de aanbieders die zichzelf voordoen als legitieme aanbieders onder het type “ondernemer” en aanbieders die zichzelf presenteerden als technische experts met veel vaardigheden onder het type “expert”. Aanbieders die het criminele karakter van het aanbod duidelijk naar voren lieten komen in de advertentie vallen onder het type “crimineel” en aanbieders die de nadruk legden op het ondersteunen en opleiden van potentiële klanten onder het type “mentor”. Aanbieders die meerdere van deze typen lieten zien kregen een gecombineerde vorm toegewezen. Achteraf is dit opgedeeld in vier individuele variabelen, zodat de verschillende aanbiederstypes onderling vergeleken konden worden.

Er zijn verder negentien verschillende aangeboden diensten/producten geïdentificeerd, zoals beschreven in bijlage 1. Een gedeelte hiervan is van tevoren opgesteld aan de hand van de literatuur, andere categorieën zijn tijdens de testronde van het coderen toegevoegd. Op basis hiervan is achteraf een variabele toegevoegd die laat zien hoeveel diensten en producten er in totaal werden aangeboden per advertentie. Ook is er een variabele toegevoegd die de moeilijkheidsgraad van het aangeboden delict weergeeft. De indeling van de het aanbod in de categorieën “eenvoudig”, “gecompliceerd” of “beide” is ook gebaseerd op de tabel in bijlage 1. Diensten en producten waarbij de koper zelf nog weinig kennis nodig heeft en weinig stappen zelf hoeft af te ronden, vallen onder eenvoudige delicten. Als de koper na aankoop nog wel handelingen moet verrichten en daarvoor ook geavanceerdere kennis nodig heeft, valt het aanbod onder “gecompliceerd”. In sommige gevallen werden er zowel eenvoudige als gecompliceerde delicten aangeboden in dezelfde advertentie, waardoor het viel onder de categorie “beide”.

3.5 Data-analyse

Aan de hand van alle gegevens die zijn ingevuld tijdens het codeerproces, is er een dataset opgebouwd die zowel alle kwantitatieve als kwalitatieve data bevat. De kwantitatieve data is gebruikt om een SPSS-dataset van te maken. Deze dataset is gebruikt om de kwantitatieve analyses mee uit te voeren. Er is een bivariate analyse uitgevoerd aan de hand van correlaties, kruistabellen en chi-kwadraattoetsen, waarin is gekeken naar de samenhang tussen de variabelen. Er is ook een multivariate analyse uitgevoerd aan de hand van een logistische regressieanalyse, om te onderzoeken welke variabelen samenhangen met de kans op het gebruik van neutralisatietechnieken in een advertentie. De keuze voor een logistische regressieanalyse is gemaakt op basis van de aard van de afhankelijke variabele. Het gebruik van neutralisatietechnieken heeft de mogelijkheden “ja” en “nee”. Dit maakt de logistische regressieanalyse geschikt om de kans op het gebruiken van neutralisatietechnieken te bepalen met meerdere voorspellers. Een alternatief was om het aantal neutralisatietechnieken per advertentie als afhankelijke variabele te nemen, maar deze variabele is erg scheef verdeeld en zou daardoor de betrouwbaarheid van de resultaten beperken. Dit maakt het gebruik van neutralisatietechnieken het meest geschikt als afhankelijke variabele. Aan de hand van deze logistische regressieanalyse zijn ook de drie gestelde hypothesen getoetst. Hierbij is gelet op de significantieniveaus en de odds ratio’s om de sterkte en richting van de relaties te interpreteren.

De logistische regressieanalyse is in drie blokken uitgevoerd. De blokken zijn ingedeeld op basis van hun theoretische betekenis. In het eerste blok zijn de basiskenmerken van de advertenties opgenomen: het platform, het aantal woorden en het aantal aangeboden diensten/producten. In het tweede blok zijn de variabelen toegevoegd die de communicatiestijl van de aanbieder weergeven: groepsgevoel, toon, type doelwit en moeilijkheidsgraad. In het derde blok zijn de variabelen toegevoegd die iets zeggen over hoe de aanbieder zichzelf presenteert: het type aanbieder en de aanwezigheid van klantenservices, reputatieverwijzingen en kortingen/promoties. Deze indeling van de blokken maakt het mogelijk om stapsgewijs te onderzoeken hoe de verschillende lagen van de advertentie bijdragen aan de kans op het gebruik van neutralisatietechnieken. Eerst worden de meer algemene en vorm gerelateerde variabelen getoetst en later de meer strategische kenmerken.

De kwalitatieve data is op een verkennende wijze geanalyseerd. Hierbij is gezocht naar terugkerende formuleringen, overtuigingsstrategieën en variaties in de toon en de framing. Aan de hand hiervan konden de kwantitatieve bevindingen worden verdiept.

3.6 Ethische overwegingen

De verzamelde data is afkomstig uit openbare bronnen die voor iedereen beschikbaar zijn. Vanwege de openbare beschikbaarheid is het niet nodig om toestemming te vragen van de aanbieders om data te verzamelen. De verzamelde data bestaat niet uit persoonsgegevens, maar uit anonieme gegevens die niet herleidbaar zijn naar een persoon. Gebruikersnamen van aanbieders worden wel opgeslagen, maar

omdat aanbieders gebruikmaken van pseudoniemen is er geen sprake van identificeerbaarheid. De anonimiteit van de aanbieders wiens advertenties worden geanalyseerd is dus gewaarborgd.

Om de eigen veiligheid tijdens de dataverzameling ook te waarborgen, is er goed op gelet dat er geen eigen persoonsgegevens beschikbaar zijn gesteld voor criminelen. Er zijn geen accounts aangemaakt op dark websites en er is niet deelgenomen aan Telegram-groepen om zo meer advertenties te kunnen verkrijgen. Er is ook geen interactie geweest met andere gebruikers of criminelen/aanbieders. Daarnaast is het dark web uitsluitend bezocht met gebruik van een laptop met een VPN-verbinding, zodat de online activiteiten niet traceerbaar zijn. Om het dark web te bezoeken is de TOR-browser gedownload, welke openbaar beschikbaar is en ook extra veiligheidsmaatregelen biedt aan gebruikers.

Alle verzamelde data is opgeslagen op een beschermde schijf bij het RIEC Noord-Nederland. Alle medewerkers van RIEC Noord-Nederland hebben toegang tot deze schijf. De verzamelde data zal uitsluitend gebruikt worden voor deze masterscriptie en wordt niet gedeeld met derden. Om de data beschikbaar te stellen voor de tweede codeur is het tijdelijk op een USB-stick geplaatst, waarna de data weer van de USB-stick is verwijderd. Na afronding van het onderzoek worden de gegevens op een veilige manier verwijderd volgens de richtlijnen van het RIEC Noord-Nederland.

Hoofdstuk 4: Resultaten

In dit hoofdstuk worden de resultaten van het onderzoek gepresenteerd. Allereerst worden de beschrijvende analyses besproken, waarin de gemeten variabelen uit de Cybercrime-as-a-Service-advertenties worden beschreven en weergegeven. Vervolgens worden de resultaten van de bivariate en multivariate analyses besproken die zijn uitgevoerd om de gestelde hypothesen te toetsen en om op exploratieve wijze mogelijke verbanden te ontdekken. Tot slot wordt de kwalitatieve analyse besproken die is uitgevoerd om een beter beeld te geven van de context waarin het aanbod plaatsvindt en de neutralisatietechnieken worden toegepast.

4.1 Beschrijvende analyse

4.1.1 Algemene advertentiekenmerken

De univariate beschrijvende statistieken van de variabelen die de algemene kenmerken van de advertenties weerspiegelen worden weergegeven in tabel 1. De geanalyseerde advertenties hadden een gemiddeld aantal woorden van 174,55, met een minimum van 2 woorden en een maximum van 1.128 woorden. De spreiding is groot, wat ook blijkt uit de standaarddeviatie van 165,32 woorden die bijna net zo hoog is als het gemiddelde. Dit duidt op veel variatie in het aantal woorden per advertentie. Verder werden er in de advertenties gemiddeld 1,44 diensten en/of producten aangeboden. Hoewel er in enkele gevallen tot wel 8 verschillende diensten en/of producten in één advertentie werden aangeboden, blijkt uit de kwartielen dat het in de meeste advertenties slechts om één dienst of product ging.

Verder is in tabel 1 te zien dat de meeste advertenties voornamelijk Engelstalig waren (83,20%) en een kleiner gedeelte voornamelijk Nederlandstalig was (16,80%). Wat ook opvalt is dat het overgrote deel van de aanbieders een dienst en/of product aanbiedt die een eenvoudig delict representeert. Maar liefst 88,9 procent van de aanbieders bood een eenvoudig delict aan, waarvan 82,7 procent bestond uit enkel het aanbod van een eenvoudig delict en in 6,2 procent van de gevallen werd het aanbod gecombineerd met dat van een gecompliceerd delict. Het creëren van groepsgevoel is gebaseerd op de gehanteerde aanspreekvorm. In ongeveer een derde van de advertenties is de potentiële koper aangesproken met de “wij-vorm”, waarbij het beeld wordt geschept dat er een grotere groep bestaat in de context van de aankoop (31,7%). Bij de overige advertenties was hier geen sprake van, wat betekent dat de koper werd aangesproken in de “jij-vorm” of dat er helemaal geen sprake was van een aanspreekvorm in de advertentie (68,3%). Tot slot was de toon van de advertentie in de meeste gevallen zakelijk (74,00%) en in ongeveer een kwart van de advertenties informeel (26,00%).

Tabel 1: Univariate beschrijvende statistieken van variabelen met algemene advertentiekenmerken (n = 369)

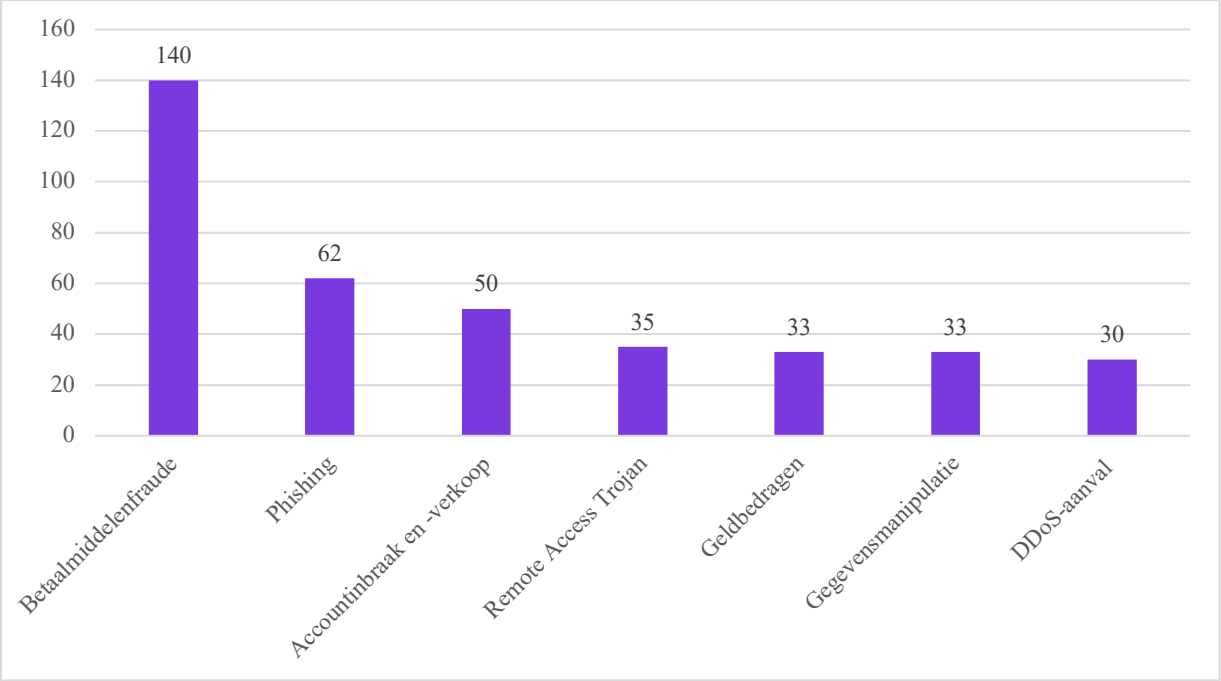
Variabele	Gemiddelde (standaarddeviatie)*	Minimum	Maximum	Eerste kwartiel	Mediaan	Derde kwartiel
Totaal aantal woorden	174,55 (165,32)	2,00	1128,00	72,00	138,00	233,50
Aantal aangeboden diensten/producten per advertentie	1,44 (1,20)	1,00	8,00	1,00	1,00	1,00
Taal (Engels=0, Nederlands=1)	83,20% Engels 16,80% Nederlands					
Moeilijkheidsgraad delict (eenvoudig=1, gecompliceerd=2, beide=3)	82,70% eenvoudig 11,10% gecompliceerd 6,20% beide					
Groepsgevoel (0=nee, 1=ja)	68,3% nee 31,7% ja					
Toon (zakelijk=0, informeel=1)	74,00% zakelijk 26,00% informeel					

*Bij nominale variabelen is de frequentieverdeling vermeld in percentages

4.1.2 Aangeboden diensten en/of producten

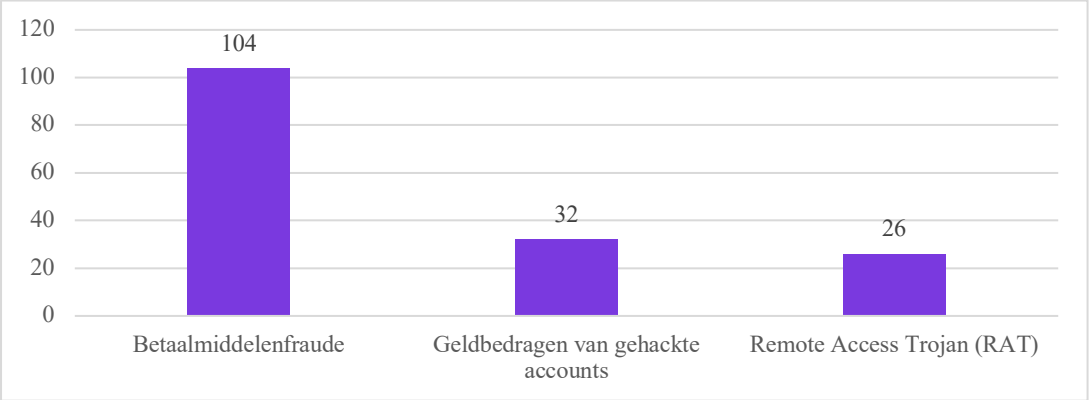
In figuur 2 wordt een overzicht gegeven van de diensten en producten die het vaakst werden aangeboden in alle advertenties. De dienst die verreweg door de meeste aanbieders werd aangeboden is betaalmiddelenfraude, dit kwam naar voren in 140 advertenties (37,94%). Daarna kwam phishing het meest voor in 62 advertenties (16,80%). Ook het aanbod van accountinbraak- en verkoop kwam vaak voor, namelijk in 50 van de advertenties (13,55%). Het aanbod van een Remote Access Trojan, geldbedragen van gehackte accounts, gegevensmanipulatie in bestaande systemen en DDoS-aanvallen kwamen ongeveer evenveel voor, variërend tussen de 35 en de 30 keer. Alle overige diensten en producten kwamen minder dan 30 keer voor in de advertenties. Een figuur met het volledige overzicht van de frequenties alle diensten en producten die zijn aangeboden, kan worden gevonden in bijlage 7 (figuur 7.1).

Figuur 2: De zeven meest aangeboden diensten/producten in de advertenties (n = 369)



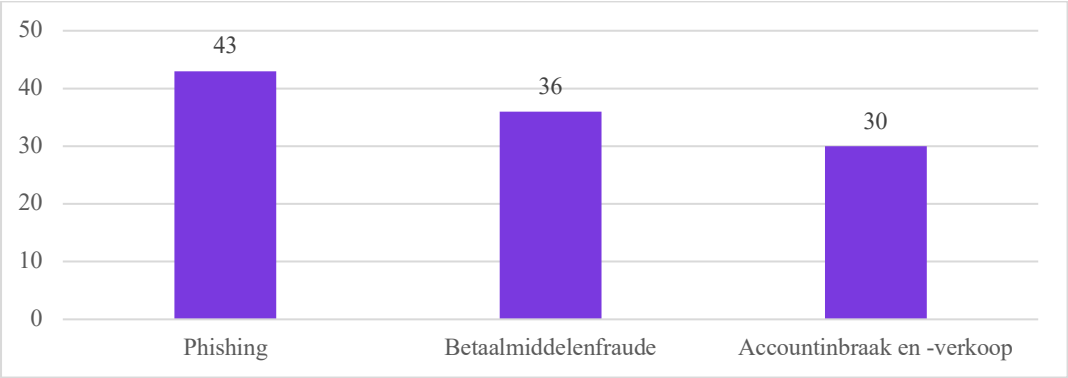
Welke dienst of product het meest werd aangeboden verschilt per platform. In figuur 3 worden de drie meest aangeboden diensten en/of producten op het dark web weergegeven. Hier is te zien dat betaalmiddelenfraude nog steeds bovenaan staat, gevonden in 104 advertenties (39,69%). De diensten/producten die daarna volgen zijn anders dan in het totale aanbod. Op de tweede plaats staat nu het aanschaffen van geldbedragen van gehackte accounts in 32 advertenties (12,21%), gevolgd door de Remote Access Trojan in 26 advertenties (9,92%). Het volledige overzicht van het aanbod op het dark web is te vinden in bijlage 7 (figuur 7.2).

Figuur 3: De drie meest aangeboden diensten/producten op het dark web (n = 262)



In figuur 4 worden de drie meest aangeboden diensten en/of producten op Telegram weergegeven. Hier is phishing de meest aangeboden dienst in 43 advertenties, wat betekent dat het in bijna de helft van alle advertenties op Telegram is aangeboden (40,19%). Betaalmiddelenfraude is op Telegram ook nog een van de meest aangeboden diensten, dit kwam in 36 advertenties voor en komt daarmee op de tweede plaats (33,64%). Op de derde plaats staat accountinbraak en -verkoop, dit werd in ongeveer één op de tien advertenties aangeboden (11,45%). Het volledige overzicht van het aanbod op Telegram kan ook worden gevonden in bijlage 7 (figuur 7.3).

Figuur 4: De drie meest aangeboden diensten/producten op Telegram (n = 107)



4.1.3 Neutralisatietechnieken

Wat betreft de toepassing van neutralisatietechnieken is te zien in tabel 2 dat dit varieerde van 0 tot maximaal 3 per advertentie, met een gemiddelde van 0,40 neutralisatietechnieken per advertentie. De kwartielverdeling laat zien dat in het overgrote deel van de advertenties geen neutralisatietechnieken zijn toegepast: in 70,7 procent van de gevallen zijn er geen technieken aangetroffen. In de overige 29,3 procent van de advertenties kwam wel één of meer neutralisatietechnieken voor, wat betekent dat bijna drie op de tien advertenties gebruikmaakt van neutralisaties.

Tabel 2: Univariate beschrijvende statistieken van variabelen over neutralisatietechnieken (n = 369)

Variabele	Gemiddelde (standaarddeviatie)*	Minimum	Maximum	Eerste kwartiel	Mediaan	Derde kwartiel
Aantal neutralisatietechnieken per advertentie	0,40 (0,68)	0,00	3,00	0,00	0,00	1,00
Gebruik neutralisatie-technieken (Nee=0, Ja=1)	70,70% nee 29,30% ja					

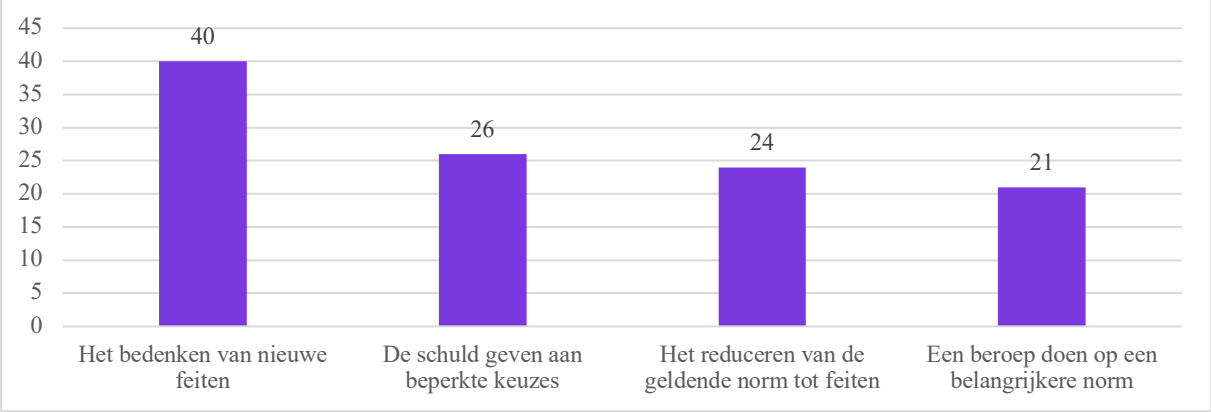
*Bij nominale variabelen is de frequentieverdeling vermeld in percentages

Het overzicht van de neutralisatietechnieken die het meest zijn gebruikt in alle advertenties staat in figuur 5. Hier is te zien dat één neutralisatietechniek aanzienlijk vaker is gebruikt dan de andere technieken: het bedenken van nieuwe feiten. Deze techniek werd het meest gebruikt om te stellen dat het aanbod niet is bedoeld voor criminele doeleinden maar voor educatieve of andere legitieme doeleinden zoals online marketing, of door te stellen dat het aanbod helemaal niet crimineel van aard is maar dat het een legitieme manier is om geld te verdienen. In sommige gevallen werd ook een alternatief scenario geschetst waarin het delict rechtvaardig leek.

De drie neutralisatietechnieken die daarna het vaakst zijn gebruikt, liggen qua frequentie dichter bij elkaar, van 26 tot 21 keer. Deze aantallen zijn hoog in vergelijking met de overige neutralisatietechnieken, die minder dan vijftien keer voorgekomen zijn.

Van de twaalf technieken zijn er twee helemaal niet voorgekomen, namelijk het relativeren van de normoverschrijding en het verschuilen achter onvolmaakte kennis. Het volledige overzicht van alle gebruikte neutralisatietechnieken staat in bijlage 7 (tabel 7.4). Verdere inzichten over het gebruik van deze neutralisatietechnieken worden gegeven in paragraaf 4.3.

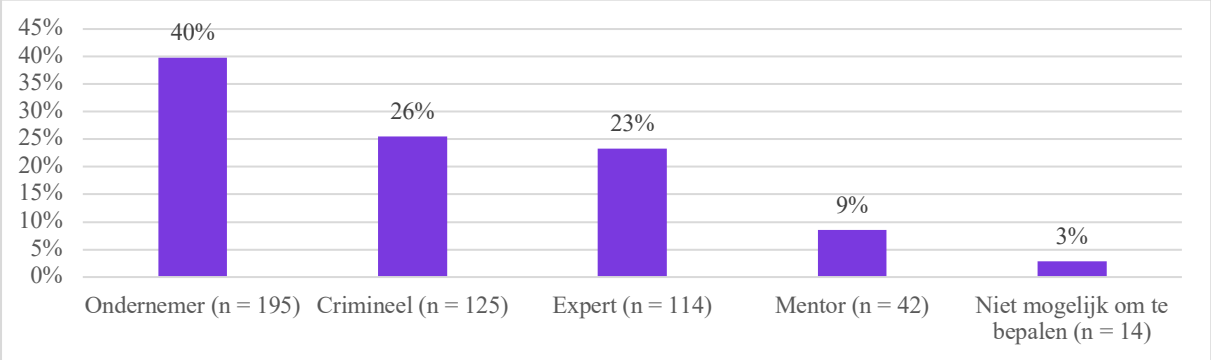
Figuur 5: De vier meest gebruikte neutralisatietechnieken in de advertenties (n = 369)



4.1.4 Type aanbieder

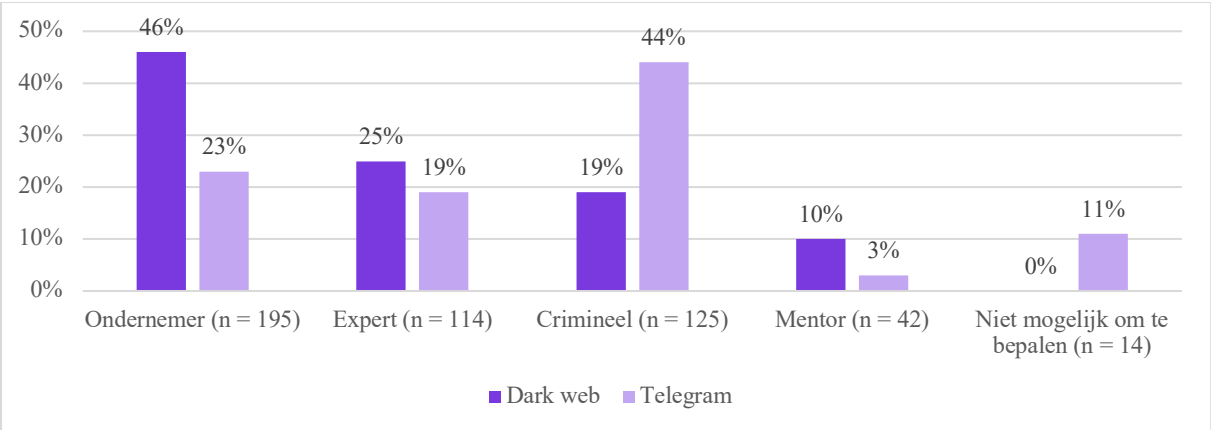
In de advertenties was “ondernemer” het type aanbieder dat het meest voorkwam, namelijk in 40 procent van alle advertenties, zoals te zien is in figuur 6. De typen “crimineel” en “expert” kwamen ongeveer even vaak voor, waarbij 26 procent van de aanbieders viel onder crimineel en 23 procent onder expert. Het type “mentor” is het minst vaak voorgekomen, in 9 procent van de advertenties. In 3 procent van de advertenties was het niet mogelijk om een type vast te stellen. De figuur met alle originele uitsplitsingen die zijn gebruikt tijdens het coderen is terug te vinden in bijlage 7 (tabel 7.5).

Figuur 6: De type aanbieders in de advertenties (n = 369)



Wanneer het type aanbieder wordt uitgesplitst per platform, zoals weergegeven in figuur 7, valt op dat er duidelijke verschillen zijn tussen het dark web en Telegram. Op het dark web was de ondernemer het meest voorkomende type aanbieder (46%), terwijl op Telegram juist de criminele aanbieder het meest voorkwam (44%). Opvallend is bovendien dat alle advertenties waarbij het type aanbieder niet kon worden vastgesteld afkomstig zijn van Telegram. Dit kan worden verklaard aan de hand van het verschil in het gemiddelde woordenaantal tussen de platforms. Telegram-advertenties bevatten gemiddeld slechts 61 woorden, tegenover gemiddeld 221 woorden op het dark web. Op Telegram was het woordenaantal van sommige advertenties zo beperkt dat er geen type aanbieder kon worden vastgesteld.

Figuur 7: De type aanbieders in de advertenties, uitgesplitst per platform (n = 369)

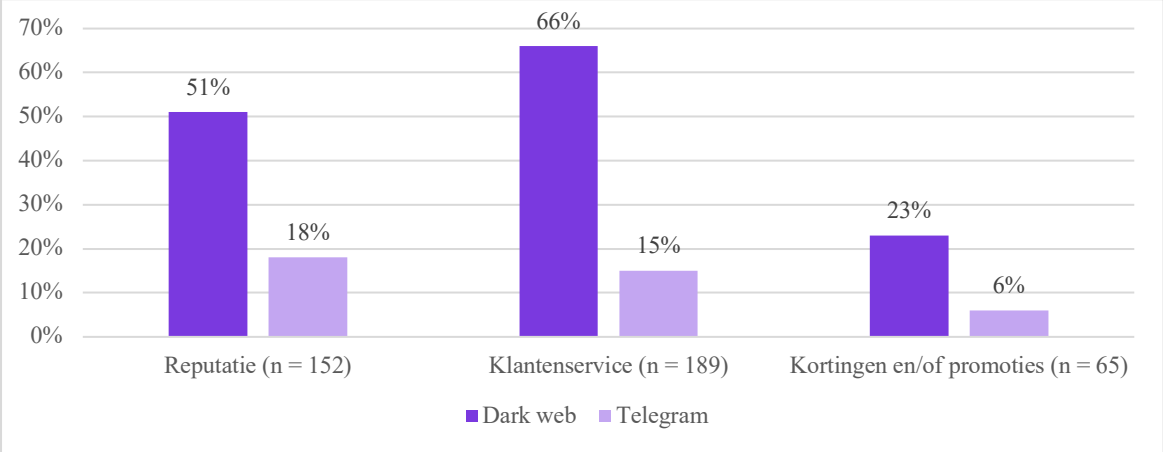


4.1.5 Alternatieve overtuigingsstrategieën

Het gebruik van alternatieve overtuigingsstrategieën is bijgehouden, namelijk het verwijzen naar de eigen positieve reputatie, het bieden van een klantenservice en van kortingen en/of promoties. Vooral het verwijzen naar de eigen reputatie en het bieden van een klantenservice werd door veel aanbieders gebruikt. In vier op de tien advertenties verwees de aanbieder naar de eigen positieve reputatie of betrouwbaarheid (41,19%) en in de helft van alle advertenties werd een klantenservice aangeboden ter ondersteuning van de koper (51,22%). Het bieden van kortingen en/of promoties kwam minder vaak voor, maar werd toch in bijna twee op de tien advertenties gevonden (17,62%).

In figuur 8 is te zien dat deze overtuigingsstrategieën vooral werden gebruikt door aanbieders op het dark web. In meer dan de helft van de advertenties op het dark web werd verwezen naar reputatie (51,00%) en in 66 procent van de advertenties werd een klantenservice geboden. Kortingen en/of promoties waren in ongeveer twee op de tien advertenties aanwezig (23,00%). Op Telegram werden deze overtuigingsstrategieën aanzienlijk minder vaak toegepast. In 18 procent van de advertenties werd naar reputatie verwezen en in 15 procent van de advertenties werd een klantenservice geboden. Kortingen en/of promoties kwamen zelden voor, maar in 6 procent van de advertenties.

Figuur 8: De aanwezigheid van alternatieve overtuigingsstrategieën in advertenties (n = 369)



4.2 Kwantitatieve analyse

In deze paragraaf worden zowel de eerder opgestelde hypothesen getoetst als op exploratieve wijze patronen in de data onderzocht. De hypothesen zijn gebaseerd op bestaande literatuur over neutralisatietechnieken en de context waarin online criminaliteit zich afspeelt. Tegelijkertijd worden er nieuwe patronen en associaties onderzocht op exploratieve wijze, omdat veel aspecten van de manier waarop CaaS-aanbieders hun diensten aanbieden nog onvoldoende in kaart zijn gebracht. Het doel van de exploratieve analyse is dan ook om tekortkomingen in de huidige kennis te vullen door inzicht te krijgen in hoe het gebruik van neutralisatietechnieken samenhangt met verschillende kenmerken van advertenties en aanbieders, zoals de rol die aanbieders aannemen, de toon van de advertentie en het gebruiken van alternatieve overtuigingsstrategieën zoals reputatie. Door deze verbanden te analyseren en in kaart te brengen, wordt duidelijker hoe CaaS-aanbieders in hun advertenties communiceren en hun aanbod overtuigend presenteren.

Ten eerste is er gekeken naar de bivariate statistieken tussen alle variabelen die zijn opgenomen in de regressieanalyse. De resultaten hiervan worden weergegeven in tabel 3 (blz. 41). Op basis hiervan kunnen een aantal verbanden alvast exploratief worden geanalyseerd. Wat opvalt is dat het gebruikte platform significant samenhangt met alle andere variabelen in het model. Dit wijst op veel variatie in het aanbod en de presentatie van advertenties tussen het dark web en Telegram. Zo zijn Telegram-advertenties aanzienlijk vaker Nederlandstalig dan dark web-advertenties, die uitsluitend Engelstalig zijn ($X^2(1, N = 369) = 182{,}472$, $p < 0{,}001$). Dit verschil kan mogelijk verklaard worden door de aard van de platforms. Het dark web richt zich op een internationaal publiek, waardoor Engels de standaardtaal is om zo veel mogelijk gebruikers te bereiken. Openbare groepen op Telegram worden daarentegen vaker gebruikt binnen kleinere, lokale groepen, waar men vaker de eigen taal gebruikt. Ook gebruiken advertenties op Telegram significant minder woorden dan advertenties op het dark web ($r = -0{,}440$, $p < 0{,}001$). Daarnaast zijn er verschillen in de toon en aanspreekvorm zichtbaar: op het dark web creëren aanbieders vaker een groepsgevoel via de gebruikte aanspreekvorm ($X^2(1, N = 369) = 40{,}861$, $p < 0{,}001$) en hanteren zij vaker een zakelijke toon dan aanbieders op Telegram ($X^2(1, N = 369) = 179{,}005$, $p < 0{,}001$). Wat betreft het soort aanbod blijkt dat gecompliceerde diensten en producten vaker voorkomen op het dark web ($X^2(1, N = 369) = 21{,}614$, $p < 0{,}001$). Tot slot komen alle drie de overtuigingsstrategieën (reputatie, klantenservice en kortingen/promoties) significant vaker voor op het dark web dan op Telegram.

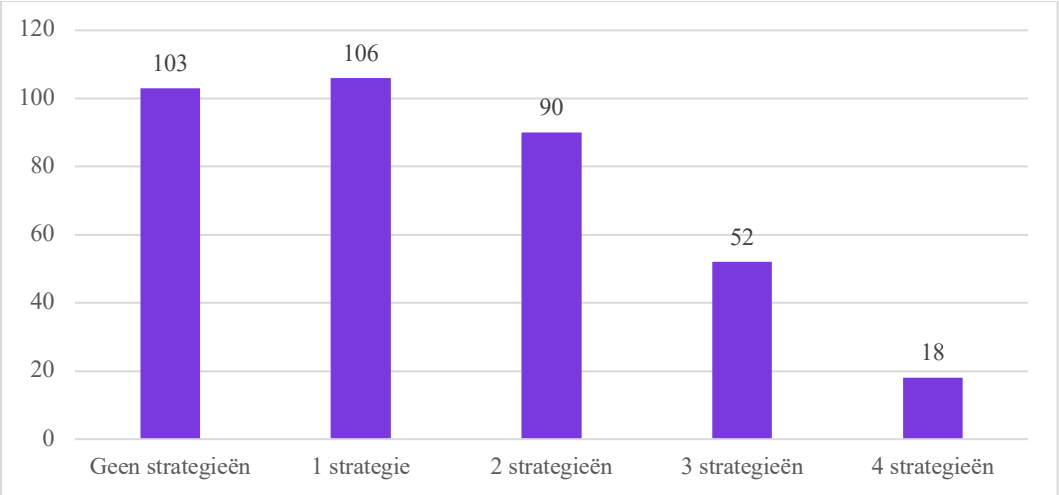
Neutralisatietechnieken komen significant vaker voor op het dark web ($X^2(1, N = 369) = 23{,}725$, $p < 0{,}001$) en in langere advertenties ($r = 0{,}358$, $p < 0{,}001$). Advertenties waarin een groepsgevoel wordt gecreëerd bevatten ook significant vaker neutralisatietechnieken ($X^2(1, N = 369) = 23{,}596$, $p < 0{,}001$). Aanbieders die zich richten op het creëren van collectieve identificatie lijken dus eerder geneigd om hun aanbod moreel te onderbouwen of verzachten via neutralisatietechnieken.

Daarnaast komen neutralisatietechnieken vaker voor in advertenties met een zakelijke toon dan in advertenties met een informele toon ($X^2(1, N = 369) = 5{,}629, p = 0{,}018$).

Criminele aanbieders gebruiken significant minder vaak neutralisatietechnieken dan andere aanbieders ($X^2(1, N = 369) = 17{,}723, p < 0{,}001$), terwijl mentors dit juist significant vaker doen ($X^2(1, N = 369) = 5{,}839, p = 0{,}016$). Bij ondernemers en experts zijn geen significante verschillen gevonden.

Verder is gekeken naar de samenhang tussen het gebruiken van neutralisatietechnieken en het gebruiken van alternatieve overtuigingsstrategieën: reputatie, klantenservice en kortingen en/of promoties. Voor alle drie de strategieën geldt dat als deze in een advertentie worden gebruikt, de advertentie significant vaker neutralisatietechnieken bevat. Dit kan betekenen dat deze aanbieders actief bezig zijn om hun aanbod zo legitiem en overtuigend mogelijk over te laten komen. Op basis hiervan is het ook te verwachten dat alternatieve overtuigingsstrategieën vaker in combinatie met elkaar worden gebruikt. Aanbieders die verwijzen naar hun eigen reputatie, bieden significant vaker een klantenservice aan ($X^2(1, N = 369) = 30{,}610, p < 0{,}001$) en bieden ook significant vaker kortingen en/of promoties aan ($X^2(1, N = 369) = 25{,}605, p < 0{,}001$). Ook tussen het bieden van een klantenservice en het bieden van kortingen en/of promoties is een significante samenhang gevonden ($X^2(1, N = 369) = 14{,}043, p < 0{,}001$). Om een goed beeld te kunnen geven van in hoeverre aanbieders meerdere overtuigingsstrategieën combineren, is een aanvullende analyse uitgevoerd waarin per advertentie het aantal gebruikte strategieën, inclusief neutralisatietechnieken, is geteld. Deze aantallen worden weergegeven in figuur 9. Hier is te zien dat ongeveer 72 procent van alle advertenties gebruik heeft gemaakt van minimaal één overtuigingsstrategie. Dit is ook getoetst aan de gehanteerde toon. Hieruit blijkt dat advertenties met een zakelijke toon significant vaker meerdere strategieën bevatten, terwijl informele advertenties in 63 procent van de gevallen geen enkele strategie gebruiken ($X^2(4, N = 369) = 82{,}275, p < 0{,}001$). Het inzetten van meerdere strategieën komt vrijwel uitsluitend voor in zakelijke advertenties.

Figuur 9: Het aantal gebruikte overtuigingsstrategieën per advertentie (n = 369)



Uit de analyse blijkt verder dat criminelen significant minder vaak gebruikmaken van overtuigingsstrategieën in vergelijking met de andere typen aanbieders ($X^2(4, N = 369) = 11{,}398$, $p = 0{,}022$). Van de advertenties waarin helemaal geen strategieën voorkomen, behoort 46 procent tot het type crimineel. De groep mentors maakt daarentegen significant vaker gebruik van overtuigingsstrategieën ($X^2(4, N = 369) = 35{,}281$, $p < 0{,}001$). Waar geen significant verschil was in het gebruiken van neutralisatietechnieken voor ondernemers, is er nu wel een significante associatie gevonden met het gebruiken van overtuigingsstrategieën. Ondernemers gebruiken significant vaker overtuigingsstrategieën in vergelijking met de andere typen aanbieders ($X^2(4, N = 369) = 53{,}324$, $p < 0{,}001$). Deze resultaten bevestigen de eerdere bevindingen dat het type aanbieder samenhangt met de mate van strategisch communiceren in een advertentie.

Het totale woordenaantal van de advertentie heeft ook significante samenhang met meerdere advertentiekenmerken. Zo is er een significante, negatieve correlatie gevonden tussen het aantal woorden en de gehanteerde toon ($r = -0{,}344$, $p < 0{,}001$). Dit betekent dat de advertenties met een zakelijke toon gemiddeld langer zijn dan advertenties met een informele toon. Mogelijk proberen aanbieders met een zakelijke toon hun professionaliteit te benadrukken door meer informatie te geven.

Het aantal diensten/producten dat wordt aangeboden in een advertentie heeft ook een significante samenhang met enkele advertentiekenmerken. Criminelen en experts bieden significant meer producten aan ($r = 0{,}113$, $p = 0{,}30$; $r = 0{,}164$, $p = 0{,}002$), terwijl ondernemers juist significant minder producten aanbieden ($r = -0{,}176$, $p < 0{,}001$). Dit suggereert dat criminelen en experts hun aanbod breder presenteren, terwijl ondernemers zich juist vaker beperken tot een select aanbod.

Er is ook significante samenhang gevonden tussen het creëren van groepsgevoel in een advertentie en andere advertentiekenmerken. Advertenties die een groepsgevoel creëren door de wij-vorm te hanteren, hanteren vrijwel altijd een zakelijke toon. Slechts 6 procent van deze advertenties is informeel. Dit is een significante samenhang ($X^2(1, N = 369) = 35{,}722$, $p < 0{,}001$). Mogelijk proberen aanbieders via een zakelijke toon de groepsidentiteit overtuigender te brengen. Daarnaast creëren ondernemers significant vaker een groepsgevoel in advertenties dan de andere aanbiedertypen ($X^2(1, N = 369) = 24{,}687$, $p < 0{,}001$), terwijl experts dit juist significant minder vaak doen in vergelijking met de andere aanbiedertypen ($X^2(1, N = 369) = 6{,}035$, $p = 0{,}014$). Dit sluit aan bij het patroon waarin ondernemers zich in hun communicatie richten op het opbouwen van legitimiteit en betrouwbaarheid. Een gevoel van verbondenheid wordt mogelijk als strategisch middel ingezet om vertrouwen te stimuleren. Experts zijn daarentegen meer afstandelijk en leunen wellicht meer op hun technische autoriteit dan op sociale banden. Aanvullend hierop gebruiken aanbieders die een groepsgevoel creëren ook significant vaker reputatieverwijzingen ($X^2(1, N = 369) = 24{,}564$, $p < 0{,}001$) en kortingen/promoties ($X^2(1, N = 369) = 6{,}071$, $p = 0{,}014$). Dit versterkt het idee dat het creëren van een groepsgevoel strategisch wordt ingezet om de morele drempel te verlagen.

Tabel 3: Bivariate beschrijvende statistieken van alle variabelen die zijn opgenomen in de analyse (n = 369)

	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.
1. Gebruik neutralisaties	-	-0,254**	-0,114*	0,358**	-0,025	0,253**	-0,124*	0,096	0,219**	-0,072	0,086	0,126*	0,200**	0,127*	0,187**
2. Platform		-	0,703**	-0,440**	0,253**	-0,333**	0,696**	0,242**	0,237**	-0,342**	-0,130*	-0,154**	-0,304**	-0,464**	-0,201**
3. Taal			-	-0,308**	-0,083	-0,288**	0,642**	0,188**	0,184**	-0,200**	-0,238**	-0,093	-0,185**	-0,373**	-0,151**
4. Aantal woorden				-	-0,037	0,217**	-0,344**	0,173**	-0,008	0,195**	0,085	0,255**	0,412**	0,476**	0,408**
5. Aantal diensten/ producten					-	-0,098	0,054	0,320**	0,113*	-0,176**	0,164**	-0,098	-0,081	-0,068	-0,071
6. Groepsgevoel						-	-0,311**	0,113	-0,032	0,259**	-0,128*	-0,006	0,258**	0,094	0,128*
7. Toon							-	0,155*	0,267**	-0,318**	-0,168**	-0,115*	-0,308**	-0,410**	-0,193**
8. Moeilijkheids-graad								-	0,128*	0,227**	0,356**	0,097	0,034	0,174**	0,018
9. Crimineel									-	-0,345**	-0,169**	-0,022	-0,122*	-0,246**	-0,030
10. Ondernemer										-	-0,367**	-0,174**	0,272**	0,327**	0,266**
11. Expert											-	-0,129*	0,024	0,054	-0,140**
12. Mentor												-	0,168**	0,162**	0,237**
13. Reputatie													-	0,288**	0,263**
14. Klantenservice														-	0,195**
15. Kortingen															-

* significant bij p <0,05; ** significant bij p <0,01

Om de gevonden verbanden verder te toetsen, is aanvullend een logistische regressieanalyse uitgevoerd die onderzoekt welke kenmerken van advertenties significant bijdragen aan het gebruik van neutralisatietechnieken. De afhankelijke variabele is hier het gebruik van neutralisatietechnieken. Alle andere variabelen, behalve de taal, zijn aan het model toegevoegd als onafhankelijke variabelen. De resultaten van de regressieanalyse worden weergegeven in tabel 5 (blz. 46 & 47).

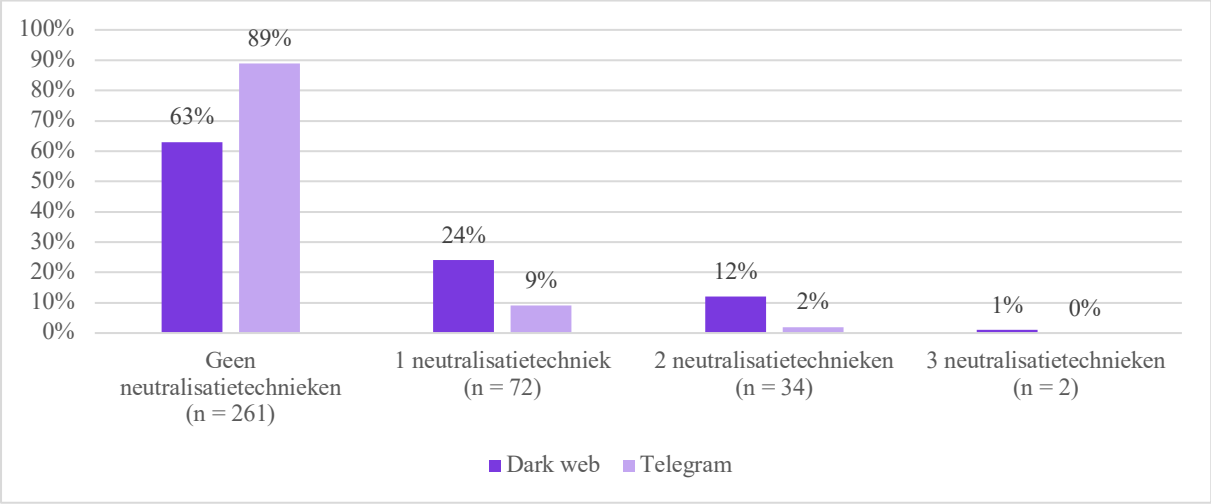
Het is belangrijk om allereerst stil te staan bij de modelkwaliteit. De geschiktheid van het regressiemodel is geëvalueerd aan de hand van de Hosmer-Lemeshowtoets, de Nagelkerke R^2 en de Log-Likelihood ratio. De Hosmer-Lemeshowtoets geeft aan of de geobserveerde uitkomsten significant afwijken van de door het model voorspelde waarden. Voor model 1 is de *p*-waarde 0,354, voor model 2 is de *p*-waarde 0,331 en voor model 3 is de *p*-waarde 0,336. Geen van de modellen laat hiermee een significante afwijking zien tussen de voorspelde en geobserveerde waarden, wat betekent dat ze goed bij de data passen. De Nagelkerke R^2-waarden laten zien dat elk model een groter gedeelte van de variantie in het gebruiken van neutralisatietechnieken verklaart. De waarden nemen toe van 0,194 in model 1 naar 0,273 in model 2 en uiteindelijk 0,336 in model 3. Met het complete model wordt dus 33,6 procent van de variantie in het gebruiken van neutralisatietechnieken verklaard. Gezien het exploratieve karakter van dit onderzoek is dit een substantieel percentage. Ook de Log Likelihood ratio ondersteunt de geschiktheid van het complete model. De daling in de waarden tussen model 1 en 3 wijst erop dat elk uitgebreider model een betere verklaring biedt voor de geobserveerde data. Deze toets bevestigt dat model 3 het best passende model is. De overige modelinspecties zijn uitgevoerd in bijlage 8. Aan alle assumpties is voldaan, alleen was er een te hoge multicollineariteit tussen het platform en de taal. De taal is daarom niet meegenomen in het regressiemodel.

In het eerste model zijn het platform, het totaal aantal woorden en het aantal aangeboden diensten/producten opgenomen als onafhankelijke variabelen. Hier is te zien dat het platform en het aantal woorden significante voorspellers zijn van het gebruik van neutralisatietechnieken. Met elk extra woord dat wordt toegevoegd aan de advertentie, neemt het gebruik van neutralisatietechnieken licht toe ($\text{Exp}(b) = 1{,}004$, $p < 0{,}001$). Hoewel het effect per woord klein is, kan dit bij langere advertenties toch een aanzienlijk verschil opleveren. Het aantal diensten en producten dat wordt aangeboden in de advertentie heeft geen significante invloed op het gebruik van neutralisatietechnieken. Dit komt overeen met de resultaten uit de bivariate analyse.

Aan de hand van dit eerste model kan de eerste hypothese worden getoetst, die luidde als volgt: “Telegram-advertenties bevatten meer neutralisatietechnieken dan dark web-advertenties”. Uit het eerste model blijkt dat het platform waarop de advertentie is geplaatst een significante voorspeller is van het gebruik van neutralisatietechnieken, met een odds-ratio van 0,401 ($p = 0{,}016$). Dit betekent dat de kans dat een Telegram-advertentie een neutralisatietechniek bevat ongeveer 60 procent lager is dan bij een advertentie op het dark web. Hiervan wordt ook een visuele weergave gegeven in figuur 10. Hier is te zien dat 37 procent van de dark web-advertenties ten minste één techniek bevatte. Op Telegram bevatte slechts 11 procent ten minste één techniek. Dit betekent dat de eerste hypothese niet

wordt ondersteund door de data. Er is juist sprake van het tegenovergestelde verband: advertenties op het dark web bevatten significant vaker neutralisatietechnieken dan advertenties op Telegram. Een mogelijke verklaring hiervoor zou kunnen zijn dat dark web advertenties langer zijn, een zakelijke toon hanteren en vaker overtuigingsstrategieën toepassen. Dit laat zien dat er meer sprake is van strategische communicatie vanuit de aanbieder, wat zou kunnen leiden tot het gebruiken van neutralisatietechnieken.

Figuur 10: De hoeveelheid gebruikte neutralisatietechnieken in percentages, uitgesplitst per platform (n = 369)

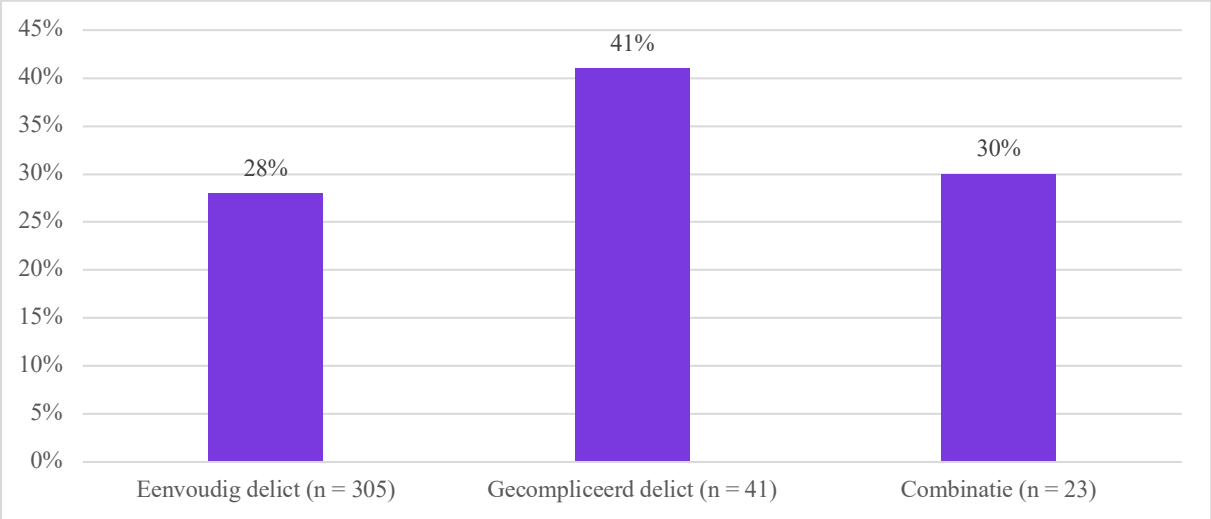


In het tweede model zijn het groepsgevoel, de toon, het doelwit en de moeilijkheidsgraad van het delict toegevoegd als onafhankelijke variabelen. Hier is te zien dat groepsgevoel, toon en het type doelwit significante voorspellers zijn van het gebruik van neutralisatietechnieken. Advertenties waarin een groepsgevoel wordt opgeroepen, hebben bijna drie keer zoveel kans om een neutralisatietechniek te bevatten (Exp(b) = 2,890, $p < 0{,}001$). Daarnaast hebben advertenties met een zakelijke toon ook bijna drie keer zoveel kans om neutralisatietechnieken te bevatten dan advertenties met een informele toon (Exp(b) = 2,894, $p = 0{,}025$). De toon en het creëren van een groepsgevoel in combinatie met het gebruik van neutralisatietechnieken lijken dus nog steeds strategische keuzes te zijn vanuit aanbieders om kopers te overtuigen.

Aan de hand van dit tweede model kunnen ook de tweede en derde gestelde hypothese worden getoetst. De tweede hypothese luidde als volgt: “Bij het aanbieden van eenvoudige delicten worden meer neutralisatietechnieken gebruikt dan bij het aanbieden van gecompliceerde delicten”. Uit de regressieanalyse blijkt dat de moeilijkheidsgraad van het delict geen significante voorspeller is voor het gebruiken van neutralisatietechnieken. Hoewel de kans op het gebruiken van een neutralisatietechniek 1,39 keer hoger is bij gecompliceerde delicten ten opzichte van eenvoudige delicten, is dit effect niet significant ($p = 0{,}410$). Dit blijkt ook uit figuur 11. Hier is te zien dat er

neutralisatietechnieken worden gebruikt in 28 procent van de advertenties waarin een eenvoudig delict wordt aangeboden. Bij de gecompliceerde delicten worden er meer neutralisatietechnieken gebruikt, namelijk in 41 procent van de advertenties. Dit weergeeft een tegenovergestelde trend ten opzichte van de hypothese. Omdat dit effect niet significant is, kan niet met zekerheid worden gesteld dat gecompliceerde delicten vaker gepaard gaan met neutralisatietechnieken dan eenvoudige delicten. Er kan wel worden vastgesteld dat de tweede hypothese niet wordt ondersteund door de data. Dit kan mogelijk worden verklaard door de zwaardere ernst van het delict en dus grotere risico's die verbonden zitten aan gecompliceerde delicten, waardoor er vaker neutralisatietechnieken nodig zijn om dit moreel te kunnen rechtvaardigen.

Figuur 11: Het gebruik van neutralisatietechnieken per moeilijkheidsgraad van het delict (n = 369)



De derde hypothese luidde als volgt: "Er worden meer neutralisatietechnieken gebruikt als het type doelwit een persoon is, dan wanneer het doelwit een bedrijf of instantie betreft". In totaal is in slechts 22 advertenties (6%) expliciet verwezen naar een specifiek type doelwit. Deze beperkte steekproefomvang bemoeilijkt een betrouwbare statistische toetsing. In de advertenties waar wel naar een type doelwit werd verwezen, ging dit in de meeste gevallen om particuliere doelwitten, namelijk in 16 advertenties. In 8 advertenties werd verwezen naar een bedrijf als doelwit en in 2 naar een overheidsinstantie. In tabel 4 is het gemiddelde aantal gebruikte neutralisatietechnieken weergegeven per type doelwit. Hieruit blijkt dat het gemiddelde bij particuliere doelwitten het hoogst ligt (0,75), gevolgd door bedrijven (0,63) en overheden (0,50). Deze gemiddelden liggen allemaal boven het algemene gemiddelde (0,40).

In de regressieanalyse is specifiek gekeken naar advertenties waarin een particulier doelwit werd genoemd, afgezet tegen advertenties waarin een ander type doelwit werd genoemd of helemaal geen verwijzing naar een doelwit plaatsvond. Uit deze analyse blijkt dat het benoemen van een particulier doelwit, oftewel een persoon, een significante voorspeller is voor het gebruiken van

neutralisatietechnieken, met een odds-ratio van 4,736 (p = 0,011). Dit zou betekenen dat advertenties waarin een particulier doelwit wordt benoemd, tussen de vier en vijf keer meer kans hebben om neutralisatietechnieken te bevatten dan advertenties zonder verwijzing naar een particulier doelwit. Vanwege de beperkte groepsgrootte zou er echter ook sprake kunnen zijn van een overschatting van het effect van het type doelwit. De groepsgrootte blijft dus een belangrijk aandachtspunt, waardoor deze resultaten enkel als indicatief kunnen worden geïnterpreteerd. Hoewel betrouwbare statistische toetsing niet mogelijk is, blijft de hypothese theoretisch relevant. In de literatuur wordt gesuggereerd dat de aard van het doelwit (persoon tegenover bedrijf/instantie) invloed kan hebben op het gebruik van neutralisatietechnieken. De framing van deze doelwitten en de toepassing van neutralisatietechnieken daarbij wordt daarom verder verkend in paragraaf 4.3.

Tabel 4: Aantal advertenties per type doelwit en gemiddeld aantal toegepaste neutralisatietechnieken (n = 22)

Type doelwit	*Aantal advertenties*	*Gemiddelde aantal neutralisatietechnieken*
Particulier	16	0,75
Bedrijf	8	0,63
Instantie	2	0,50

Naast het toetsen van de gestelde hypothesen, biedt de regressieanalyse in tabel 4 aanvullende inzichten die verder bijdragen aan het begrijpen van de onderzochte verbanden. In model 3 zijn de aanbiedertypen en de alternatieve overtuigingsstrategieën toegevoegd. Een opvallende bevinding is dat het beeld van de aanbiedertypen verandert zodra er wordt gecontroleerd voor andere advertentiekenmerken. Ondernemers blijken significant minder vaak gebruik te maken van neutralisatietechnieken dan criminelen, met een odds-ratio van 0,232 (p < 0,001). Ondernemers zijn dus bijna vier keer minder geneigd om neutralisatietechnieken toe te passen dan criminelen. Dit kan erop wijzen dat zij zich meer profileren als legitieme aanbieders, waarbij het criminele karakter zodanig naar de achtergrond wordt geplaatst dat neutralisatietechnieken overbodig zijn. Wat verder opvalt is dat mentors, die in de bivariate analyse significant vaker neutralisatietechnieken gebruikten, dit verschil niet weergeven in het regressiemodel (Exp(b) = 0,745, p = 0,554). Het eerder gevonden effect van het type mentor hing dus mogelijk samen met andere factoren.

Tot slot verandert ook de invloed van de alternatieve overtuigingsstrategieën, nadat er wordt gecontroleerd voor andere variabelen. Waar eerder alle drie de strategieën (reputatie, klantenservice en kortingen/promoties) significant samenhingen met het gebruik van neutralisatietechnieken, geldt dit nu voor geen enkele strategie meer. Dit kan betekenen dat hun effect vooral indirect van aard is en samenhangt met andere kenmerken, zoals de toon, het groepsgevoel of het platform.

Tabel 5: Resultaten van een logistische regressieanalyse met het gebruik van neutralisatietechnieken als afhankelijke (n = 369)

	Model 1			*Model 2*			*Model 3*		
	b (SE)	*Exp (B)*	*p*	*b (SE)*	*Exp (B)*	*p*	*b (SE)*	*Exp (B)*	*p*
Constante	-1,588 (0,286)**	0,204	<0,001	-2,426 (0,393)**	0,088	<0,001	-1,699 (0,513)**	0,183	<0,001
Platform	-0,915 (0,381)*	0,401	0,016	-1,346 (0,533)*	0,260	0,012	-1,780 (0,602)**	0,169	0,003
(0 = dark web, 1 = Telegram)									
Totaal aantal woorden	0,004 (0,001)**	1,004	<0,001	0,005 (0,001)**	1,005	<0,001	0,005 (0,001)**	1,005	0,001
Aantal aangeboden diensten/producten	0,061 (0,119)	1,063	0,609	0,148 (0,184)	1,160	0,419	0,137 (0,195)	1,146	0,483
Groepsgevoel				1,061 (0,286)**	2,890	<0,001	1,187 (0,313)**	3,277	<0,001
(0 = nee, 1 = ja)									
Toon				1,063 (0,473)*	2,894	0,025	1,117 (0,532)*	3,054	0,036
(0 = zakelijk, 1 = informeel)									
Doelwit				1,661 (0,587)**	5,263	0,005	1,555 (0,610)*	4,736	0,011
(0 = particulier, 1 = anders)									
Moeilijkheidsgraad delict									
Eenvoudig (ref.)									
Gecompliceerd				0,392 (0,400)	1,390	0,410	-0,135 (0,447)	0,874	0,763
Beide				-0,042 (0,799)	0,959	0,958	-0,451 (0,860)	0,637	0,600
Type aanbieder									
Crimineel (ref.)									
Ondernemer							-1,461 (0,415)**	0,232	<0,001
Expert							-0,070 (0,372)	0,932	0,850
Mentor							-0,294 (0,496)	0,745	0,554

Reputatie					0,359 (0,303)	1,432	0,236
(0 = nee, 1 = ja)							
Klantenservice					-0,083 (0,332)	0,921	0,803
(0 = nee, 1 = ja)							
Kortingen/promoties					0,714 (0,377)	2,041	0,059
(0 = nee, 1 = ja)							
Hosmer-Lemeshowtoets	8,861	0,354	9,139	0,331	12,895		0,115
Nagelkerke R^2	0,194		0,273		0,336		
-2LL	392,311		367,831		346,809		

* significant bij p <0,05; ** significant bij p <0,0

4.3 Kwalitatieve analyse

Tijdens het coderen zijn kwalitatieve gegevens verzameld over de advertenties, die in deze paragraaf op exploratieve wijze worden geanalyseerd. Daarbij is gekeken naar hoe aanbieders gebruikmaken van neutralisatietechnieken, reputatieverwijzingen en klantenservices met behulp van citaten. Daarnaast is de wijze waarop aanbieders zichzelf en het doelwit framen geanalyseerd, indien er specifiek naar een doelwit verwezen werd. Ook zijn er citaten genoteerd die een beeld schetsen van de gehanteerde toon in de advertentie. De citaten in deze paragraaf worden aangeduid met het advertentienummer per platform, waarbij DW staat voor dark web en T voor Telegram. Deze kwalitatieve analyse biedt aanvullende inzichten gericht op de taalvormgeving en context waarin neutralisatietechnieken en andere overtuigingsstrategieën worden toegepast.

4.3.1 De context van de online platforms

Om de verschillende elementen die aanbieders in hun advertenties toepassen goed te kunnen begrijpen, is het allereerst van belang om stil te staan bij de bredere context waarin deze advertenties worden geplaatst. Deze advertenties zijn namelijk niet alleen zakelijke aanbiedingen die de drempel tot online criminaliteit verlagen; ze maken ook deel uit van een bredere online subcultuur. In deze subcultuur lijkt vooral mannelijkheid een prominente rol te spelen. Dit valt niet alleen op in de advertenties, maar kwam ook duidelijk naar voren tijdens het verzamelen van de data. Op de websites en in de groepen waar deze diensten en producten worden aangeboden, circuleren veel expliciete en seksuele beelden van vrouwen. Deze beelden lijken daarmee in te spelen op een overwegend mannelijk publiek, waarbij deze beelden worden ingezet om het aanbod aantrekkelijker te maken. Tegelijkertijd worden vrouwen gepresenteerd als (seksuele) instrumenten, wat aansluit bij huidige online trends waarin traditionele ideeën over mannelijkheid worden verheerlijkt. In sommige van deze online gemeenschappen, vaak aangeduid als de *'manosphere'*, staat mannelijkheid centraal en worden vrouwonvriendelijke opvattingen verspreid die stellen dat vrouwen inferieur zijn aan mannen (Weale, 2023; NOS, 2025). Ook in sommige advertenties komt dit erg expliciet naar voren, bijvoorbeeld door termen te gebruiken als "*fucking whore*" (DW120). In een ander voorbeeld wordt ook op een denigrerende manier gesproken over vrouwelijke ex-partners, waarbij de bedreiging rechtvaardig lijkt: *"call to your ex and tell her who is she and where is her place."* (DW79) Maar ook in meerdere advertenties wordt het monitoren van de online activiteiten van je vriendin gepresenteerd als een normale zaak: *"Want to Spy your Girlfriend?"* (DW113) of "*Hack your girlfriend's account? […] No problem!*" (DW118). Deze verwijzingen laten zien dat aanbieders in hun advertenties elementen gebruiken die ook terugkomen in populaire online subculturen. Dit kan erop wijzen dat zij zelf deel uitmaken van deze subcultuur, of dat ze bewust inspelen op de interesses van hun doelgroep.

In de beschrijvende analyses kwam naar voren dat ongeveer een derde van de advertenties een groepsgevoel probeert te creëren in de advertentie door gebruik te maken van collectieve

aanspreekvormen. Door bijvoorbeeld de “wij-vorm” te hanteren, wordt de suggestie gewekt dat het aanbod afkomstig is van een team of gemeenschap in plaats van een individuele aanbieder. Dit draagt bij aan het beeld dat online criminaliteit een collectieve, genormaliseerde activiteit is. Een voorbeeld hiervan is de uitspraak: *“We offer high-quality products at the best price first-hand, from our team!”* (DW136). Hiermee wordt niet alleen professionaliteit, maar ook legitimiteit gesuggereerd.

Het benadrukken van een groepsverband kan verschillende doelen hebben, zoals het vergroten van vertrouwen of het normaliseren van deviant gedrag. Binnen een gemeenschap waarin iedereen zich met online criminaliteit bezighoudt, lijkt het plegen van strafbare feiten niet langer een normoverschrijding. Het gaat hier niet alleen om het gebruiken van de “wij-vorm” als aanspreekvorm, maar ook om een bredere sociale dynamiek. In sommige advertenties worden jonge mannen bijvoorbeeld specifiek aangesproken, zoals hier: *“Boys interesse BE PANEL MET LOGS”* (T42). Hiermee wordt wederom expliciet aansluiting gezocht bij een mannelijk publiek. Ook wordt er regelmatig verwezen naar onderling broederschap. Bijvoorbeeld: *“This Is Where You Will Make Friends Who Become Close As Brothers.”* (DW166) Hier wordt benadrukt dat het niet alleen gaat om de geleverde dienst, maar ook het broederschap dat ermee gepaard gaat. Zo wordt er ook vaker expliciet naar de online context verwezen als een gemeenschap: *“Because I’m a new user in this community […]”* (DW210) en *“I have been serving the Darknet community with high quality items for 20+ markets.”* (DW243). Het gedrag wordt hiermee gepresenteerd als sociaal gelegitimeerd binnen de groep, wat ook aansluit bij de neutralisatietechniek “een beroep doen op een belangrijkere norm” die verder wordt toegelicht in paragraaf 4.3.2.

De normalisatie van dit gedrag binnen de online subcultuur zie je ook terug in de namen van de online groepen en de termen die worden gebruikt. Het complete overzicht van de groepsnamen staat in bijlage 2. Vooral op Telegram is dit zichtbaar. Er wordt in de groepsnamen verwezen naar frauduleuze praktijken met termen als “F Game” of door specifiek fraude te benoemen. Deze term “F Game” komt vaker naar voren in Telegram-berichten, zoals hier: *“Welkom bij F-game”* (T43). Deze term die vooral door jongeren wordt gebruikt betekent fraudegame, waarbij geld wordt verdiend met vormen van online criminaliteit zoals phishing (Nederlandse Politie, z.d.). Jongeren die hieraan deelnemen maken daar op sociale media openlijk reclame voor en pronken hierbij met geld en succes, waardoor zij het niet echt meer als crimineel gedrag lijken te beschouwen (NOS, 2022). Andere online termen die in de groepsnamen zijn gebruikt zijn “bonkers”, “rakkers” en “mapsers”. Deze termen zijn afkomstig uit de Smibanese straattaal, die afkomstig is uit de Bijlmer. Hier is het gebruikelijk om woorden om te draaien (Straattaal Woordenboek, z.d.). Zo staat “mapser” bijvoorbeeld voor spammer. Het gebruik van deze specifieke straattaal fungeert niet alleen als een vorm van codetaal, maar versterkt ook het gevoel van een gedeelde identiteit binnen de subcultuur.

Al deze elementen wijzen erop dat de advertenties niet op zichzelf staan, maar deel uitmaken van een bredere online subcultuur waarin vooral jonge mannen zich verenigen. Hier worden

groepsgevoel en broederschap centraal gesteld, waarbij online criminaliteit wordt voorgesteld als een normale handeling of zelfs als sociaal wenselijk gedrag.

4.3.2 De toepassing van neutralisatietechnieken

In paragraaf 4.1 werden de meest gebruikte neutralisatietechnieken weergegeven. Bovenaan stond de techniek 'het bedenken van nieuwe feiten, die in totaal 40 keer is gebruikt. Bij deze techniek wordt er een alternatieve realiteit geschetst waarin het delict niet langer meer als immoreel wordt beschouwd, maar als onschuldig en legitiem gedrag, of juist als rechtvaardig. De manier waarop deze techniek het vaakst door aanbieders werd gebruikt, is door te stellen dat de dienst/het product expliciet bedoeld is voor educatieve doeleinden en niet voor criminaliteit. Bijvoorbeeld: *"These Tools are for educational and pentesting purpose, it's highy illegal to use them against networks without permission of the owner!"* (DW15) Dit is een bewuste aanpassing van de feitelijke situatie, waarin het wordt aangeboden voor criminele doeleinden, naar een fictieve situatie waarin het als leerzaam en onschuldig wordt gepresenteerd. Wat ook meerdere keren naar voren kwam, is dat de aanbieders hun aanbod presenteren als iets dat überhaupt niet crimineel van aard lijkt te zijn: *"PayPal transfers are a quick and safe way to get clean money."* (DW112) Het delict wordt gepresenteerd als een betrouwbare en legitieme manier om 'schoon geld' te krijgen, in plaats van een frauduleuze transactie. Hierdoor lijkt het gedrag onschuldig. In andere scenario's worden de criminele handelingen gepresenteerd als onderdeel van een legitieme carrière. Zo brengt één aanbieder zijn product als zakelijke hulp om je professionele vaardigheden mee te vergroten:

> *"If you want to be a Professional Carder and raise your success rate 300 percent then you need this software. This software will make you card like a professional and you will be able to have a much higher accept rate."* – DW81

In deze advertentie wordt de criminele handeling vervangen voor een fictief verhaal, namelijk een carrièrekans. Het gaat daarom niet langer om de vraag of het moreel juist is, maar of je de handeling op een goede manier uitvoert, net als in een legitieme carrière. Daarnaast zijn er aanbieders die een scenario schetsen waarin het delict een rechtvaardige reactie lijkt te zijn op de situatie waarin de koper zich bevindt: *"Since the power in the hand has grown so much, a control over that power is also needed. DroidJack is what you need for that."* (DW249) Er wordt hier gesteld dat de kracht van mobiele apparaten ('*the power in the hand*') tegenwoordig zo groot is, dat het belangrijk is als gebruiker om hier zelf ook controle over te hebben. Hoewel het gaat om het controleren van andermans mobiele apparaat, wordt het als rechtvaardig gepresenteerd. Verder valt het op dat bijna 90 procent van de advertenties die deze neutralisatietechniek hebben gebruikt een zakelijke toon bevatten. Het aanbod wordt hier op een professionele manier gebracht. Aanvullend lijken experts en

ondernemers vaak gebruik te maken van deze techniek, in 86 procent van de gevallen is het type aanbieder volledig of gedeeltelijk expert en/of ondernemer. Dit sluit inhoudelijk goed op elkaar aan, omdat de neutralisatietechniek vaak het delict schetst als een alledaagse handeling in een legitiem werkveld. Door het delict op deze manier te verpakken lijkt het niet langer meer om een criminele handeling te gaan.

Op de tweede plaats stond 'de schuld geven aan beperkte keuzes', die in totaal 25 keer is gebruikt. Bij deze techniek wordt het gedrag gerechtvaardigd door te stellen dat er een gebrek aan alternatieve keuzes is. Door omstandigheden als externe druk en grote verleiding blijft criminaliteit over als de enige keuze. Deze nadruk op verleiding wordt ook duidelijk teruggezien in de advertenties. Aanbieders leggen de nadruk op de hoeveelheid geld en status die verkregen kan worden aan de hand van deze aankoop, waarbij voornamelijk geld veel naar voren komt als motivatie. Sommige aanbieders houden het enkel bij het creëren van grote verleiding: *"Once you get setup and you disperse the stealer you can easily make thousands in Bitcoin in a couple weeks."* (DW234) Andere aanbieders benoemen ook expliciet waarom de alternatieve keuzes ondermaats zijn om de potentiële koper nog meer aan te moedigen. Een aanbieder schreef bijvoorbeeld:

> *"Are you tired of your boring job, stupid boss, old car and vacation at home? Then you came to the right place! With our help and our PayPal transfers you can reach the life of your dream and completely change the way you live! It costs you just 2 clicks to finish your past and start your fascinating future! Don't miss your chance!"* – DW126

De verleiding wordt vergroot door aan de ene kant de nadruk te leggen op de negatieve aspecten van de alternatieve keuzes, zoals een saaie baan en een vervelende baas, en aan de andere kant geld en status te beloven via deze aankoop. Driekwart van de aanbieders die deze techniek heeft gebruikt, presenteert zichzelf als crimineel. Dit betekent dat de aanbieders open zijn over het criminele karakter van de dienst of het product dat ze aanbieden. De focus wordt echter gelegd op de voordelen die de klant kan halen uit deze illegale handelingen. Hierin wordt het (snel) verdienen van geld als grootste motivatie gepresenteerd. Deze aanbieder benoemt bijvoorbeeld expliciet dat het gaat om frauduleuze handelingen, maar brengt het als een manier waarmee de koper een stabiel inkomen voor zichzelf kan creëren: *"So how many of you are tired of being noobs, or are still looking for the right high paying niche in the fraud world?, or want to have a steady monthly or weekly income through the dark means?"* (DW165) Daarnaast wordt de potentiële koper in de meeste gevallen erg direct aangesproken, wat de urgentie van de boodschap kan versterken. Door deze techniek te gebruiken wordt dus de verantwoordelijkheid afgeschoven op de externe druk, terwijl er een aantrekkelijk alternatief wordt geboden. Het CaaS-aanbod wordt daarmee in een positief daglicht gezet.

De neutralisatietechniek die op de derde plaats staat is 'het reduceren van de geldende norm tot feiten'. Deze is 24 keer naar voren gekomen in advertenties. Hier wordt de geldende norm (die het

delict afwijst) ongeldig verklaard door het weg te zetten als een persoonlijke voorkeur, of door een ander label te hangen aan het delict om het te minimaliseren. In de advertenties is meermaals naar voren gekomen dat de aanbieder het criminele gedrag romantiseert. Deze aanbieder presenteert het oplichten van mensen bijvoorbeeld als een gewaardeerde kunstvorm:

"Hacking a Social Media account is a Social Engineering task. SE is the art of tricking people into performing actions or revealing information with the aim of gaining access to information systems or confidential information." – DW198

De geldende norm wordt hierbij niet expliciet ontkend, maar door het delict op een mooie manier te verpakken wordt de afwijzende norm minder relevant. Binnen deze neutralisatietechniek wordt ook vaak gebruikgemaakt van eufemismen en andere labels die het delict minimaliseren. Het volgende citaat is daarvan een voorbeeld: *"Want to Hide/Spoof any virus/exploit so you can infiltrate undetected inside a computer like a ninja?"* (DW14) Met termen als 'infiltrate' en 'ninja' worden er spelelementen geïntroduceerd in het delict, waardoor het delict op een spannende manier wordt gepresenteerd. Vooral in de online wereld waar veel potentiële kopers wellicht affiniteit hebben met technologie en gamen, kan dit helpen om het aanbod aantrekkelijker te maken.

De neutralisatietechniek die hierop volgt is 'een beroep doen op een belangrijkere norm'. Deze techniek werd in totaal 21 keer gebruikt. Hierbij wordt er een overschrijdende norm gepresenteerd die belangrijker is dan de norm over deviant gedrag. Dit kan gaan om een hoger doel als verzet of vergelding, maar het kan ook draaien om groepsdruk en het conformeren aan de sociale normen. Beide vormen van de neutralisatietechniek kwamen naar voren in de advertentie, maar vooral vergelding werd vaak als belangrijkere norm gepresenteerd. Dit komt duidelijk naar voren in het volgende citaat:

"Do you want to hack your girl's messenger? Or maybe you want to hack your fucking boss emails? Copy the phone number of your girlfriend and log into any social network! Be careful, she may be a fucking whore" – DW120

De aanbieder zet de mogelijke slachtoffers in een negatief daglicht, wat het beeld schetst dat het rechtvaardig zou zijn om het delict te plegen. Dit wordt gedeeltelijk verklaard vanuit vergelding (*"hack your fucking boss"*) maar ook gedeeltelijk uit zelfbescherming (*"Be careful"*). In andere advertenties wordt verwezen naar de criminele carrière als het vinden van je roeping, of als vorm van rechtvaardige rebellie:

"Based on the date of the last transactions on these wallet addresses, I can confidently say that getting access and transferring the coins to your account will be considered a patriotic move to revive the economy" – DW212

Deze aanbieder stelt dat deze vorm van diefstal, waarbij cryptovaluta uit de portefeuilles van slachtoffers worden gestolen, kan worden gezien als een handeling uit vaderlandsliefde en om de economie een nieuw leven in te blazen. Er wordt een erg duidelijke overschrijdende norm gesteld die belangrijker wordt geacht. Verwijzingen naar groepsdruk kwamen minder vaak voor in de advertenties, maar zaten er wel duidelijk tussen. Dit sluit aan op de eerdere verwijzingen naar broederschap en gemeenschap die zijn genoemd. Bijvoorbeeld: *"This Group Is Where I Have Made My Closest Friends, Whom I Talk To Everyday."* (DW107) De aanbieder benadrukt hier vriendschap en verbondenheid, wat tegelijkertijd een sociale norm weerspiegeld waarbinnen het criminele gedrag genormaliseerd is.

De neutralisatietechniek 'het ontkennen van de feiten' kwam in elf advertenties voor. Bij deze techniek wordt het deviante gedrag niet in zijn geheel ontkend, maar bepaalde onderdelen ervan, zoals het bestaan van een slachtoffer of het toedoen van schade. Door deze elementen te ontkennen, wordt het gedrag minder snel als strafbaar of immoreel geïnterpreteerd. In meerdere advertenties werd expliciet gesteld dat er geen sprake was van een slachtoffer. Zo stelde een aanbieder over een methode die gebruikmaakt van geïnfecteerde computers: *"This is by far the best way to make money in the darknet without hurting people, safe and 100% anonymous"* (DW31). Hier wordt impliciet toegegeven dat het om een illegale activiteit gaat, maar tegelijkertijd wordt de schade ontkend, wat het gedrag onschuldig laat lijken. Een andere aanbieder probeert de ernst van het delict te minimaliseren door te benadrukken dat slechts verwaarloosde cryptoportefeuilles worden aangevallen: *"We primarily target old and abandoned wallets, minimizing the risk of detection."* (DW239) De aanbieder suggereert dat het delict geen daadwerkelijke impact heeft, terwijl er in werkelijkheid nog steeds sprake is van diefstal. Opvallend is dat deze neutralisatietechniek wordt toegepast door verschillende typen aanbieders. Dit wijst erop dat het ontkennen van het delict breed toegepast kan worden om morele bezwaren bij kopers weg te nemen, ongeacht de stijl of toon van de aanbieder.

De neutralisatietechniek 'het nuanceren van de feiten' kwam in zeven advertenties voor. Deze techniek draait om het ondermijnen of verdraaien van de waarheid die het gedrag als deviant kenmerkt. Door twijfel te zaaien over morele en juridische grenzen, wordt het gedrag gepresenteerd als toelaatbaar. Het doel is om het onderscheid tussen legaal en illegaal gedrag te vervagen, zodat het criminele karakter van het aanbod minder duidelijk overkomt. Een voorbeeld hiervan is de volgende uitspraak: *"To take everything of your credit score and erase all score and use legal loopholes"* (DW13). Er wordt gesteld dat de aanbieder gebruikmaakt van mazen in de wet, waardoor het niet langer overkomt als een strafbaar feit. In meerdere advertenties werden er geldbedragen van gehackte accounts aangeboden, waarbij de volgende metafoor wordt gebruikt: *"It is like when somebody on the*

street gives you cash for no reason. Of course he can not cancel that transfer later or go to police and ask them to do that." (DW124) Deze vergelijking doet het gedrag overkomen als iets onschuldigs, waarmee de suggestie wordt gewekt dat het hier niet om een delict gaat omdat er geen aangifte kan worden gedaan. Opvallend is dat deze neutralisatietechniek vooral is gebruikt door aanbieders met als type ondernemer. Dit sluit aan bij het strategisch karakter van deze techniek: het criminele gedrag wordt verpakt als legitiem aanbod.

De neutralisatietechniek 'de schuld geven aan de beperkte rol' kwam met zes keer voor in de advertenties. Bij deze techniek wordt benadrukt dat de koper slechts een kleine rol speelt in het deviante gedrag, waardoor het gevoel van verantwoordelijkheid voor de toegedane schade afneemt. Dit kwam vooral naar voren in advertenties waar de aanbieder zichzelf als de uitvoerende partij presenteert, terwijl de rol van de koper wordt beperkt tot een eenvoudige handeling. Bijvoorbeeld: *"In order to receive money, you just need to provide your email address. Thanks to this, you remain completely anonymous and most importantly, the money will be credited to your account within 20-30 minutes."* (DW135) De koper hoeft hier enkel een e-mailadres op te geven, wat het beeld schetst dat er weinig betrokkenheid is bij het delict. Door de drempel zo laag te maken, wordt het gedrag gepresenteerd als relatief onschuldig. Deze neutralisatietechniek is niet vaak voorgekomen. Een mogelijke verklaring hiervoor is dat het expliciet nemen van verantwoordelijkheid door de aanbieder ook zijn eigen aansprakelijkheid vergroot.

De neutralisatietechniek 'verschuilen achter een gebrek aan goede intenties' kwam ook in zes advertenties voor. Hierbij wordt een delict gepleegd zonder schaamte en schuldgevoelens, omdat de pleger zichzelf neerzet als iemand die geen behoefte heeft zich te conformeren aan morele normen. Er wordt niet geprobeerd het gedrag te rechtvaardigen of de ernst ervan te verzachten, in plaats daarvan wordt normloosheid centraal gesteld en in sommige gevallen verheerlijkt. In advertenties is dit teruggezien aan de morele onverschilligheid en roekeloosheid die worden gepromoot door de aanbieder. Deze aanbieder moedigt bijvoorbeeld potentiële kopers aan om over morele grenzen heen te stappen: *"Success is always for those who are fearless. knock yourself out!!"* (DW164) De koper wordt hier niet alleen aangemoedigd om het delict te plegen, maar ook om dat zelfverzekerd en zonder terughoudendheid te doen. Er wordt geen poging gedaan om het gedrag te verantwoorden, maar er wordt gesteld dat dit iets is waarmee je jezelf kunt bewijzen; het delict wordt gepresenteerd als bewonderingswaardig. In een andere advertentie kwam deze morele onverschilligheid nog explicieter naar voren: *"It is very simple and easy to use, and very effective, it gives you a command shell, can do whatever you want, and the AV doesn't give a shit! Have fun brother!"* (DW1) Hier wordt de potentiële koper zelfs aangemoedigd om er plezier in te hebben, wat de morele en juridische grenzen irrelevant maakt. Er wordt juist een omgeving gecreëerd waarin regels overtreden wenselijk is. In geen enkele van deze advertenties is een poging gedaan om het criminele karakter van het aanbod te verbloemen. Een aantal advertenties hebben wel een commerciële insteek, maar het criminele aspect wordt in iedere advertentie duidelijk benoemd. De advertenties laten zien dat deze

neutralisatietechniek zich richt op het normaliseren en aanmoedigen van criminaliteit door morele onverschilligheid te verheerlijken. Deze techniek onderscheidt zich door de afwezigheid van schaamte of legitimering.

De neutralisatietechniek ‘de schuld geven aan beperkte opties’ is slechts drie keer voorgekomen. Deze techniek houdt in dat het delict wordt gepresenteerd als de enige overgebleven, realistische optie omdat alternatieven als onhaalbaar, onbereikbaar of onvoldoende effectief worden neergezet. In de betreffende advertenties is zichtbaar dat het aanbod wordt gepresenteerd als een unieke kans om de persoonlijke situatie te verbeteren, omdat reguliere wegen niet zouden volstaan. Zo probeert één aanbieder kopers te overtuigen met de belofte dat zijn dienst de oplossing biedt als je financiële situatie niet toereikend genoeg is op de woningmarkt: *“Wil je een woning 🏠 huren maar verdien je te weinig? Wij veranderen je loonstroken zodat jij kan wonen waar je wilt!!”* (T97) Hier wordt het plegen van fraude niet alleen gelegitimeerd, maar gepresenteerd als noodzakelijk om toegang te krijgen tot huisvesting. Het morele bezwaar wordt daarmee ondergeschikt gemaakt aan het geschetste probleem. Een andere aanbieder verwijst naar sociaaleconomische achterstand als rechtvaardiging, met expliciete verwijzing naar armoede in ontwikkelingslanden: *“I've had guys from third world shitholes with 6 figure opportunities make their first $10,000. Fraud requires you to be hungry, always.”* (DW107) Door te spreken in termen van overlevingsdrang en schaarste wordt een context gecreëerd waarin criminaliteit wederom noodzakelijk lijkt. Deze aanbieders zetten daarmee druk op de koper; als je je bevindt in een achtergestelde situatie, dan is dit je kans om deze te verbeteren. De schuld voor de normovertreding wordt verplaatst naar het gebrek aan betere alternatieven, waarbij het deviante gedrag niet direct wordt verheerlijkt, maar wel als enige resterende optie wordt gepresenteerd.

De neutralisatietechniek ‘verschuilen achter onvolmaakte capaciteiten’ is slechts één keer aangetroffen in de advertenties. Op basis van de theorie werd al verwacht dat deze techniek weinig tot niet gebruikt zou worden, aangezien deviant gedrag gepresenteerd wordt als het gevolg van gebrekkige zelfbeheersing of beperkte bekwaamheid. Dit draagt niet bij aan een geloofwaardige of aantrekkelijke presentatie van het aanbod, terwijl betrouwbaarheid juist belangrijk is in de presentatie en leidt tot meer transacties. Toch werd de neutralisatietechniek door één aanbieder gebruikt: *“Fraud's not dead, you're just lazy. Fraud rewards effort but attracts the laziest of people.”* (DW107) In deze uitspraak wordt de potentiële koper lui genoemd, maar wordt het gebruikt om diegene juist aan te spreken op zijn gebrek aan inzet of discipline. Interessant is dat deze techniek niet wordt ingezet om het aanbod te legitimeren, maar om de potentiële koper uit te dagen. Er wordt een boodschap overgebracht die stelt dat het volledig aan jezelf ligt als je faalt, want dit komt voort uit luiheid. Het gedrag wordt neergezet als haalbaar voor wie zich niet laat tegenhouden door eigen zwakte en probeert op die manier potentiële kopers te activeren. Deze specifieke aanbieder paste bij het type mentor, omdat vervolgens het aanbod wordt gedaan om kopers te begeleiden in het succesvol uitvoeren van

criminaliteit. Deze techniek is dus niet gebruikt om het gedrag te excuseren, maar juist om de koper te motiveren om te betalen voor de begeleiding van de aanbieder.

4.3.3 De framing van de aanbieders

Er zijn vier hoofdcategorieën aanbieders: ondernemer, crimineel, expert en mentor. Iedere advertentie heeft op basis van de zelfpresentatie van de aanbieder één of maximaal twee van deze typen aangewezen gekregen. Als het niet mogelijk was om in de advertentie het type aanbieder te bepalen, omdat de advertentietekst te kort was, is er geen type aanbieder aangewezen.

De criminele aanbieder wordt gekenmerkt door het criminele karakter dat openlijk wordt erkend, waarbij geen poging wordt gedaan om het illegale karakter van de dienst of het product te verbloemen of legitimeren. Zo wordt in advertenties regelmatig gesproken over slachtoffers in termen als *"target"* (DW155), of komt er duidelijk naar voren dat er geen morele grenzen aan het aanbod verbonden zijn: *"I will call anywhere you want, […] or call to your ex and tell her who is she and where is her place."* (DW79) Ook is er soms sprake van een dreigende of intimiderende toon, met bijvoorbeeld scheldwoorden of het kleineren van de koper: *"Geen geflikflooi aan deze kant"* (T81) of *"[…] do not waste our time and ask unnecessary questions"* (DW127). Het taalgebruik is vaak kortaf en dwingend, waarbij een dominante rol wordt aangenomen door de aanbieder ten opzichte van de koper. Technische details en een klantgerichte aanpak worden meestal achterwege gelaten, omdat de focus ligt op de uitkomst. In de meeste gevallen gaat dit om financieel gewin of het uitoefenen van macht over anderen. De aanbieder creëert een omgeving waarin morele onverschilligheid ontstaat.

Het type ondernemer kenmerkt zich door een sterk commerciële en klantgerichte presentatie van het aanbod. In deze advertenties ligt de nadruk op gebruiksgemak, klanttevredenheid, de kwaliteit van de service en betrouwbaarheid. Het criminele karakter wordt daarom verpakt op een legitieme, klantgerichte manier (*"Ideal for beginners"* – DW243). De toon is doorgaans professioneel en zakelijk, waarbij termen worden gebruikt die doen denken aan de verkoop op legitieme marktplaatsen. In veel gevallen presenteert de aanbieder het product als een legitieme dienst, waarbij praktische informatie zoals prijzen, levertijden, garantievoorwaarden en retourbeleid centraal staan. De belangrijkste componenten zijn de efficiënte afhandeling van de aankoop en het bieden van een positieve klantervaring. De koper wordt aangesproken als klant in plaats van als medepleger van het delict. Dit wordt duidelijk door termen als *"VIP customers"* (DW139) en *"professional service"* (T19). Op deze manier wordt het aanbod op zo'n aantrekkelijk mogelijke manier te presenteren. Deze commerciële framing van de aanbieder en het aanbod zouden ervoor kunnen zorgen dat de morele implicaties minder duidelijk worden gevoeld door potentiële kopers.

De experts kenmerken zich door een focus op technische kennis, functionaliteiten van het aanbod en inhoudelijke diepgang. Deze aanbieders presenteren zichzelf als technologisch vaardige professionals. Hun diensten en producten worden gepresenteerd met inhoudelijke uitleg over

technische specificaties en software-eigenschappen. Veel advertenties bestaan uit lange opsommingen hiervan, waarbij gebruik wordt gemaakt van vakjargon zoals *"SQL injection"* (DW71)*, "FUD backdoor binder"* (DW181) en *"panel gateway"* (T70). Dit soort taalgebruik legt de drempel voor de advertentie daarmee wel hoger, gericht op een doelgroep met bestaande technische kennis. Op interactioneel niveau ligt de nadruk op functionele en technische betrouwbaarheid van de dienst of het product. Door te verwijzen naar de eigen ervaring (*"Since 2007 we have been involved in this area"* – DW142*, "team of professionals"* – DW109), de kwaliteit van de software (*"we guarantee quality and reliable services at all time"* – DW139) of het geavanceerde aanbod (*"over 5000 lines of Python code"* – DW250). Het gedrag wordt gepresenteerd als een technologisch proces, waardoor het morele karakter van het delict naar de achtergrond kan verplaatsen. Sommige aanbieders framen hun diensten expliciet als *"cybersecurity services"* (T17) of *"digital solutions"* (T101) waardoor het aanbod wordt gelegitimeerd. Deze aanbieders proberen dus potentiële klanten te overtuigen door een beroep te doen op technologische expertise.

Het type mentor presenteert zichzelf als een begeleider of opleider, met als voornaamste doel het ondersteunen en onderwijzen van de koper. In tegenstelling tot de andere typen aanbieders staat het product hier niet centraal, maar het leerproces en de kennis van de koper. De aanbieders focussen zich in veel advertenties expliciet op het aanleren van vaardigheden en het uitleggen van verschillende technieken. In sommige gevallen gaat dit ook om langdurige ondersteuning. De mogelijke ondersteuning die wordt geboden varieert van stap-voor-stap tutorials (*"the best EVER tutorial written by the best ever vendor"* – DW252) en het opzetten van gepersonaliseerde phishing-pagina's, tot het geven van video-instructies of live begeleiding tijdens de uitvoering. In veel gevallen wordt de koper aangesproken als iemand die nog moet leren en begeleiding nodig heeft (*"GoldApples Fraud Bible is best for newbies in the fraud game who want to get immersed with a variety of their needed fraud knowledge and dont know where to start"* – DW260). Het delict wordt daarom ook meer gepresenteerd als een vaardigheid die je kunt ontwikkelen. Door de aankoop te framen als kennisdeling of coaching, komt het criminele karakter ook minder expliciet naar voren. Door ondersteuning te bieden wordt de instapdrempel voor potentiële kopers verlaagd.

Hoewel de meeste advertenties duidelijk binnen één type aanbieder vielen, is in een aantal gevallen gekozen om twee aanbiedertypen toe te wijzen per advertentie. De aanbieders waren niet altijd eenduidig in hun zelfpresentatie, soms zat hier ook overlap tussen. Een veelvoorkomende combinatie was die tussen crimineel en ondernemer, in 36 advertenties. Deze advertenties bevatten zowel openlijke verwijzingen naar strafbare activiteiten als een klantgerichte toon. Het product wordt dus tegelijkertijd gepresenteerd als deviant en als efficiënt en winstgevend. Een andere veelvoorkomende combinatie was expert en ondernemer, in 29 advertenties. Hierbij werd technische expertise gecombineerd met commerciële presentatie. De aanbieder overtuigde niet alleen met inhoudelijke kennis, maar ook met servicegerichte taal, levertijden en garanties. Ook de combinatie crimineel en expert kwam 25 keer voor in advertenties. In deze advertenties stond het criminele

karakter van het product centraal, maar werd dit onderbouwd met technische specificaties en inhoudelijke uitleg. Overige combinaties kwamen minder vaak naar voren. Deze combinaties illustreren wel dat aanbieders flexibel om kunnen gaan met hun zelfpresentatie. De overtuigingskracht van de advertentie zou vergroot kunnen worden door meerdere rollen tegelijkertijd aan te nemen.

4.3.4 De framing van het doelwit

In 22 advertenties werd er expliciet verwezen naar een type doelwit. In de meeste gevallen ging dit om een particulier doelwit, oftewel personen. In de helft van de advertenties met personen als doelwit was sprake van ondermijning van de menselijkheid van de doelwitten. In advertenties voor phishing worden er bijvoorbeeld mensen van 65 jaar en ouder specifiek uitgefilterd en gepresenteerd als een kwetsbare en daarom winstgevende doelgroep. Deze groep wordt daarmee gereduceerd tot een productcategorie. Eén van de aanbieders die persoonsgegevens van deze groep aanbiedt biedt zelfs *"Prikgarantie"* (T24), wat suggereert dat deze doelwitten gegarandeerd te misleiden zijn. De doelwitten werden gepresenteerd als instrumenten in plaats van mensen. Het delict lijkt daarom eerder op een neutrale transactie dan een handeling met schadelijke gevolgen. Waar de doelwitten wel als mensen werden omschreven, gebeurde dit vaak op een manier die hun slachtofferschap rechtvaardigt. In deze advertenties werd de neutralisatietechniek "een beroep doen op een belangrijkere norm" gebruikt. De doelwitten worden gepresenteerd als personen die het verdienen. In de meeste gevallen gaat het om (ex-)partners of vijanden. Het uitoefenen van wraak (*"Punish your competitors"* – DW118) of het bespioneren van een mogelijk ontrouwe partner (*"Find out if your wife or husband is cheating on you"* – DW19) legitimeert het gebruik van de dienst, omdat het een belangrijkere norm is dan degene die het gedrag afwijst.

Als het type doelwit een bedrijf betreft, wordt het bedrijf altijd op een neutrale en instrumentele manier weergegeven. Door te spreken over *"Shops you can hit"* (DW55) en *"anything carry IP"* (DW248) worden doelwitten gereduceerd tot objecten en obstakels. In sommige gevallen wordt er ook expliciet benoemd dat het om bedrijven en instellingen gaat en dat er geen schade wordt toegedaan aan individuen. Hiermee wordt het beeld geschetst dat de schade aan bedrijven en andere instanties minder erg is dan aan individuen. Het plegen van het delict lijkt daardoor ook onschuldiger.

De verschillende vormen waarop doelwitten worden gepresenteerd kunnen er uiteindelijk voor zorgen dat de morele implicaties minder erg lijken. Door het doelwit te rechtvaardigen, objectiveren of ontmenselijken wordt hun schade buiten beeld geplaatst.

4.3.5 De gehanteerde toon

De toon van de advertentie kan een belangrijk onderdeel uitmaken van de overtuigingsstrategie van aanbieders. In paragraaf 4.1 werd al weergegeven dat 74 procent van de advertenties een zakelijke toon bevatte en 26 procent een informele toon. Deze toonaanduiding is gebaseerd op de stijl en

formulering van de advertentietekst, waarbij per advertentie is gekeken naar onder andere woordkeuze, aanspreekvorm, opmaak en het gebruik van straattaal en emoji's.

Een zakelijke toon wordt gekenmerkt door formeel en functioneel taalgebruik. De aanbieder presenteert zichzelf als een professionele dienstverlener, waarbij het aanbod gestructureerd en feitelijk wordt omschreven. Dit soort advertenties bevatten vaak vaste formats, zoals een opsomming van kenmerken, technische specificaties of garanties. De koper wordt aangesproken als klant, waarvan deze citaten een goede weerspiegeling vormen: *"We are glad to welcome you in our store!"* (DW133) en *"Check my shop to see other listings!"* (DW171) De potentiële klant wordt hier op een uitnodigende, gastvrije manier begroet door de aanbieder. Dit is een weerspiegeling van de klantbenadering van legitieme winkels. Advertenties met een zakelijke toon zijn niet uitsluitend op een klantvriendelijke manier geformuleerd. Deze aanbieder hanteert geen vriendelijke toon, maar geeft alsnog een duidelijk geformuleerde instructie aan potentiële kopers: *"It is assumed the buyer knows exactly what they are buying and how to use it upon purchase."* (DW6) In veel advertenties wordt duidelijk verwezen naar de geldende garanties: *"By purchasing this account, you automatically agree with the rules of this service."* (DW10) Hier wordt ook duidelijk dat de aanbieder formeel taalgebruik toepast om professioneel over te komen. De afstandelijke en informatieve toon in de advertenties lijkt bij te dragen aan een beeld van betrouwbaarheid.

Een informele toon is daarentegen vaak erg direct, speels, confronterend of zelfs provocerend. Hier wordt regelmatig gebruikgemaakt van emoji's (*"Message me and make* 💰🛬 *"* – T79), straattaal (*"Btc ready anders niet mij baren"* – T35) en soms scheldwoorden (*"This product is normally 550 dollars..... This is a FUCKING DEAL!"* – DW81). De verkoper positioneert zichzelf niet als professionele dienstverlener, maar spreekt potentiële aanbieders meer aan als onderdeel van de groep zijnde (*"Kom halen ah boys"* – T44). De informele toon werd dan ook vaker bij criminele aanbieders teruggezien. De potentiële koper wordt op een vrij directe manier aangesproken (*"Boys die vragen om test zonder te betalen gelijk blok bespaar aub elkaars tijd*🤝 *"* – T2, *"Direct in chat"* – T5).

Er zijn dus duidelijke verschillen tussen de twee gehanteerde tonen. De zakelijke toon legitimeert door het aanbod te structureren en formaliseren. De informele toon is meer verheerlijkend en amuserend ingestoken. Beide strategieën lijken wel hetzelfde doel te dienen, namelijk het overtuigen van de potentiële koper. De zakelijke toon speelt daarbij meer in op vertrouwen en de informele toon op emotie en impuls.

4.3.6 De toepassing van alternatieve overtuigingsstrategieën

Naast het inzetten van neutralisatietechnieken maken aanbieders in advertenties ook gebruik van andere overtuigingsstrategieën om potentiële kopers te overtuigen. In deze analyse is gekeken naar drie veelvoorkomende elementen: reputatieverwijzingen, het bieden van een klantenservice en het

bieden van kortingen en/of promoties. Deze strategieën richten zich vooral op het verhogen van vertrouwen en het aantrekkelijk maken van het aanbod.

Uit eerdere onderzoeken is gebleken dat een positieve reputatie van belang is voor aanbieders op illegale marktplaatsen. Een goede reputatie vergroot het vertrouwen van potentiële kopers en leidt daarom tot meer transacties. Aanbieders verwijzen daarom naar elementen als kwaliteit, transparantie en ervaring. Deze strategieën komen overeen met de reputatieverwijzingen van de aanbieders die zijn gevonden in deze advertenties. Een veelgebruikte tactiek is het benadrukken van de inzet en zorg waarmee producten of diensten worden geleverd. In het onderstaande citaat presenteert de aanbieder zichzelf als iemand die ver gaat om kwaliteit te garanderen:

"Do you remember when you asked when will I post crypto accounts? Well, when I said I will swim the ocean and climb mountains just to make sure you get quality stuff I meant it." – DW212

Deze aanbieder wekt de indruk dat hij er persoonlijk erg betrokken bij is, waardoor het aanbod minder afstandelijk overkomt. Dit zou de betrouwbaarheid in de ogen van potentiële kopers kunnen verhogen. Daarnaast verwijzen aanbieders regelmatig naar hun eigen ervaring en langdurige aanwezigheid op de markt als een bewijs van betrouwbaarheid, zoals in dit citaat:

"Our team has been founded in 2015 and we have a lot of experience. If you want to make someone bad, you won't find a better team! We do our job very clean, no traces will be left." – DW149

Deze aanbieder gebruikt de duur van de eigen ervaring om te laten zien dat het om een team gaat met veel ervaring, dat diensten met een hoge kwaliteit kan leveren. Het beeld van een professionele en deskundige organisatie wordt gecreëerd. Wat hier opvallend is, en ook in meerdere advertenties is gevonden, is dat er specifiek wordt verwezen naar het teamverband. De aanbieders lijken zichzelf hiermee te willen onderscheiden van amateurs. Sommige aanbieders verwijzen zelfs naar hun eigen team als een organisatie: *"We are The Wizard. A very experienced company specializing in all aspects of the Dark Web and trading on many of the Dark Web Market places."* (DW19) Sommige aanbieders verwezen ook zelf naar hun beoordelingen of klanttevredenheidsscores (*"OVER 4500+ SALES 99% POSITIVE FEEDBACK"* – DW45). Het gebruiken van reputatie als overtuigingsstrategie lijkt dus vooral gericht te zijn op het wekken van vertrouwen via ervaring, kwaliteit en toewijding.

Daarnaast is uit eerder onderzoek gebleken dat aanbieders op illegale online marktplaatsen regelmatig een klantenservice aanbieden om klanten te ondersteunen in hun aankoop. Ook in de geanalyseerde advertenties komt deze strategie naar voren: in ongeveer de helft van advertenties wordt op de een of andere manier verwezen naar een klantenservice of ondersteuning. Vaak is deze ondersteuning functioneel van aard, gericht op het oplossen van problemen die zich voordoen na aankoop: *"Full refund if not working."* (DW47) Deze aanbieder biedt een geld-terug-garantie,

waarmee de koper meer als klant wordt behandeld dan als een medepleger van het delict. Het gebruik van zulke beloften kan een gevoel van veiligheid wekken bij kopers. In sommige advertenties werd een meer uitgebreide en professionele klantenservice gepresenteerd, die doet denken aan legitieme webwinkels: *"Our team works without holidays and weekends in the London time zone 8 AM - 12 PM."* (DW137) Deze verwijzing naar een team, vaste openingstijden en een tijdzone wekt de indruk van een georganiseerde onderneming, waarbij bereikbaarheid wordt afgegeven als teken van betrouwbaarheid. Sommige aanbieders leggen de nadruk op bereikbaarheid en persoonlijke ondersteuning op een klantvriendelijke manier: *"Don't hesitate to contact me if you have any question, I'm always willing to help and solve any issue."* (DW35) Deze toon laat zien dat de aanbieder zich behulpzaam opstelt en ervoor open staat om mee te denken, dit creëert een beeld van toegankelijkheid. Dit zou de drempel voor de aankoop kunnen verlagen en kopers gerust kunnen stellen. Tegelijkertijd hanteren sommige aanbieders juist een voorwaardelijke of defensieve houding tegenover het bieden van service achteraf: *"In case you get a dead log dont forget to send me a message upload proof and send it to me to help you solve your issue, if proof is not provided there won't be chance to replacement"*. (DW39) Hier wordt de verantwoordelijkheid nadrukkelijk bij de koper gelegd; er wordt alleen ondersteuning geboden als er aantoonbaar bewijs is van een defect. De aangeboden klantenservice varieert dus van minimale probleemoplossing tot uitgebreide ondersteuning, waarbij het doel wel lijkt te zijn om het vertrouwen van de koper te winnen.

Een andere strategie die naar voren is gekomen in de advertenties, is het aanbieden van kortingen of promoties. Aanbieders doen pogingen om het aanbod aantrekkelijker te maken door tactieken als gereduceerde prijzen, beloningen voor loyale klanten of tijdelijke acties. Opvallend is dat deze benadering overeenkomt met promotietactieken op legitieme markten. Zo verwees een aanbieder expliciet naar een tijdelijke, seizoensgebonden actieperiode waarin producten verkrijgbaar waren voor een gereduceerde prijs: *"! ! ! Spring sale have already started ! ! !"* (DW124) Door uitroeptekens te gebruiken en te benadrukken dat deze deals maar een beperkte periode gelden, kan er een gevoel van urgentie gecreëerd worden. Deze urgentie werd in sommige advertenties versterkt door te benadrukken dat er sprake was van een beperkte voorraad (*"Only 3 Left In Stock"* – DW35). In andere advertenties werd een gratis extra product beloofd na aankoop (*"One Extra Item Free"* – DW6). Daarnaast werd er meermaals verwezen naar beloningen in ruil voor positieve feedback over de dienst: *"Positive feedback will be rewarded with Bonus accounts Special cashout guides and many more"* (DW10). Hiermee worden kopers gestimuleerd om bij te dragen aan de positieve reputatie van de aanbieder, in ruil voor voordelen. Sommige promoties waren gericht op het opbouwen van een langdurige klantrelatie. Een voorbeeld hiervan is de belofte van toegang tot een exclusief, besloten Telegramgroep na aankoop: *"A nice bonus - after making a purchase, each customer gets access to our private Telegram channel!"* (DW132) Hiermee wordt niet alleen een extra voordeel aangeboden, maar wordt ook een gevoel van exclusiviteit en verbondenheid met de aanbieder gecreëerd. Deze verschillende

vormen van kortingen en promoties dragen ook bij aan de professionalisering en klantgerichtheid van de advertenties.

Hoofdstuk 5: Conclusie en discussie

5.1 Conclusie en discussie

In dit onderzoek stond de volgende vraag centraal: “Op welke manier gebruiken aanbieders van Cybercrime-as-a-Service op illegale online marktplaatsen neutralisatietechnieken in hun advertenties?”. Aan de hand van een inhoudsanalyse met zowel een kwantitatief als een kwalitatief component is in kaart gebracht welke neutralisatietechnieken aanbieders gebruiken om hun illegale aanbod te legitimeren en hoe deze technieken zich verhouden tot andere advertentiekenmerken.

Een van de meest opvallende bevindingen is dat neutralisatietechnieken vaak deel uitmaken van een bredere, overtuigende communicatiestijl. Advertenties die een groepsgevoel oproepen of een zakelijke toon hanteren, bevatten significant vaker neutralisatietechnieken: in beide gevallen was de kans ruim drie keer zo hoog. Deze kenmerken bleken ook onderling sterk samen te hangen. Aanbieders die zich professioneel en als onderdeel van de gemeenschap presenteren, lijken bewust neutralisatietechnieken in te zetten om bij te dragen aan de overtuigingskracht van hun aanbod.

Verder bleek ook het type aanbieder samen te hangen met het gebruik van neutralisatietechnieken. Ondernemers gebruikten significant minder neutralisatietechnieken dan criminelen. Mogelijk komt dit doordat zij hun diensten nadrukkelijker legitimeren, onder andere via reputatieverwijzingen en klantenservices, waardoor morele rechtvaardiging minder nodig is. Het gebruik van alternatieve overtuigingsstrategieën hing verder niet significant samen met het gebruik van neutralisatietechnieken, wanneer er werd gecontroleerd voor andere kenmerken zoals de toon en het platform.

De gehanteerde toon in de advertenties sluit ook aan bij de bevindingen uit het theoretisch kader. De resultaten lieten zien dat advertenties op het dark web voornamelijk een zakelijke toon hanteren en gebruikmaken van tactieken die kenmerkend zijn voor legale markten. De professionele standaarden die in legitieme markten worden gebruikt om het vertrouwen van de consument te winnen, zoals snelle levering, een bereikbare klantenservice en transparantie, worden ook hier teruggezien. Afgezien van het illegale karakter van het aanbod zijn er dus veel overeenkomsten met het legale aanbod. Advertenties op Telegram daarentegen zijn aanzienlijk informeler van aard, met voornamelijk korte beschrijvingen en meer gebruik van straattaal. In eerder onderzoek naar aanbieders op het dark web werd ook vastgesteld dat zij vaker legitieme businessmodellen imiteren en voor Telegram is in recente literatuur ook de communicatie gekenmerkt door informele taal en het gebruik van emoji’s.

Uit de analyse van de neutralisatietechnieken bleek dat zij op doeltreffende wijze worden ingezet. De neutralisatietechniek “het bedenken van nieuwe feiten” werd het vaakst gebruikt, waarbij het aanbod werd gepresenteerd als legitiem, educatief of zelfs als een carrièrekans. Daarnaast werd de techniek “de schuld geven aan beperkte keuzes” vaak gebruikt, waarbij er voornamelijk verleiding werd gecreëerd door rijkdom te beloven. Ook de techniek “het reduceren van geldende normen tot

feiten" kwam vaak voor. Hier werden criminele handelingen gepresenteerd als kunstvorm of strategisch spel, waardoor de morele implicaties ervan werden vervaagd. Deze neutralisatietechnieken schetsen dus een beeld waarin deviant gedrag is genormaliseerd en morele bezwaren zijn afgezwakt.

Dit sluit ook aan op de analyse over de context waarin de advertenties zijn geplaatst. Die liet zien dat het creëren van een groepsgevoel en een gemeenschap een belangrijke aanvulling zijn op het gebruiken van neutralisatietechnieken. De advertenties zijn niet alleen commerciële uitingen, maar maken deel uit van een online subcultuur waarin met name jonge mannen worden aangesproken en deviant gedrag wordt genormaliseerd. Dit blijkt uit het gebruik van straattaal (zoals "mapsers" en "F-game") en verwijzingen naar broederschap met termen als "boys", waarmee expliciet aansluiting wordt gezocht bij een jong, mannelijk publiek. Ook vrouwonvriendelijke uitingen kwamen in verschillende advertenties voor, wat duidt op een subcultuur waarin traditionele opvattingen over mannelijkheid worden aangehouden. Door deze elementen met elkaar te combineren, presenteren aanbieders hun diensten niet alleen als commercieel interessant, maar ook als sociaal geaccepteerd binnen de groep.

Deze rol van het groepsgevoel is een opvallend nieuw inzicht. Hoewel eerder onderzoek al heeft aangetoond dat het schetsen van bepaalde groepsnormen kan aanzetten tot conformerend gedrag, is de toepassing hiervan in advertenties voor online criminaliteit nog niet eerder geanalyseerd. De bevinding dat neutralisatietechnieken juist vaker voorkomen wanneer er een groepsgevoel wordt gecreëerd, kan wijzen op een strategische wijze waarmee aanbieders de morele drempel voor potentiële kopers proberen te verlagen aan de hand van een gemeenschapsgevoel. Het verwijzen naar een bredere gemeenschap schept niet alleen het beeld van andere geldende normen, maar ook een gevoel van vertrouwen en loyaliteit.

De voorgekomen neutralisatietechnieken in de verzamelde data bleken ook goed te passen bij de indeling van de technieken zoals voorgesteld door Kaptein & Van Helvoort (2019). De verschillende technieken uit het model konden duidelijk herkend worden in de manier waarop CaaS-aanbieders hun diensten presenteren. Dit strategische gebruik is tot nu toe nog weinig onderzocht, maar blijkt in deze context veel voor te komen. Dit duidt erop dat neutralisatietechnieken niet alleen interne verdedigingsmechanismen zijn, maar ook strategische middelen kunnen zijn binnen een bredere overtuigingsstrategie in illegale online marktplaatsen. Hoewel de motivatie van de aanbieders met dit onderzoek niet is vast te stellen, schetst dit wel het beeld dat neutralisatietechnieken op interactioneel niveau in een bredere communicatiestijl worden toegepast, waarbij legitimiteit en vertrouwen ook centraal staan.

Deze verschillen in toon en stijl sluiten ook aan bij de drie hypothesen die zijn opgesteld op basis van eerder onderzoek. De eerste twee hypothesen waren gebaseerd op mogelijke verschillen tussen beginnende en ervaren criminelen op basis van de literatuur. Er werd verwacht dat de doelgroep van beginnende criminelen meer behoefte zou hebben aan morele rechtvaardiging en dat dit zich zou uiten via het gebruik van neutralisatietechnieken op laagdrempelige platforms en bij eenvoudige

delicten. De resultaten lieten echter een ander beeld zien. Advertenties op het dark web bevatten juist meer neutralisatietechnieken dan advertenties op Telegram. Een mogelijke verklaring hiervoor is de hogere mate van professionaliteit die zichtbaar is in advertenties van aanbieders op het dark web. Deze CaaS-aanbieders passen meer strategieën toe om hun aanbod legitiem te laten overkomen, zoals garanties, klantenservice en transparantie. Telegram-advertenties waren daarentegen korter, informeler en minder commercieel opgesteld. Voor beginnende kopers zouden juist de professioneel ogende advertenties op het dark web aantrekkelijker zijn, omdat deze meer vertrouwen wekken. Een andere mogelijke verklaring ligt aan de kant van de aanbieders zelf. Het is aannemelijk dat meer ervaren en professionele aanbieders hun diensten aanbieden via meer georganiseerde platforms zoals het dark web en ook vaker complexere delicten aanbieden. Deze aanbieders hebben vanwege ervaring mogelijk ook meer inzicht in hoe een dienst overtuigend gepresenteerd kan worden en zetten daarom bewust neutralisatietechnieken in. Het zijn dus mogelijk niet alleen de typen kopers die verschillen per platform en delict, maar ook de typen aanbieders die daar opereren.

Er is ook geen significante associatie gevonden tussen de moeilijkheidsgraad van het delict en het gebruik van neutralisatietechnieken. Wel werden er bij gecompliceerde delicten juist meer neutralisatietechnieken gebruikt dan bij eenvoudige delicten. Dit zou kunnen samenhangen met de toegedane schade die over het algemeen groter is bij gecompliceerde delicten dan bij eenvoudige delicten. De ernst van het delict vraagt mogelijk om een sterkere rechtvaardiging. De aanbieder zelf is ook op de hoogte van de ernst van het delict en zet daarom wellicht sneller neutralisatietechnieken in als strategisch middel om zijn diensten overtuigender en acceptabeler te presenteren aan een zo breed mogelijke groep potentiële kopers. De hogere mate van neutralisatietechnieken bij gecompliceerde delicten zou dus een strategische keuze van aanbieders kunnen zijn om de morele drempel te verlagen voor een zo breed mogelijke doelgroep.

De derde hypothese ging uit van het idee dat er meer neutralisatietechnieken worden gebruikt als het doelwit van het delict een persoon is in plaats van een organisatie, omdat er bij een kleinere afstand tot het slachtoffer meer morele rechtvaardiging nodig is. Hoewel de kwantitatieve toetsing van deze hypothese niet op een betrouwbare manier kon worden uitgevoerd vanwege het lage aantal advertenties waarin expliciet een doelwit werd genoemd, bood de kwalitatieve analyse wel relevante inzichten. Hieruit bleek dat de neutralisatietechniek ‘een beroep doen op een belangrijkere norm’ vaak werd gebruikt om het maken van potentiële persoonlijke slachtoffers te rechtvaardigen, waarbij het delict werd voorgesteld als een vorm van zelfbescherming of vergelding. Dit wijst erop dat aanbieders een poging doen om een morele afweging te presenteren die het individuele slachtofferschap overschaduwt.

Dit onderzoek laat zien dat neutralisatietechnieken een belangrijk element zijn voor aanbieders van Cybercrime-as-a-Service om hun illegale aanbod op een aantrekkelijke en legitieme manier te presenteren aan potentiële kopers. Deze technieken worden niet willekeurig gebruikt, maar hangen samen met de rol die de aanbieder aanneemt, de toon van de advertentie en het creëren van een

groepsgevoel. Dit heeft relevante implicaties voor zowel de wetenschappelijke als de praktijkgerichte benadering van online criminaliteit. Het laat namelijk zien dat neutralisatietechnieken niet alleen door criminelen zelf worden gebruikt, maar ook strategisch worden ingezet als overtuigingsmiddel in de interactie met de koper. Daarmee leveren deze bevindingen een bijdrage aan de bestaande literatuur over neutralisatietechnieken, door duidelijk te maken dat deze technieken ook een functionele rol kunnen spelen in de communicatie van online criminelen, gericht op het verlagen van drempels tot deviant gedrag bij anderen.

5.1.1 Beperkingen

Dit onderzoek kent enkele beperkingen die mogelijk invloed hebben op de generaliseerbaarheid van de bevindingen. Vanwege de beperkte tijd die beschikbaar was, vond de dataverzameling plaats over een periode van drie weken. Gedurende deze periode zijn alle advertenties verzameld die aan de vooraf gestelde criteria voldeden. Dit resulteerde in een steekproef van 369 advertenties, wat voldoende is gebleken om algemene patronen en significante verbanden te analyseren binnen de totale steekproef. Echter, bij bepaalde uitsplitsingen, zoals naar het type doelwit of naar de moeilijkheidsgraad van het aangeboden delict, bleek het aantal relevante advertenties te beperkt om robuuste statistische toetsen toe te passen. Hierdoor kon één van de hypothesen niet getoetst worden. Deze beperkte groottes betekenen dat de generaliseerbaarheid van de bevindingen omtrent specifieke advertentiekenmerken met enige voorzichtigheid moet worden geïnterpreteerd. Voor toekomstig onderzoek is het aan te bevelen om de dataverzameling over een langere periode uit te spreiden, zodat een grotere steekproef ontstaat. Dit zou het niet alleen mogelijk maken om kenmerken te bestuderen die minder vaak voorkomen, maar ook om de betrouwbaarheid en generaliseerbaarheid van de uitspraken over de subgroepen te vergroten.

Daarnaast richtte dit onderzoek zich uitsluitend op de inhoudelijke analyse van de advertenties. Er kunnen daarom geen uitspraken worden gedaan over de effectiviteit van neutralisatietechnieken en het beïnvloeden van koopgedrag. Het blijft onduidelijk of deze technieken de advertenties daadwerkelijk aantrekkelijker maken voor potentiële kopers. Toekomstig onderzoek zou kunnen uitwijzen in hoeverre neutralisatietechnieken bijdragen aan het succes van een advertentie, bijvoorbeeld door transactiegegevens of de hoogte van prijzen te analyseren als indicatoren voor populariteit. Ook een longitudinale benadering kan hierbij waardevol zijn. Technieken die effectief blijken in het overtuigen van kopers zullen vermoedelijk door aanbieders worden herhaald en mogelijk overgenomen worden door anderen, wat leidt tot een bredere verspreiding van de techniek in de markt. Op die manier kan inzicht worden verkregen in welke neutralisatietechnieken zich op termijn ontwikkelen tot effectieve overtuigingsmiddelen binnen de illegale online marktplaatsen.

5.1.2 Aanbevelingen

Als dit fenomeen, waarin aanbieders zich voordoen als legitiem aan de hand van neutralisatietechnieken en commerciële overtuigingsstrategieën, zich blijft voortzetten, zou dit kunnen bijdragen aan de algehele normalisering van online criminaliteit. Door deviant gedrag te presenteren als technisch, onschuldig of zelfs noodzakelijk, wordt de morele drempel tot deelname verlaagd. Online criminaliteit krijgt hierdoor steeds meer het karakter van een reguliere activiteit, in plaats van een normoverschrijdende handeling. Vooral voor beginnende of gelegenheidscriminelen wordt de stap naar het plegen van een delict kleiner, omdat de context waarin zij opereren het delict als iets gebruikelijks schetst. Als deze ontwikkeling zich ongestoord voortzet, is het voor de hand liggend dat de huidige toename in online criminaliteit zich ook blijft voortzetten. Dit benadrukt het belang van beleidsaanknopingspunten en verdere aandacht voor de manier waarop online criminaliteit wordt gepresenteerd binnen online omgevingen. Op basis van de bevindingen uit dit onderzoek kunnen aanbevelingen worden gedaan voor zowel vervolgonderzoek als voor de praktijk.

Bij de beperkingen werd reeds aangeraden om hetzelfde onderzoek nogmaals uit te voeren bij een grotere steekproef, om de resultaten nog meer te onderbouwen en de generaliseerbaarheid van het onderzoek te vergroten. Daarnaast heeft dit onderzoek al gedemonstreerd dat neutralisatietechnieken een rol spelen in de manier waarin aanbieders hun potentiële kopers proberen te overtuigen om hun diensten aan te schaffen. Een interessante vervolgstap zou zijn om te onderzoeken of deze neutralisatietechnieken daadwerkelijk invloed uitoefenen op het gedrag van kopers.

Een ander interessant aanknopingspunt voor vervolgonderzoek is de rol van memes binnen het creëren en versterken van het gemeenschapsgevoel op illegale online marktplaatsen. Aangezien deze online omgeving functioneert als een eigen subcultuur, is er ook sprake van een unieke vorm van communicatie waarin memes en andere “inside jokes” een rol spelen. Zij dragen namelijk ook de groepsnormen en identiteit van de subcultuur uit. Toekomstig onderzoek zou kunnen analyseren welke typen memes er worden gedeeld op illegale online marktplaatsen. Er kan een vergelijking worden gemaakt met andere platforms waarop dezelfde memes circuleren, zoals groepen op Reddit of Discord. Dit kan inzicht bieden in de bredere infrastructuur van deze subcultuur en de onderlinge verbondenheid van gebruikers op meerdere kanalen. Mogelijk kunnen er ook duidelijkere profielen worden opgesteld van degenen die behoren tot deze online criminele gemeenschap.

Voor de praktijk is het allereerst aan te bevelen om binnen de bestrijding van online criminaliteit nadrukkelijk in te zetten op bewustwording bij handhavers, toezichthouders, jongerenwerkers en andere professionals binnen het werkveld. Dit onderzoek kan een ondersteunende rol spelen bij het herkennen van strategisch taalgebruik dat zich richt op het normaliseren van online criminaliteit binnen CaaS-advertenties. Door inzicht te krijgen in hoe aanbieders moreel weerstand verlagen en crimineel gedrag presenteren als legitiem of sociaal wenselijk, kunnen deze professionals beter begrijpen hoe jongeren in aanraking kunnen komen met online criminaliteit zonder dit als crimineel te ervaren. Dit kan ook helpen in de manier waarop jongerenwerkers en opsporingsinstanties

signaleren wanneer jongeren mogelijk negatief beïnvloed worden door de online context. Met meer achtergrondinformatie over wat er zich afspeelt op deze illegale online marktplaatsen, kan de gespreksvoering met jongeren mogelijk bevorderd worden.

Verder kan het onderzoek ook bijdragen aan preventieve interventies. Bijvoorbeeld in de vorm van bewustwordingscampagnes die zich richten op potentiële kopers. Om het narratief dat aanbieders online creëren te doorbreken, zouden gerichte campagnes kunnen worden ontwikkeld die de andere kant van het verhaal zichtbaar maken. In deze campagnes kan worden benadrukt dat ook de online aangeboden diensten en producten die op het eerste gezicht onschuldig of legitiem lijken, zoals de tools die zogenaamd voor ‘educatieve doeleinden’ bestemd zijn, daadwerkelijk deel uitmaken van een criminele handeling. Er zijn risico’s aan verbonden voor zowel slachtoffers als de koper van de dienst of het product. Ook al maakt de koper in sommige gevallen slechts een bedrag over en doet de aanbieder de rest, er zitten nog steeds juridische consequenties aan deze handeling verbonden. Door het publiek te informeren van deze consequenties die de aanbieders verbergen en minimaliseren, kan worden bijgedragen aan het verminderen van de aantrekkingskracht van deze advertenties.

Literatuurlijst

Ablon, L., Libicki, M.C., Abler, A.M., Rand Corporation, Acquisition and Technology Policy Center, Juniper Networks, Inc, & Rand Corporation National Security Research Division. (2014). *Markets for cybercrime tools and stolen data: hackers' bazaar*. RAND Corporation.

Achuthan, K., Khobragade, S., & Kowalski, R. (2025). Cybercrime through the public lens: a longitudinal analysis. *Humanities and Social Sciences Communications*, *12*(1). https://doi.org/10.1057/s41599-025-04459-x

Akyazi, U., Van Eeten, M., Gañán, C.H. (2021). *Measuring Cybercrime as a Service (CaaS) Offerings in a Cybercrime Forum*. Paper presented at Workshop on the Economics of Information Security.

Bossler, A.M. (2021). Neutralizing Cyber Attacks: Techniques of Neutralization and Willingness to Commit Cyber Attacks. *American Journal of Criminal Justice: The Journal of the Southern Criminal Justice Association*, *46*(6), 911–934. https://doi.org/10.1007/s12103-021-09654-5

Brewer, R., Fox, S., Miller, C. (2020). Applying the Techniques of Neutralization to the Study of Cybercrime. In: Holt, T., Bossler, A. (Red.) *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 547-563). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-78440-3_22

Centraal Bureau voor de Statistiek. (2023, 4 augustus). *Ruim 2 duizend bedrijven in 2021 de dupe van ransomware*. Geraadpleegd op 14 april 2025, van https://www.cbs.nl/nl-nl/nieuws/2023/31/ruim-2-duizend-bedrijven-in-2021-de-dupe-van-ransomware

Centraal Bureau voor de Statistiek. (2025, 15 april). *Online Veiligheid en Criminaliteit 2024.* Geraadpleegd op 24 juni 2025, van https://www.cbs.nl/nl-nl/longread/rapportages/2025/online-veiligheid-en-criminaliteit-2024/7-online-criminaliteit-totaal#:~:text=Krap%201%20procent%20werd%20slachtoffer,van%20online%20oplichting%20en%20fraude.

Cialdini, R. B. (2021). *Influence, new and expanded: the psychology of persuasion* (First Harper Business new and expanded hardcover edition). Harper Business, an imprint of HarperCollinsPublishers.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588–608.

Connolly, L.Y., Borrion, H., & Arief, B. (2025). Ransomware crime through the lens of neutralisation theory. *European Journal of Criminology*. https://doi.org/10.1177/14773708251320464

Europol. (2024, 11 december). *Law enforcement shuts down 27 DDoS booters ahead of annual Christmas attacks*. Geraadpleegd op 14 april 2025, van https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-shuts-down-27-ddos-booters-ahead-of-annual-christmas-attacks

Fisher, T., Pieri, Z., Howell, C.J., O'Malley, R., Tremblay, L., & Dawoud, M. (2025). Vendor communication themes in darknet Ransomware-as-a-Service (RaaS) advertisements. *Computers in Human Behavior*, *165*. https://doi.org/10.1016/j.chb.2025.108571

Furnell, S. (2020). Technology Use, Abuse, and Public Perceptions of Cybercrime. In: Holt, T., Bossler, A. (Red.) *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 46-65). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-78440-3_9

Ganguli, P. (2024). *The Rise of Cybercrime-as-a-Service: Implications and Countermeasures.* Heritage Group of Institutions.

Goldsmith, A., & Brewer, R. (2015). Digital drift and the criminal interaction order. *Theoretical Criminology*, *19*(1), 112–130. https://doi.org/10.1177/1362480614538645

Holt, T.J. (2019). Cybercrime subcultures: Contextualizing offenders and the nature of the offence. In Leukfeldt, R., & Holt, T.J. (Eds.), *The Human Factor of Cybercrime* (pp. 159-172). Routledge.

Holt, T.J., Lee, J.R., & O'Dell, E. (2022). Assessing the Practices of Online Counterfeit Currency Vendors. *Crime & Delinquency*. https://doi.org/10.1177/00111287221134047

Huang K., Siegel M., & Madnick S. (2018). Systematically understanding the cyber attack business: A survey. *ACM Computing Surveys*, *51*(4). https://doi.org/10.1145/3199674

Hyslip, T.S. (2020). Cybercrime-as-a-Service Operations. In: Holt, T., Bossler, A. (Red.) *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 815-846). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-78440-3_22

Junger, M., Hartel, H., Montoya, L., & Heydari, M. (2017). Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in Europe. *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment, Cyber SA 2017, June.*

Kaptein, M., & van Helvoort, M. (2019). A Model of Neutralization Techniques. *Deviant Behavior*, *40*(10), 1260–1285. https://doi.org/10.1080/01639625.2018.1491696

Klucharev, V., Smidts, A., & Fernández, G. (2008). Brain mechanisms of persuasion: how 'expert power' modulates memory and attitudes. *Social Cognitive and Affective Neuroscience*, *3*(4), 353–366. https://doi.org/10.1093/scan/nsn022

Krippendorff, K. (2019). *Content analysis: an introduction to its methodology* (Fourth edition). SAGE.

Kshetri, N., & Chauhan, P.S. (2023). Ransomware as a Service Kit: A Novel Cybercrime Strategy to Monetize Victims' Data. *Computer*, *56*(10), 102–106. https://doi.org/10.1109/MC.2023.3298072

Laferrière, D., & Décary-Hétu, D. (2023). Examining the Uncharted Dark Web: Trust Signalling on

Single Vendor Shops. *Deviant Behavior*, *44*(1), 37–56. https://doi.org/10.1080/01639625.2021.2011479

Leukfeldt, R., Kleemans, E., & Stol, W. (2017). The Use of Online Crime Markets by Cybercriminal Networks: A View From Within. *American Behavioral Scientist, 61*(11), 1387-1402. https://doi-org.proxy-ub.rug.nl/10.1177/0002764217734267

Manky, D. (2013). Cybercrime as a service: a very modern business. *Computer Fraud & Security*, *2013*(6), 9–13. https://doi.org/10.1016/S1361-3723(13)70053-8

Maruna, S., & Copes, H. (2005). What Have We Learned from Five Decades of Neutralization Research? *Crime and Justice*, *32*, 221–320.

Matza, D. (1964). *Delinquency and Drift*. Wiley.

Mogaji, E. (2017). *Reaching out to African Caribbeans: content analysis of UK cancer charity YouTube advertisements*. SAGE Publications Ltd. https://dx.doi.org/10.4135/9781526419644

Nathan, M. (2020). Credential stuffing: new tools and stolen data drive continued attacks. *Computer Fraud & Security*, *2020*(12), 18–19. https://doi.org/10.1016/S1361-3723(20)30130-5

Nederlandse Politie. (2024). *Online fraude in beeld: Fenomeenbeeld 2024*. Geraadpleegd op 11 maart 2025, van https://www.politie.nl/binaries/content/assets/politie/onderwerpen/publicaties/2025/fenomeenbeeld-online-fraude-in-infographics.pdf

Nederlandse Politie. (z.d.). *Wat zijn F-games?* Geraadpleegd op 30 juni 2025, van https://www.politie.nl/informatie/wat-zijn-f-games.html

Neuendorf, K. A., Skalski, P. D., Cajigas, J. A., & Allen, J. C. (2017). *The content analysis guidebook* (Second edition). SAGE.

NOS. (2022, 14 december). *Dit zijn de jongeren achter online oplichting: 'Het is een soort hype'*. Geraadpleegd op 30 juni 2025, van https://nos.nl/artikel/2456409-dit-zijn-de-jongeren-achter-online-oplichting-het-is-een-soort-hype

NOS. (2024, 9 juli). *Hacker met 'Zwitsers zakmes voor cybercrime' voor de rechter*. Geraadpleegd op 14 april 2025, van https://nos.nl/artikel/2528055-hacker-met-zwitsers-zakmes-voor-cybercrime-voor-de-rechter

NOS. (2024, 25 januari). *Miljoenen drugsadvertenties op Telegram, platform laat handel ongemoeid*. Geraadpleegd op 8 april 2025, van https://nos.nl/artikel/2506160-miljoenen-drugsadvertenties-op-telegram-platform-laat-handel-ongemoeid

NOS. (2025, 18 maart). *Meer jonge mannen vrouwonvriendelijk: serie 'Adolescence' toont invloed manosphere*. Geraadpleegd op 30 juni 2025, van https://nos.nl/nieuwsuur/artikel/2560212-meer-jonge-mannen-vrouwonvriendelijk-serie-adolescence-toont-invloed-manosphere

Openbaar Ministerie. (z.d.). *Cybercrime*. Geraadpleegd op 24 juni 2025, van https://www.om.nl/onderwerpen/cybercrime

Przepiorka, W., Norbutas, L., & Corten, R. (2017). Order without Law: Reputation Promotes

Cooperation in a Cryptomarket for Illegal Drugs. *European Sociological Review*, *33*(6), 752–764. https://doi.org/10.1093/esr/jcx072

Ridley, A., & Selck-Paulsson, D. (2022, 11 oktober). Reframing ransomware as a 'service' for the victim: the denial of injury neutralization technique. *Orange Cyberdefense*. Geraadpleegd op 2 april 2025, van https://www.orangecyberdefense.com/global/blog/research/reframing-ransomware-as-a-service-for-the-victim-the-denial-of-injury-neutralization-technique

Rijksoverheid. (z.d.). *Cybercrime bestrijden*. Geraadpleegd op 29 maart 2025, van https://www.rijksoverheid.nl/onderwerpen/cybercrime-en-cybersecurity/cybercriminaliteit-bestrijden

Roks, R., & Monshouwer, N. (2020). F-gamers die 'mapsen', 'swipen' en 'bonken': een netnografisch onderzoek naar fraude en oplichting op Telegram Messenger. *Justitiële Verkenningen*, *46*(2), 44–58.

Saleem, J., Islam, R., & Kabir, M.A. (2022). The Anonymity of the Dark Web: A Survey. *IEEE Access*, *10*. https://doi.org/10.1109/ACCESS.2022.3161547

Straattaal Woordenboek. (z.d.). *Smibanese straattaal*. Geraadpleegd op 30 juni 2025, van https://www.straattaalwoordenboek.nl/smibanese-straattaal/

Sykes, G.M., & Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review*, *22*(6), 664–670.

Telegram. (z.d.). *FAQ for the technically inclined.* Geraadpleegd op 25 maart 2025, van https://core.telegram.org/techfaq#q-how-does-end-to-end-encryption-work-in-mtproto

Tidy, J. (2024, 31 augustus). *Telegram: 'The dark web in your pocket'*. BBC World Service. Geraadpleegd op 24 juni 2025, van https://www.bbc.com/news/articles/cdey4prn3e1o

United Nations. (z.d.). *Darknet investigations.* Geraadpleegd op 8 april 2025, van https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/detectandrespond/investigation/darknet.html

Walters, G. D., Runell, L., & Kremser, J. (2023). Drifters and Delinquents: Commitment and Neutralization in Low- and High-Rate Offending Early Adolescents. *Crime & Delinquency*, *69*(1), 66–87. https://doi.org/10.1177/00111287211039992

Weale, S. (2023, 2 februari). *'We see misogyny every day': how Andrew Tate's twisted ideology infiltrated British schools.* The Guardian. Geraadpleegd op 30 juni 2025, van https://www.theguardian.com/society/2023/feb/02/andrew-tate-twisted-ideology-infiltrated-british-schools

Weulen Kranenbarg, M., & Leukfeldt, R. (2021). *Cybercrime in context: the human factor in victimization, offending, and policing*. Springer. https://doi.org/10.1007/978-3-030-60527-8

Bijlage 1: Overzicht CaaS-vormen en moeilijkheidsgraad

Tabel 1.1: Overzicht van alle CaaS-vormen met hun definitie en moeilijkheidsgraad

CaaS-vorm	Definitie	Moeilijkheidsgraad
Accountinbraak- en verkoop*	Het hacken van accounts anders dan bankaccounts, zoals sociale media of e-mailaccounts, om toegang te verkrijgen tot privé-gegevens of handelingen te verrichten	Eenvoudig
Botnet huren/kopen	Toegang verkrijgen tot geïnfecteerde computers om gegevens te stelen of delicten van te plegen (Hyslip, 2020)	Eenvoudig
Betaalmiddelenfraude	Verkoop van gestolen betaalgegevens (Hyslip, 2020)	Eenvoudig
Credential stuffing	Een geautomatiseerd proces om gelekte inloggegevens in te voeren (Nathan, 2020)	Eenvoudig
Gegevensmanipulatie in bestaande systemen*	Bestaande systemen waarin data wordt opgeslagen worden gehackt, waarna de data wordt aangepast om af te wijken van de werkelijkheid.	Eenvoudig
Geldbedragen van gehackte accounts	Geldbedragen worden tegen betaling overgemaakt vanaf eerder gehackte bank- of betaalaccounts naar de koper.	Eenvoudig
DDoS-aanval (Stressers en booters)	Tijdelijk platleggen van een website door deze te overbelasten met veel verkeer (Ganguli, 2024)	Eenvoudig
Digitale opsporing*	Er wordt informatie over een persoon achterhaald zonder toestemming, zoals iemands IP-adres of live locatie.	Eenvoudig
Spamdiensten	Grote hoeveelheden misleidende spamberichten versturen om geld of informatie te verkrijgen (Hyslip, 2020)	Eenvoudig
Phishing	Slachtoffers misleiden om vertrouwelijke informatie in te vullen in valse berichten/websites (Ganguli, 2024)	Eenvoudig
Ransomware	Bestanden/systemen van slachtoffers versleutelen en losgeld eisen om toegang te herstellen (Fisher et al., 2025)	Eenvoudig
Reputatiediensten	Kunstmatig verbeteren van een online reputatie met bijvoorbeeld valse reviews of volgers (Akyazi et al., 2021)	Eenvoudig
Verificatiediensten	Omzeilen van verificatieprocessen op telefoons (Akyazi et al., 2021)	Eenvoudig
Botnet framework	Verkoop van software om zelf een botnet op te zetten (Hyslip, 2020)	Gecompliceerd
Bulletproof hosting	Het beschermd hosten van een website waar niet wordt meegewerkt aan verzoeken van opsporingsdiensten (Hyslip, 2020)	Gecompliceerd
Exploit kits	Software voor het binnendringen in systemen via kwetsbaarheden in software/hardware (Huang et al., 2018)	Gecompliceerd

Malware/payload	Infecteren van systemen om data te stelen, systemen over te nemen of slachtoffers te bespioneren (Hyslip, 2020)	Gecompliceerd
Obfuscation	Verhullen van malware om detectie te voorkomen (Akyazi et al., 2021)	Gecompliceerd
Remote access trojan	Het op afstand binnendringen in en langdurig overnemen van het systeem van een slachtoffer (Huang et al., 2018)	Gecompliceerd

*Deze diensten/producten zijn toegevoegd op basis van de inhoud uit de advertenties zelf.

Bijlage 2: Overzicht gebruikte sites en groepen

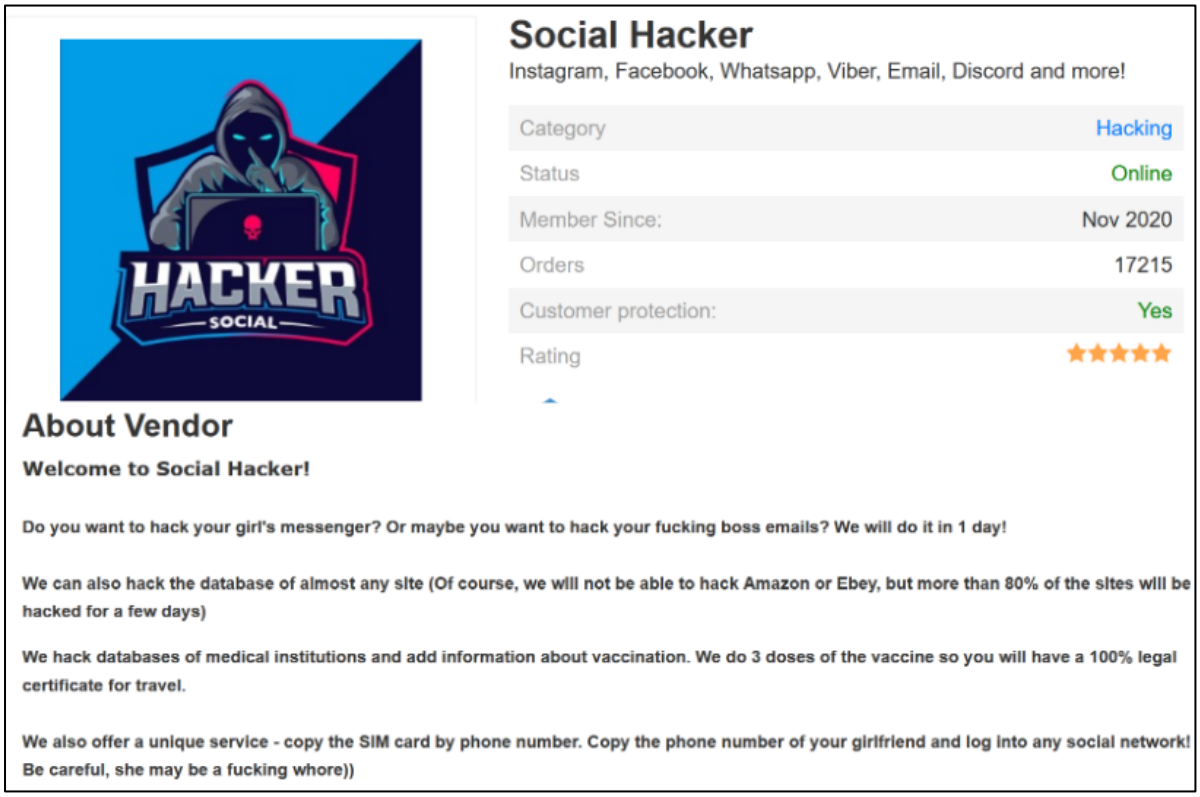
Tabel 2.1: Overzicht van alle gebruikte dark websites en Telegram groepen

Dark websites	**Telegram groepen**
Deep market	FRAUDEHANDEL
Black market	010 bonkers
Torbay	Exploits Service Chat
Drughub	FRAUDE BETAALD!
Tor Buy	F Game Chat
Trust Market	Mapsers/Orgiimapsers*
Hidden Marketplace	ONLY FR@UD
Undermarket 2.5	Bonkers&Rakkers*
White House Market	DjoenGG
Dark Onion Market	HANDEL
E-Market	Crypto Handel
Pablo Escobar Market	Darkhandel

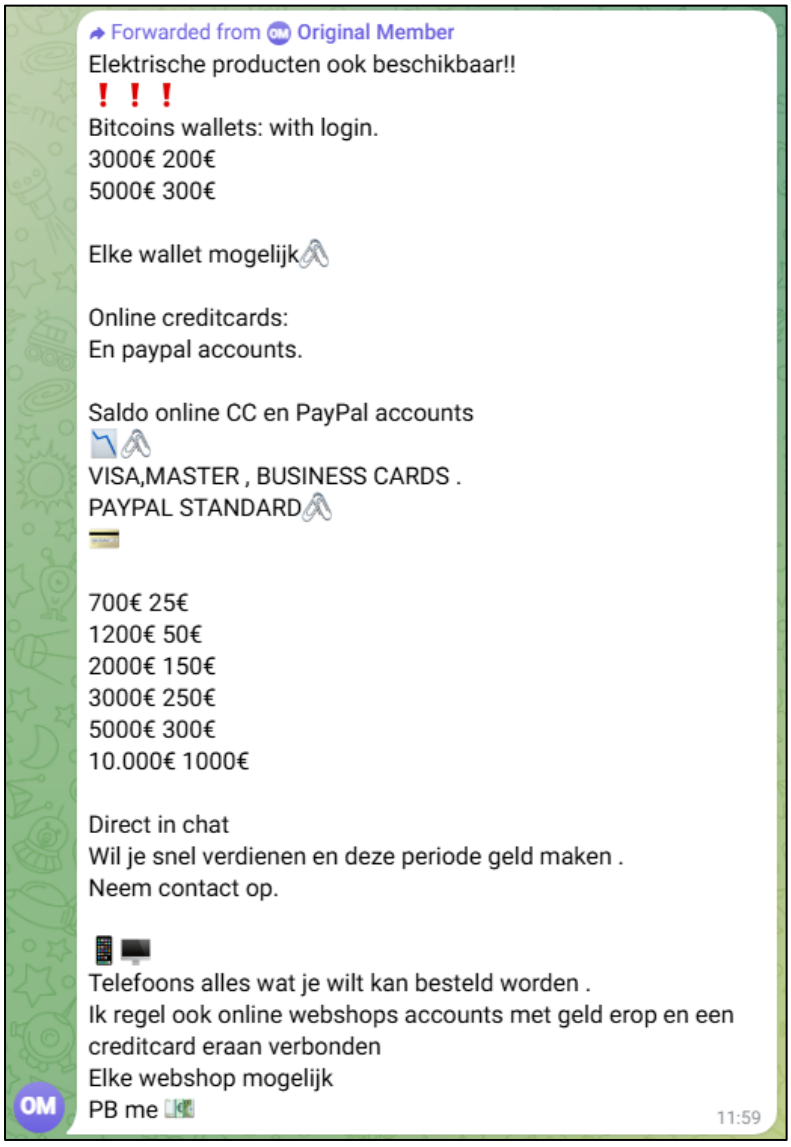
*Deze groepen zijn offline gegaan tijdens de periode van dataverzameling.

Bijlage 3: Voorbeelden weergave advertenties

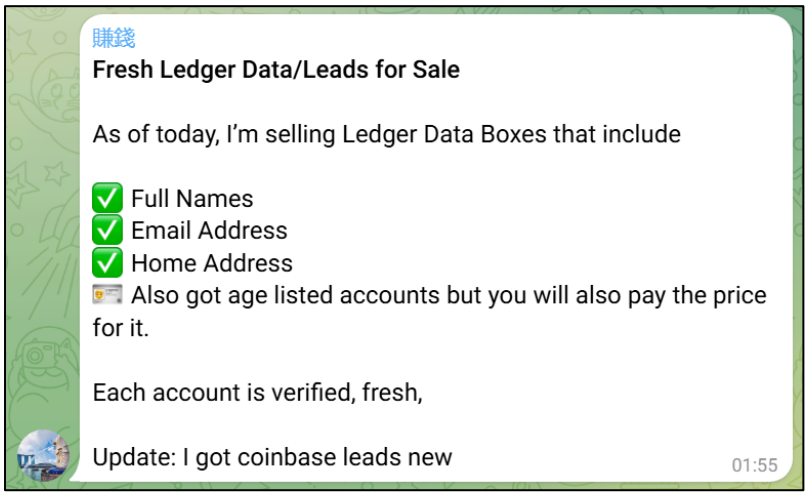
Figuur 3.1: Visuele weergave willekeurige dark web-advertentie



Figuur 3.2: Visuele weergave willekeurige Nederlandstalige Telegram-advertentie



Figuur 3.3: Visuele weergave willekeurige Engelstalige Telegram-advertentie



Bijlage 4: Uitkomsten betrouwbaarheidsanalyse

Tabel 4.1: Betrouwbaarheidscoëfficiënt per kwantitatieve variabele (N =50)

Variabele	*Kappa*	*SE*	*T*	*p-waarde*	*Interpretatie*
Taal	0,947	0,053	6,704	<0,001	Zeer goed
Aangeboden diensten/producten	0,863	0,051	18,938	<0,001	Zeer goed
Neutralisatietechniek 1	0,744	0,085	9,633	<0,001	Acceptabel
Neutralisatietechniek 2	1,000	0,000	10,794	<0,001	Zeer goed
Neutralisatietechniek 3	1,000	0,000	7,071	<0,001	Zeer goed
Type aanbieder	0,788	0,063	14,832	<0,001	Acceptabel
Aanspreekvorm	0,970	0,030	9,974	<0,001	Zeer goed
Benoeming type doelwit	0,847	0,150	6,058	<0,001	Zeer goed
Type doelwit	0,850	0,147	8,743	<0,001	Zeer goed
Toon	0,669	0,106	4,796	<0,001	Acceptabel
Aanwezigheid reputatie	0,729	0,100	5,354	<0,001	Acceptabel
Aanwezigheid klantenservice	0,841	0,075	6,022	<0,001	Zeer goed
Aanwezigheid kortingen/promoties	0,891	0,075	6,335	<0,001	Zeer goed

Bijlage 5: Codeboek

Codegroep	Code	Omschrijving	Voorbeeld(en)
Platform	Telegram	De advertentie wordt aangeboden op Telegram.	-
	Dark web	De advertentie wordt aangeboden op het dark web.	-
Taal	Nederlands	De hoofdzakelijke taal van de advertentie is Nederlands. Dit geldt ook wanneer de tekst enkele buitenlandse woorden bevat, als het overgrote deel van de advertentie Nederlands is.	“Stop met broke zijn.” “Wij leveren snel. Check onze reviews.”
	Engels	De hoofdzakelijke taal van de advertentie is Engels. Dit geldt ook wanneer de tekst enkele buitenlandse woorden bevat, als het overgrote deel van de advertentie Engels is.	“Secure your targets now, binnen 24 uur.” “Fast and undetectable tool available now. Kein Risiko. 100% secure.”
Aangeboden dienst/product (1), (2), (3), (4), (5) en (6)	Accountinbraak en -verkoop	De advertentie biedt de dienst om andermans account te hacken om toegang te leveren tot diens privé-gegevens, om handelingen vanuit diens account te verrichten (zoals oplichting of aankopen) of om schade te verrichten. Dit betreft alle accounts behalve bankaccounts, zoals sociale media of e-mailaccounts. Je kunt betalen om toegang te verkrijgen tot het account van een specifiek persoon, maar je kunt ook toegang kopen voor een reeds gehackt account.	“Do you want to hack your girl’s accounts?” “Haal het Insta-account van je vijanden offline.”
	Botnet huren/kopen	De advertentie biedt toegang tot een netwerk van reeds geïnfecteerde apparaten (botnets), om hiervan gegevens te	“Huur krachtig botnet met 5.000 nodes, direct inzetbaar.”

	stelen of te gebruiken om delicten van te plegen. Let op uitspraken over de omvang (aantal 'nodes') en snelheid.	"High value botnet available with up to 10k infected devices online now."
Betaalmiddelenfraude	Er worden gestolen betaalgegevens aangeboden, zoals creditcardinformatie, bankinloggegevens, accounts van PayPal/Skrill/Wise/etc. of toegang tot cryptowallets, vaak in specifieke landen. Let op termen als 'CC' (creditcard), 'CCV/CCV2' (creditcard verificatie), 'carding', 'dumps', 'logs' (inloggegevens), 'wallet access', 'carding', 'fullz' (accountgegevens) en 'kaartgegevens'.	"Verse NL kaartgegevens met hoge limieten beschikbaar." "Live CC dumps with CVV, both EU/USA."
Credential stuffing	De advertentie biedt een geautomatiseerd proces voor loginpogingen met gelekte gebruikersgegevens, om toegang tot andermans accounts te verkrijgen. Let op termen als 'combo list' (combinaties van gebruikersnamen en wachtwoorden), 'login access' en 'bruteforce'/'cracking' (het systematisch proberen van verschillende combinaties).	"Marktplaats accounts inlog nu beschikbaar." "Fresh combo lists for credential stuffing."
DDoS-aanval (stressers en booters)	De dienst wordt verleend om een website tijdelijk plat te leggen door deze te overbelasten met dataverkeer. Er wordt vaak gerefereerd naar 'site takedowns' en 'offline halen'.	"Take down any website with our services." "Websites offline halen met stresser vanaf €50 per uur."
Digitale opsporing	Er worden diensten geboden om informatie (zowel digitaal als fysiek) over een persoon te achterhalen. Bijvoorbeeld IP-adressen, de namen van diens online accounts of iemands live locatie. Let op termen als 'trace' of 'IP trace' en 'GPS' (locatie).	"Give me the mobile number and I'll turn it into a live GPS location." "Ik achterhaal de locatie van je doelwit voor je."

	Spamdiensten	Er worden diensten geboden om slachtoffers per e-mail of sms te misleiden. Er worden geautomatiseerde systemen aangeboden om grote hoeveelheden misleidende berichten te sturen. Het doel is vaak om geld of informatie van slachtoffers te verkrijgen door zich voor te doen als iemand anders (bank, bedrijf, instantie). Let op termen als 'spoofing' (zich voordoen als een betrouwbare bron), 'scam templates' en 'SMTP access' (servers om uitgaande e-mails mee te verzenden).	"Compleet spam pakket inclusief nepdomeinen en spoof-templates." "Tool with templates to impersonate CEOs."
	Gegevensmanipulatie in bestaande systemen	De dienst wordt verleend om bestaande systemen te hacken en hierin opgeslagen gegevens doelbewust aan te passen. Dit kan betrekking hebben op cijfers, officiële documenten, aanwezigheidsregistraties, gebruikersinformatie of andere administratieve gegevens. De data wordt gemanipuleerd in het voordeel van de koper. De nadruk ligt op de wijziging van specifieke gegevens in een systeem.	"We can manipulate internal records for you." "Verbeter je cijfers binnen een paar uur."
	Geldbedragen van gehackte accounts	Er wordt aangeboden om geldbedragen over te maken vanaf eerder gehackte bank- of betaalaccounts (zoals PayPal, Revolut, cryptowallets of reguliere bankrekeningen). Het aangeschafte bedrag wordt overgeboekt naar de koper. Let op termen als 'money transfer' en 'instant payment'.	"PayPal transfers ready to cash out." "ING rekening met €1000 te koop voor €70."
	Phishing	Het aanbieden van kant-en-klare phishingkits of gehoste nep websites die zijn ontworpen om inloggegevens of	"Kant en klare panel te koop voor ING." "Pre-built phishing page for PayPal for sale."

	andere vertrouwelijke informatie van slachtoffers te stelen via misleiding. Let op termen als ‘panel’ (naam voor de kit) en ‘clone sites’ (nep websites) en ‘leads’ (lijsten met gegevens van potentiële slachtoffers).	
Ransomware	Er wordt software geboden waarmee bestanden en/of systemen van een slachtoffer kunnen worden versleuteld, waarna er losgeld wordt geëist voor het herstellen van toegang. Let op termen als ‘RaaS’ (Ransomware-as-a-Service), ‘admin panel’ (beheerpaneel) en ‘encryption payload’ (bescherming van de overgebrachte data).	“Versleutel systemen op afstand en bepaal zelf het losgeld.” “Ransomware builder, custom encryption.”
Reputatiediensten	Er worden diensten geboden die een online reputatie kunstmatig kunnen verbeteren door gegevens aan te passen. Bijvoorbeeld een dienst om negatieve reviews te verwijderen, of er worden valse likes en volgers en positieve reviews verkocht voor een vaste prijs. Let op termen als ‘reputation boosting’ en namen van online platforms zoals ‘Instagram’, ‘Snapchat’ of ‘Whatsapp’.	“Viraal gaan op TikTok met goedkope views.” “Boost your business with positive Trust Pilot reviews.”
Verificatiediensten	Er worden tools of diensten aangeboden waarmee eenmalige codes kunnen worden omzeild of ontvangen. Vaak wordt benoemd voor welke platforms het precies werkt (sms, sociale media, e-mail, banken). Let op termen als ‘bypass’, ‘OTP’ (One Time Password) en ‘2FA’ (Two Factor Authentication).	“Ontvang verificatiecodes zonder eigen nummer, werkt voor Facebook en Instagram.” “Bypass 2FA with disposable numbers.”

	Botnet framework	Er wordt software verkocht waarmee klanten zelf een netwerk van geïnfecteerde apparaten (bots) kunnen aansturen, bijvoorbeeld om criminaliteit mee te plegen. Let op termen als ‘botnet panel’.	“Eigen botnet opzetten? Download dit framework en start direct.” “Build your own botnet, fully documented.”
	Bulletproof hosting	Er wordt aangeboden om websites op een beschermde manier te hosten. De aanbieder (‘hoster’) stelt geen vragen over illegale activiteiten en verleent geen medewerking bij verzoeken van opsporingsdiensten, zodat criminele websites langdurig online gehouden kunnen worden. Let op termen als ‘offshore hosting’ (gebruik van buitenlandse servers), ‘servers’ en ‘no logs’ (gebruikersgegevens niet opgeslagen).	“Anonieme hosting, ik stel geen vragen.” “Bulletproof servers with crypto only.”
	Exploit kits	Er worden softwarepakketten aangeboden die kwetsbaarheden in de software van bepaalde systemen of browsers, zodat deze kunnen worden misbruikt. Let op termen als ‘exploit builder’, ‘vulnerability/penetration testing’ en ‘drive-by kit’ (voor gebruik tijdens mobiele operaties).	“Gebruik onze exploit om bezoekers te infecteren.” “Drive-by exploit kit targets Chrome/Edge.”
	Malware/payload	Er wordt kant-en-klare schadelijke software aangeboden (zoals keyloggers, info-stealers en spyware) die kan worden gericht op slachtoffers, vaak om vertrouwelijke informatie te kunnen verkrijgen. Let op termen als ‘stealer logs’ en ‘FUD’ (fully undetectable).	“Keylogger direct klaar voor gebruik.” “Plug & play malware payloads, choose between info stealer, keylogger or loader.”

	Obfuscation	Er worden diensten of tools aangeboden die bestaande malware van de klant kunnen verbergen om detectie bij het slachtoffer te voorkomen. Dit kan specifiek gericht zijn op het omzeilen van antivirussoftware (AV). Let op termen als ‘encryption’ en ‘FUD’ (fully undetectable).	“Malware bescherming voor virusscanners.” “We obfuscate your code to bypass AV.”
	Remote Access Trojan (RAT)	Er wordt software geboden waarmee op afstand langdurige, volledige controle wordt verkregen over een geïnfecteerd apparaat. Dit is inclusief mogelijkheden zoals webcamactivatie, het beheren van bestanden en het gebruiken van toetsen. Let op termen als ‘remote desktop’, ‘RAT builder’ of ‘webcam access’.	“Toegang tot ieder Windows-systeem met onzichtbare RAT.” “Fully undetectable RAT coded in Python.”
Neutralisatie-techniek (1), (2), (3) en (4)	Het nuanceren van de feiten	De aanbieder doet uitspraken die de waarheid over het delict in twijfel trekken. De norm over wat goed en fout is wordt gepresenteerd als subjectief, of er wordt gesteld dat er meerdere waarheden naast elkaar bestaan. Let op zinnen die twijfel zaaien over goed en fout.	“Hier is nog nooit iemand voor gepakt.” “The law is outdated on this issue.”
	Het ontkennen van de feiten	De toegedane schade, de schuld van de dader of het bestaan van een slachtoffer worden ontkend of gebagatelliseerd door de aanbieder. Er wordt gedaan alsof het delict onschuldig is en geen/weinig gevolgen heeft, bijvoorbeeld door te stellen dat slachtoffers niet bestaan, onbelangrijk zijn of geen schade oplopen.	“Nobody will really get hurt by this transaction.” “Deze accounts zijn niet gekoppeld aan een persoon.”

	Het bedenken van nieuwe feiten	De aanbieder creëert een andere realiteit waarin het gedrag in mindere mate een delict is. Bijvoorbeeld door alternatieve verklaringen of fictieve scenario's te noemen waarin het gedrag rechtvaardig of onschuldig oogt. Let op uitspraken die het delict voordoen als een legitieme handeling en de realiteit verdraaien.	"Die bedrijven kunnen het zich makkelijk veroorloven om losgeld te betalen." "Word een echte professional in de F-game met deze nieuwe tools." "These products are for educational purposes only."
	Het reduceren van de geldende norm tot feiten	De geldende norm wordt irrelevant gemaakt door deze voor te doen als persoonlijke voorkeur, of door er een ander label aan te hangen. Er wordt erkend dat het gedrag afwijkt van de norm, maar gesteld dat de norm zelf ongeldig is. Let op zinnen waarin morele oordelen worden afgedaan als persoonlijke overtuigingen en op het gebruik van eufemismen en metaforen.	"Sommige mensen beseffen niet hoe de game werkt." "Laten we die visjes (*slachtoffers*) vangen."
	Een beroep doen op een belangrijkere norm	Het gedrag wordt gerechtvaardigd vanuit bepaalde idealen, overlevingsdrang, vergelding, verzet of het conformeren aan groepsnormen. Er is sprake van een belangrijker, hoger doel. Let op het benadrukken van deze zaken, zoals geld verdienen om voor jezelf te kunnen zorgen of wraak nemen.	"We take back the money that they stole from us." "Dit is je kans om je vijanden terug te pakken."
	Het relativeren van de normoverschrijding	Het gedrag wordt als minder erg voorgesteld in vergelijking met andere overtredingen of criminelen. Of de normoverschrijding wordt verzacht door te stellen dat het niet erg is, zo lang je dit niet te vaak doet. Let op vergelijkingen met het gedrag van anderen.	"Stealing some money is not too serious compared to those who steal a lot of money." "De echte criminelen hier zijn de banken en grote bedrijven."

	De schuld geven aan beperkte opties	De aanbieder presenteert het delict als de enige realistische optie die beschikbaar is om te overleven of om geld te verdienen. Let op zinnen die het delict als haalbaar presenteren in een uitzichtloze situatie.	“Not everyone can earn money legitimately.” “Kansen moet je zelf pakken, niemand gaat ze aan je geven.”
	De schuld geven aan de beperkte rol	De rol van de koper in het delict wordt geminimaliseerd en voorgedaan als onschuldig, of de verantwoordelijkheid wordt verschoven; bijvoorbeeld door te stellen dat het slachtoffer zelf nalatig was. Let op zinnen die de betrokkenheid minimaliseren of die de schuld verschuiven.	“Jij betaalt, wij regelen. Je hoeft amper iets te doen.” “Just send over the details and it will be taken care of.”
	De schuld geven aan beperkte keuzes	Er wordt erkend dat er alternatieve keuzes beschikbaar zijn dan het delict, maar omstandigheden als externe druk en grote verleiding dwingen iemand in de richting van het delict. Let op verwijzingen naar materialisme en status.	“Who doesn't want to be financially free at 25 years old?” “De nieuwste designer outfits zijn binnen handbereik met deze methode.”
	Verschuilen achter onvolmaakte kennis	De aanbieder stelt dat de koper niet kan weten dat het gedrag niet toegestaan is. De koper wordt gepresenteerd als iemand die niet beter kan weten of onvoldoende geïnformeerd is. Let op uitspraken die gericht zijn op de kennis van de koper.	“Unless you're a lawyer, how would you even know what's allowed and what's not?” "Voor zover ik weet mag dit gewoon.”
	Verschuilen achter onvolmaakte capaciteiten	De aanbieder stelt dat kopers slechts reageren op impulsen of omstandigheden en geen volledige controle over hun gedrag hebben. Let op zinnen die gemak, impulsiviteit en gebrek aan zelfbeheersing als reden geven om te kopen.	“Why do it the hard way when it can be easy?” “Niemand kan snel geld weerstaan, dus stop met liegen tegen jezelf.”

	Verschuilen achter een gebrek aan goede intenties	De aanbieder stelt dat normen of regels niet relevant zijn voor mensen die dit soort keuzes maken. Het plegen van het delict is iets wat gebeurt omdat de dader niet de neiging heeft om zich aan normen te conformeren. Let op zinnen die normloosheid presenteren als wenselijke mentaliteit.	"Als jij je nog druk maakt over wetten, ben je niet gemaakt voor dit spel." "Do it because you like to do it, it's fun."
Quote per neutralisatie-techniek	Quote *(1), (2), (3) en (4)*	Noteer de zin(nen) die de geïdentificeerde neutralisatietechniek illustreert. Dit zijn alle woorden die bijdragen aan de uitdrukking van de betreffende techniek. Dit mag verspreid zijn over meerdere zinnen, zolang het bij dezelfde techniek hoort. Woorden met enkel een grammaticale functie, zoals lidwoorden, worden meegeteld als ze deel uitmaken van een relevante zin. Als dit niet mogelijk is, noteer dan "-".	"<u>Wil jij goed verdienen op een snelle betrouwbare manier</u>? Kom in de chat." ➔ Het onderstreepte gedeelte is specifiek toe te wijzen aan de neutralisatietechniek.
Type aanbieder	Crimineel	De aanbieder presenteert zichzelf als iemand die zich bezighoudt met illegale activiteiten, zonder deze te verpakken in een mooier imago. Let op dreigende taal of verwijzingen naar het illegale karakter van het gedrag.	"We don't play nice." "Wij maken geen onderscheid, als je betaalt regelen wij de rest. Geen gezeik."
	Expert	De aanbieder presenteert zichzelf als technisch specialist met diepgaande kennis van online criminaliteit. De nadruk ligt op technische beheersing en vakjargon, vaak gericht op functionaliteit, software-eigenschappen of technologische innovatie.	"Exploit kit supports multiple browsers. Updated weekly to bypass latest patches." "Custom paneel beschikbaar. Aanpassingen mogelijk op verzoek."

	Mentor	De aanbieder presenteert zichzelf als iemand die anderen wil helpen, opleiden of begeleiden in criminele activiteiten. Let op zinnen die instructief en ondersteunend zijn, vooral gericht op het bijstaan van beginners.	“Wil jij snel geld verdienen zodat je van de zomer kan genieten? Maar weet je niet hoe? Dan ben je bij mij aan het juiste adres.” “I will teach you this method.”
	Ondernemer	De aanbieder presenteert zichzelf als commerciële aanbieder en imiteert legitieme aanbieders. Let op zinnen die de nadruk leggen op klantgerichtheid, service, betrouwbaarheid en reputatie.	“Betrouwbare service sinds 2021. Bekijk onze reviews.” “Fast delivery guaranteed with 24/7 support.”
	Crimineel en expert	De aanbieder presenteert zichzelf als iemand die zich bezighoudt met illegale activiteiten, maar benadrukt ook de technologische expertise. De nadruk ligt op effectiviteit en technische beheersing, zonder terughoudendheid over het criminele karakter van de dienst.	“We are a professional team of hackers who have been hacking crypto wallets since 2020 by using stealers.”
	Crimineel en mentor	De aanbieder presenteert zichzelf als crimineel die anderen wil begeleiden in het plegen van criminaliteit. Het criminele karakter blijft centraal staan, maar potentiële kopers worden ook uitgenodigd om te leren.	“Begin vandaag nog, ik laat je zien hoe het spel gespeeld wordt.” “I’ll show you how to get paid the real way.”
	Crimineel en ondernemer	De aanbieder presenteert zichzelf als een criminele dienstverlener met een professionele uitstraling. De toon is zakelijk, maar het illegale karakter wordt niet verbloemd.	“Betrouwbare DDoS-aanvallen, we stellen geen vragen over het doelwit.” “We don’t care which victims, we deliver always. 48 hours money-back guarantee.”
	Expert en mentor	De aanbieder presenteert zichzelf als technisch expert die zijn/haar kennis toegankelijk wil maken voor anderen. De	“Wil je leren hoe je een stealer draait zonder detectie? Ik stuur je m’n build met uitleg.”

		nadruk ligt op technische beheersing en vakjargon, maar er worden ook instructies geboden.	"You'll get my custom scripts and instructions to modify it yourself."
	Expert en ondernemer	De aanbieder presenteert zichzelf als een technisch expert met een commerciële insteek. De nadruk ligt op technische beheersing en vakjargon, maar er wordt ook gefocust op klantvriendelijkheid en betrouwbaarheid.	"Custom malware die werkt op Windows op aanvraag beschikbaar, snel geleverd." "Builds are optimized weekly. Money back guarantee within 48 hours."
	Mentor en ondernemer	De aanbieder presenteert zichzelf als ondernemer maar biedt ook mogelijkheden tot begeleiding. De nadruk ligt op toegankelijkheid van de dienst/product, waarbij ook succes en ondersteuning wordt gegarandeerd.	"Wil je snel geld verdienen als beginner? Ik ben 24/7 beschikbaar om je te helpen." "We teach you our ways, ensured success with money-back guarantee."
Framing aanbieder	Framing aanbieder	Beschrijf in eigen woorden hoe de aanbieder zichzelf presenteert in de advertentie. Baseer je antwoord op taalgebruik, toon/formaliteit, en claims over expertise of betrouwbaarheid. Als dit niet mogelijk is, noteer dan "-".	-
Aanspreekvorm	Wij-vorm	De aanbieder gebruikt enkel de 'wij-vorm' in de advertentietekst om potentiële kopers aan te spreken.	"Laten we geld gaan verdienen." "Let's work together to take them down."
	Jij-vorm	De aanbieder gebruikt enkel de 'jij-vorm' in de advertentietekst om potentiële kopers aan te spreken.	"Order from me and get what you want." "Hier ben je aan het goede adres."
	Zowel wij als jij	De aanbieder gebruikt zowel de 'wij-vorm' als de 'jij-vorm' in de advertentietekst om potentiële kopers aan te spreken.	"We help you win, that's how we grow." "Jij vraagt het en wij fixen het voor je."
Type doelwit benoemd?	Ja	De aanbieder benoemt het mogelijke doelwit van de geboden dienst/product. De vermelding mag letterlijk of omschrijvend zijn, zolang het doelwit herkenbaar is. Dit	"Use this tool to steal from individuals or small businesses."

		kan gaan om termen als ‘bedrijven’, ‘burgers’ of ‘de overheid’, maar ook ’senioren met ING-rekeningen’.	“Ideaal om toegang te krijgen tot alle systemen, zelfs ziekenhuizen.”
	Nee	De advertentie benoemt geen mogelijk doelwit van de geboden dienst/product. De tekst richt zich enkel op het aanbod van product/dienst zonder in te gaan op voor wie deze gebruikt kan worden.	“Perfect voor het platleggen van websites.” “Voor iedereen beschikbaar.”
Type doelwit (indien “Type doelwit benoemd?” = “Ja”)	Particulier	Er wordt verwezen naar het potentiële doelwit als een individu of consument. Bijvoorbeeld een willekeurige internetgebruiker of klant. Het gaat om een persoonlijk doelwit.	“Ideaal voor het binnenhalen van PayPal-inloggegevens van Nederlandse gebruikers.” “Easy access to user data from individuals.”
	Bedrijf	Er wordt verwezen naar het potentiële doelwit als commerciële organisatie of onderneming. De advertentie richt zich op diensten die gebruikt worden tegen bijvoorbeeld webshops, hostingproviders, of financiële instellingen.	“Mogelijk om elk bedrijf plat te leggen met een DDoS-aanval.” “Steal databases from online stores.”
	Overheidsinstantie	Er wordt verwezen naar het potentiële doelwit als een publieke instelling of organisatie die tot de overheid behoort. Bijvoorbeeld de politie, belastingdienst, gemeente.	“Hit government servers without a trace.” “Richt je aanval op de instanties die ons in de gaten houden.”
Framing doelwit (indien “Type doelwit	Framing doelwit	Beschrijf in eigen woorden hoe het doelwit wordt afgebeeld in de advertentie. Baseer je antwoord op woordkeuze, toon, metaforen, context of expliciete	-

benoemd?" = "Ja")		uitspraken over het doelwit. Als dit niet mogelijk is, noteer dan "-".	
Toon	Zakelijk	De advertentie bevat hoofdzakelijk een formele, professionele en verkoopgerichte toon. De aanbieder probeert zichzelf voor te doen als legitieme aanbieder. De tekst is meestal duidelijk gestructureerd, bevat specificaties over het product/de dienst en vermijdt losse spreektaal.	"Onze diensten zijn 24/7 beschikbaar. Neem contact met ons op voor de specifieke mogelijkheden en prijzen." "Secure setup with full documentation included. Satisfaction guaranteed."
	Informeel	De advertentie bevat hoofdzakelijk een losse, directe of speelse toon. Er wordt gebruikgemaakt van spreektaal, emoji's of straattaal. De tekst is persoonlijker en minder gestructureerd. Het wordt laagdrempeliger ingestoken en de nadruk ligt minder op technische specificaties.	"Wie wil ff iemand offline halen? Stuur DM." "EZ cash, no skills needed. Hit me up if ur down."
Quote: toon	Quote: toon	Noteer een quote of zin uit de advertentie die de toon van de communicatie weerspiegelt. De quote moet kenmerkend zijn voor de stijl waarmee de aanbieder zich richt tot de koper (zakelijk of informeel). Als dit niet mogelijk is, noteer dan "-".	-
Aanwezigheid reputatie	Ja	De aanbieder verwijst naar de eigen (goede) reputatie of betrouwbaarheid. Dit kan refereren naar eerder geleverde diensten, klanttevredenheid of positieve reviews. Dit telt enkel als de aanbieder het zelf benoemt, niet als het een automatisch review- of rating-systeem is van het gebruikte platform.	"Meer dan 500 klanten geholpen zonder klachten." "I'm a trusted vendor."

	Nee	De advertentie bevat geen verwijzingen van de aanbieder zelf naar reputatie, betrouwbaarheid, ervaring of klanttevredenheid. De focus ligt uitsluitend op het product/de dienst, zonder dat er een beeld van legitimiteit wordt gecreëerd door middel van reputatie.	"DDoS-aanval binnen 5 minuten geregeld." "This vendor has a rating of 4/5 stars."
Quote: reputatie (indien "Aanwezigheid reputatie" = "Ja")	Quote: reputatie	Noteer een quote of zin uit de advertentie die laat zien dat de aanbieder in de tekst verwijst naar de eigen reputatie (betrouwbaarheid, ervaring, positieve reviews, klanttevredenheid). Als dit niet mogelijk is, noteer dan "-".	-
Aanwezigheid klantenservice	Ja	In de advertentie wordt expliciet benoemd dat er na aankoop ondersteuning of service beschikbaar is voor de koper. Dit kan in de vorm zijn van een helpdesk, begeleiding, instructies of bereikbaarheid. Het bieden van nazorg bij ontevredenheid, bijvoorbeeld door het geld terug te storten, valt hier ook onder.	"Voor vragen zijn wij bereikbaar via Telegram ter ondersteuning." "24/7 support included."
	Nee	In de advertentie wordt geen enkele verwijzing gemaakt naar een vorm van klantenservice of ondersteuning.	"Phishing panel te koop, direct beschikbaar." "Botnet for rent with monthly subscription."
Quote: klantenservice (indien "Aanwezigheid klantenservice" = "Ja")	Quote: klantenservice	Noteer een quote of zin uit de advertentie die laat zien dat de aanbieder zichzelf beschikbaar stelt om na aankoop ondersteuning of service te bieden. Als dit niet mogelijk is, noteer dan "-".	-

Aanwezigheid korting/ promoties	Ja	In de advertentie wordt een vorm van korting (prijsverlaging), een tijdelijke actie (gratis producten, korting op volgende aankoop) of promotie benoemd voor potentiële kopers.	“Get early access to our newest exploit kit.” “Vandaag met korting voor nieuwe klanten.”
	Nee	In de advertentie is geen verwijzing naar enige vorm van korting (prijsverlaging), een tijdelijke actie of promotie. De prijs kan wel worden benoemd, maar zonder verwijzingen dat deze (tijdelijk) lager is.	“Tool available for $75.” “Services are available through one-time crypto payments.”

Bijlage 6: Codeerformulier

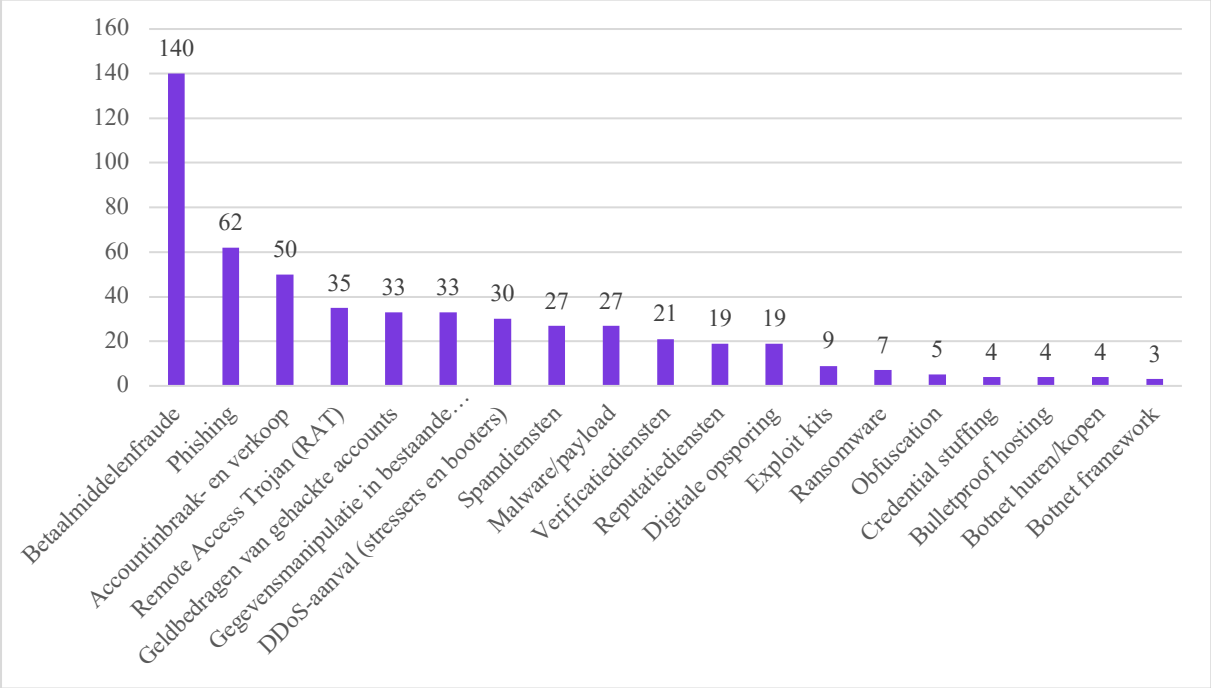
Advertentienummer	Advertentietekst	Platform	Taal	Aangeboden dienst/product (1)	Aangeboden dienst/product (2)	Aangeboden dienst/product (3)	Aangeboden dienst/product (4)	Aangeboden dienst/product (5)	Aangeboden dienst/product (6)	Neutralisatietechniek 1	Quote (1)	Neutralisatietechniek 2
Dark web 1												
Dark web 2												
Dark web 3												
Dark web 4												
Dark web 5												
Telegram 1												
Telegram 2												
Telegram 3												
Telegram 4												
Telegram 5												

Quote (2)	Neutralisatietechniek 3	Quote (3)	Neutralisatietechniek 4	Quote (4)	Neutralisatietechniek 5	Quote (5)	Type aanbieder	Framing aanbieder	Aanspreekvorm	Type slachtoffer benoemd?	Type slachtoffer	Framing slachtoffer	Toon	Quote: toon

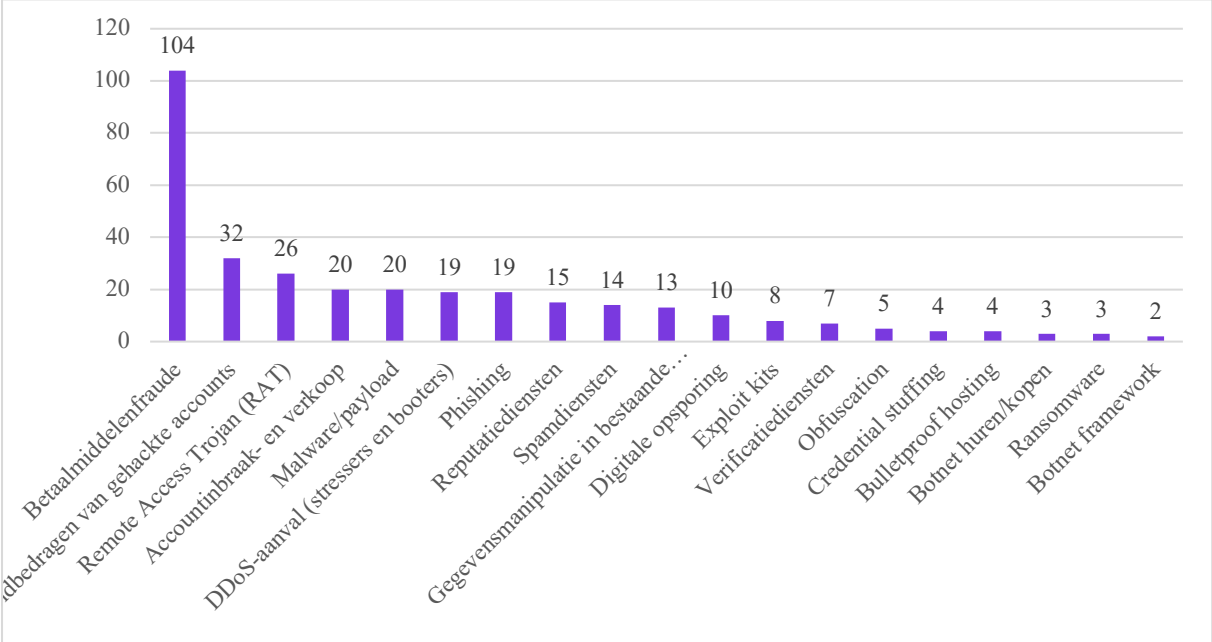
Aanwezigheid reputatie	Quote: reputatie	Aanwezigheid klantenservice	Quote: klantenservice	Aanwezigheid korting/promoties	Aanvullende overtuigingsstrategieën	Opmerkingen codeur

Bijlage 7: Overige tabellen & figuren resultaten

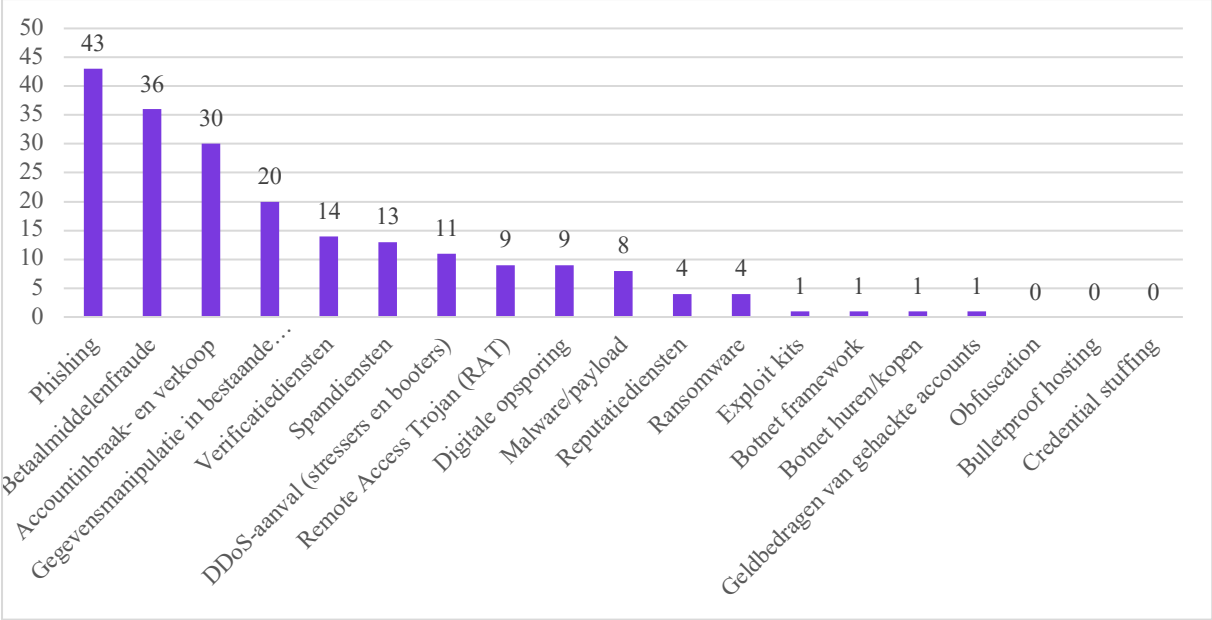
Tabel 7.1: Alle aangeboden diensten/producten in de advertenties (n = 369)



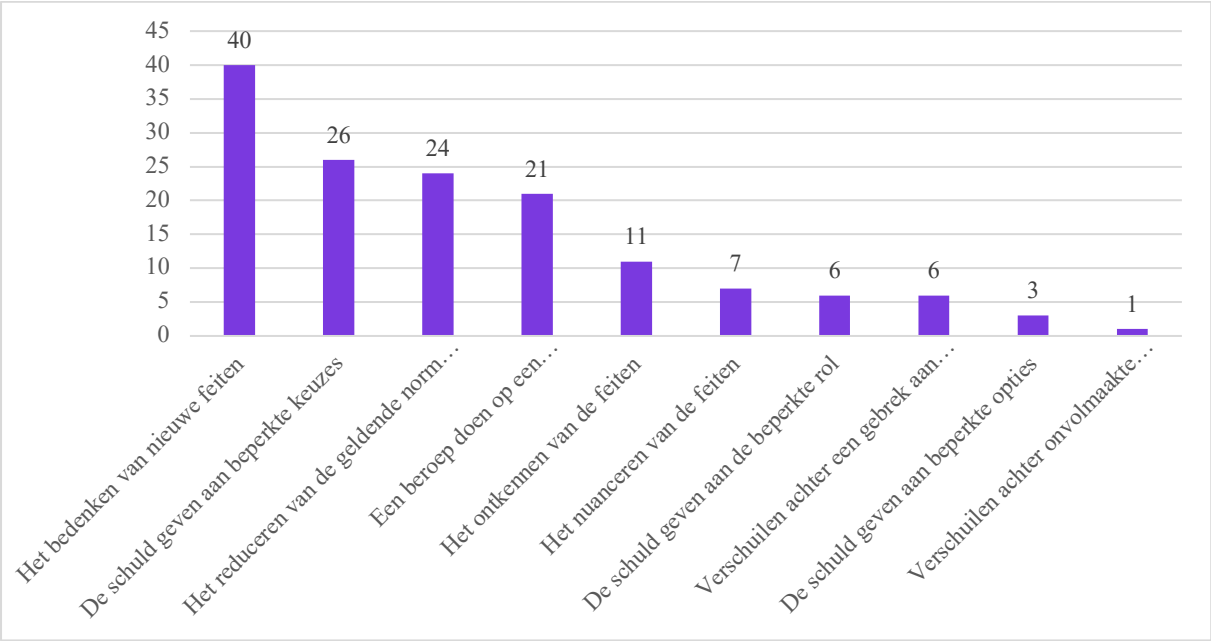
Tabel 7.2: Alle aangeboden diensten/producten op het dark web (n = 262)



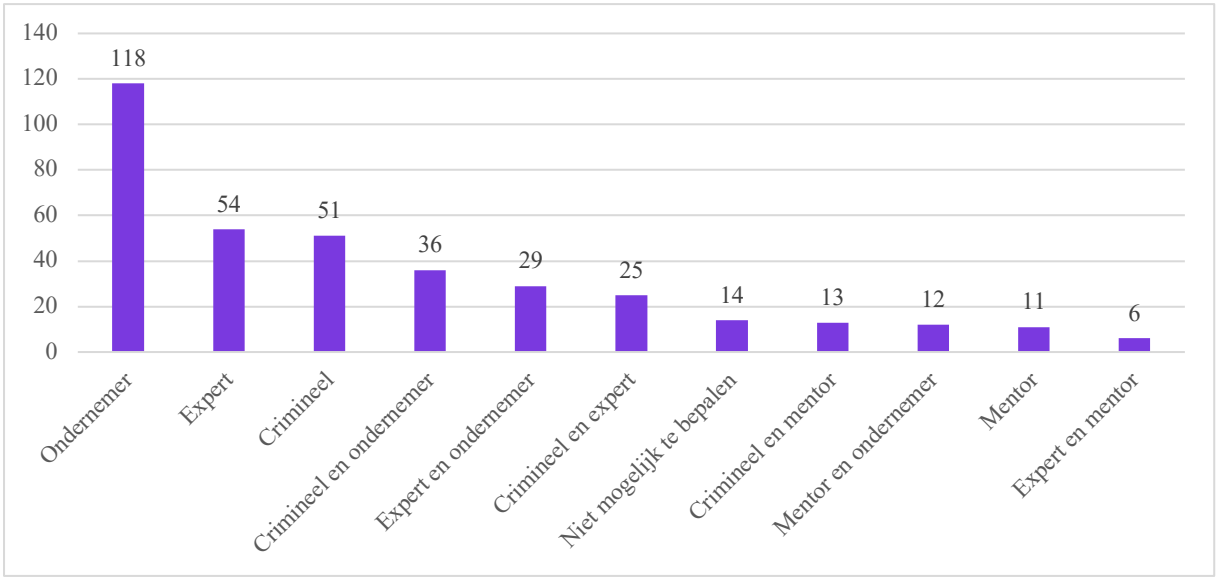
Tabel 7.3: Alle aangeboden diensten/producten op Telegram (n = 107)



Tabel 7.4: Alle gebruikte neutralisatietechnieken in de advertenties (n = 369)



Tabel 7.5: De type aanbieders in de advertenties volgens de originele uitsplitsingen (n = 369)



Bijlage 8: Modelinspectie

De eerste assumptie binnen de logistische regressie is dat de observaties in de dataset onafhankelijk van elkaar moeten zijn. Dit is grotendeels het geval. In dit onderzoek zijn meerdere advertenties afkomstig van dezelfde aanbieder, wat kan leiden tot afhankelijkheid tussen de observaties. Om deze afhankelijkheid te minimaliseren en oververtegenwoordiging van bepaalde aanbieders te voorkomen, is er echter bewust voor gekozen om per aanbieder maximaal vijf advertenties op te nemen in de dataset. Hiermee is het risico op afhankelijkheid tussen de observaties beperkt. Er kan worden aangenomen dat er wordt voldaan aan de assumptie van onafhankelijkheid.

Er is ook gekeken of er sprake is van multicollineariteit. Dit betekent dat er een te sterke samenhang is tussen de onafhankelijke variabelen. Om de variabelen afzonderlijk van elkaar te kunnen interpreteren is multicollineariteit ongewenst. Er is een lineaire regressie uitgevoerd met daarin alle predictoren, zodat er VIF-scores kunnen worden berekend per variabele. Deze scores worden weergegeven in tabel 8.1. De geldende vuistregel is dat VIF-scores van boven de 5 problematisch zijn. Aan de hand hiervan wordt duidelijk dat er sprake is van ernstige multicollineariteit tussen het platform en de taal. Er is daarom voor gekozen om slechts één van deze variabelen op te nemen in het model, namelijk het platform. Voor de context van de advertentie is het platform relevanter dan de taal.

Tabel 8.1: De VIF-scores van alle variabelen die zijn opgenomen in het model (n = 369)

Variabele	*VIF-score*
Platform	17,944
Taal	17,456
Totaal aantal woorden	1,707
Aantal aangeboden diensten/producten	2,786
Groepsgevoel	1,436
Toon	2,924
Doelwit	1,194
Moeilijkheidsgraad delict: gecompliceerd	1,474
Moeilijkheidsgraad delict: beide	2,316
Type aanbieder: crimineel	1,822
Type aanbieder: ondernemer	3,470
Type aanbieder: expert	2,345
Type aanbieder: mentor	2,481
Reputatie	1,356
Klantenservice	1,628
Kortingen/promoties	1,547

Als laatste is er gecontroleerd of er sprake is van invloedrijke uitschieters, die een vertekenend beeld kunnen geven van de geschatte coëfficiënten. Dit is gedaan aan de hand van vier verschillende gegevens: de gestudentiseerde residuen, de leverage, de Cook's distance en de DFBETA. In tabel 8.2 staan de tien meest invloedrijke observaties uit de dataset. Er is als eerste gekeken naar de studentized residuals. Dit weergeeft de verschillen tussen de geobserveerde en voorspelde waarde van de afhankelijke variabele. Op basis hiervan is een observatie invloedrijk als de waarde hoger is dan 3 of lager dan -3. Bij geen enkele observatie in de dataset was dit het geval. Vervolgens is er gekeken naar de leverage, die laat zien hoe erg een observatie afwijkt van het gemiddelde. In deze dataset is de gemiddelde leverage-waarde 0,04. De observaties die hier het meest van afweken zijn opgenomen in de tabel, dit gaat om de onderste zes observaties. Daarna is gekeken naar de Cook's distance, wat het product is van de gestudentiseerde residuen en de leverage. Observaties met een Cook's distance die hoger is dan 4/n, oftewel 4/369 = 0,01, worden als invloedrijke observaties beschouwd. Dit geldt voor 46 observaties in totaal. Degene die ook hoger scoren op andere maten zijn opgenomen in de tabel. Tot slot is er gekeken naar de DFBETA, dit laat zien hoeveel de regressiecoëfficiënt verandert als de observatie wordt weggelaten. Hier is dus gekeken naar opvallend hoge en lage waarden, die een vertekend beeld van de variabelen zouden kunnen geven. Er was geen sprake van observaties met opvallend hoge waarden die echt een invloed uitoefenen op de resultaten van een variabele. Bij het platform was de hoogste DFBETA bijvoorbeeld 0,16 en bij de toon was de hoogste 0,08.

Op basis van de observaties in tabel 8.2 kan worden gekeken of dit ook echt uitbijters zijn. Op basis van deze vier maatstaven kan worden geconcludeerd dat er geen sprake is van uitbijters die de resultaten van het model vertekenen.

Tabel 8.2: De tien meest invloedrijke observaties op basis van de gestudentiseerde residuen*, Cook's distance, leverage en DFBETA*

Observatie	Studentized residuals	Leverage	Cook's distance	DFBETA
Dark web 6	-2,64	0,05	1,27	0,14
Telegram 101	2,40	0,06	0,89	-0,12
Dark web 10	-2,28	0,07	0,73	0,15
Dark web 223	1,99	0,08	0,44	-0,11
Telegram 22	1,69	0,16	0,44	-0,12
Dark web 259	1,25	0,20	0,22	0,10
Telegram 53	-1,00	0,19	0,12	0,04
Dark web 81	0,95	0,18	0,10	0,06
Dark web 231	-1,17	0,17	0,15	-0,05
Telegram 48	1,36	0,16	0,23	-0,18

Bijlage 9: Bewerkingen en toetsen in SPSS

In deze bijlage wordt een overzicht gegeven van alle bewerkingen en toetsen die zijn uitgevoerd in SPSS. Per bewerking wordt de gebruikte syntax weergegeven.

Als eerste zijn de variabelen opnieuw gecodeerd, om ze bruikbaar te maken voor de statistische toetsen en regressieanalyse. De syntax staat in tabel 9.1.

Tabel 9.1: De syntax met de hercoderingen per variabele

```
RECODE Toon ('Zakelijk'=0) ('Informeel'=1) INTO Toon_her.
EXECUTE.

RECODE Platform ('0'=0) ('1'=1) INTO Platform_her.
EXECUTE.

RECODE Taal ('0'=0) ('1'=1) INTO Taal_her.
EXECUTE.

RECODE Moeilijkheidsgraad_delict ('Alleen eenvoudig'=1) ('Combinatie van eenvoudig en '+
    'gecompliceerd'=3) ('Alleen gecompliceerd'=2) INTO Moeilijkheidsgraad_her.
EXECUTE.

RECODE Gebruik_neutralisatietechniek ('Nee'=0) ('Ja'=1) INTO Gebruik_her.
EXECUTE.

RECODE Reputatie ('Nee'=0) ('Ja'=1) INTO Reputatie_her.
EXECUTE.

RECODE Klantenservice ('Nee'=0) ('Ja'=1) INTO Klantenservice_her.
EXECUTE.

RECODE Kortingen_promoties ('Nee'=0) ('Ja'=1) INTO Kortingen_her.
EXECUTE.

COMPUTE Strategie_totaal=Gebruik_her + Reputatie_her + Klantenservice_her + Kortingen_her.
EXECUTE.

RECODE Type_doelwit_benoemd ('Nee'=0) ('Ja'=1) INTO Doelwitbenoemd_her.
EXECUTE.

COMPUTE is_crimineel=(Type_aanbieder = "Crimineel") OR
(Type_aanbieder = "Crimineel en expert") OR
(Type_aanbieder = "Crimineel en mentor") OR
(Type_aanbieder = "Crimineel en ondernemer").
EXECUTE.

COMPUTE is_mentor=(Type_aanbieder = "Mentor") OR
(Type_aanbieder = "Crimineel en mentor") OR
(Type_aanbieder = "Expert en mentor") OR
(Type_aanbieder = "Mentor en ondernemer").
```

```
EXECUTE.

COMPUTE is_expert=(Type_aanbieder = "Expert") OR
(Type_aanbieder = "Crimineel en expert") OR
(Type_aanbieder = "Expert en mentor") OR
(Type_aanbieder = "Expert en ondernemer").
EXECUTE.

COMPUTE is_ondernemer=(Type_aanbieder = "Ondernemer") OR
(Type_aanbieder = "Crimineel en ondernemer") OR
(Type_aanbieder = "Mentor en ondernemer") OR
(Type_aanbieder = "Expert en ondernemer").
EXECUTE.

RECODE Aanspreekvorm ('Jij'=1) ('Zowel wij als jij'=2) ('Wij'=3) ('Anders'=4) INTO
   Aanspreekvorm_her.
EXECUTE.

RECODE Type_doelwit ('Particulier'=1) ('Bedrijf'=2) ('Particulier en bedrijf'=3) ('Bedrijf en '+
   'overheidsinstantie'=4) (ELSE=5) INTO Typedoelwit_her.
EXECUTE.

Dummy
RECODE Moeilijkheidsgraad_her (2=1) (1=0) (3=0) INTO Delict_gecompliceerd.
EXECUTE.

RECODE Moeilijkheidsgraad_her (3=1) (1=0) (2=0) INTO Delict_beide.
EXECUTE.

RECODE Aanspreekvorm_her (1=0) (4=0) (2=1) (3=1) INTO Groepsgevoel_dummy.
EXECUTE.

RECODE Typedoelwit_her (1=1) (3=1) (2=0) (4=0) (5=0) INTO Doelwit_particulier_dummy.
EXECUTE.
```

Een aantal van de bovenstaande variabelen zijn niet alleen opnieuw gecodeerd vanwege bruikbaarheid, maar zijn aangepast om nieuwe categorieën op te stellen voor in de analyses. Dit geldt voor groepsgevoel, type doelwit, het totaal aantal strategieën en de typen aanbieders.

Ten eerste is de variabele “groepsgevoel” gemaakt op basis van de gehanteerde aanspreekvormen in de advertenties. In de oorspronkelijke variabele zijn er vier categorieën die laten zien hoe de potentiële klant wordt aangesproken door de aanbieder. Deze frequentieverdeling wordt weergegeven in tabel 9.2. Het doel hiervan was om vast te stellen of de aanbieder een groepsgevoel probeert te creëren door de “wij-vorm” in de advertentie te gebruiken. In de nieuwe variabele “groepsgevoel” zijn daarom de advertenties waarin dit wel gebeurt afgezet tegen de advertenties waarin dit niet gebeurt. De categorieën “wij-vorm” en “zowel jij als wij” zijn samengevoegd en de categorieën “jij-vorm” en “anders”, waarbij helemaal geen aanspreekvorm werd gebruikt, zijn

samengevoegd. De nieuwe variabele laat dus zien of de “wij-vorm” is gehanteerd in de advertentie. De nieuwe frequentieverdeling wordt weergegeven in tabel 9.3.

Tabel 9.2: De frequentieverdeling van de oorspronkelijke variabele “aanspreekvorm”

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Jij-vorm	145	39,3	39,3	39,3
	Zowel jij als wij	105	28,5	28,5	67,8
	Wij-vorm	12	3,3	3,3	71,0
	Anders	107	29,0	29,0	100,0
	Total	369	100,0	100,0	

Tabel 9.3: De frequentieverdeling van de nieuwe variabele “groepsgevoel”

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Geen wij-vorm	252	68,3	68,3	68,3
	Wij-vorm	117	31,7	31,7	100,0
	Total	369	100,0	100,0	

Ten tweede is de variabele “particulier doelwit” gemaakt op basis van de typen doelwitten die zijn gecodeerd. Bij de oorspronkelijke variabelen waren er vijf verschillende categorieën, waarvan meerdere categorieën slechts enkele observaties bevatten. De frequentieverdeling uit de SPSS output van de oorspronkelijke variabele wordt weergegeven in tabel 9.4. Voor de hypothese was het van belang om particuliere doelwitten af te zetten tegen niet-particuliere doelwitten. De categorieën waarin naar een particulier doelwit werd verwezen zijn daarom samengenomen (“Particulier” en “Particulier en bedrijf”). Alle overige categorieën, waarin niet naar een particulier doelwit is verwezen, zijn samengevoegd. De frequentieverdeling van de nieuwe variabele “particulier doelwit” wordt weergegeven in tabel 9.5.

Tabel 9.4: De frequentieverdeling van de oorspronkelijke variabele “type doelwit”

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Particulier	14	3,8	3,8	3,8
	Bedrijf	4	1,1	1,1	4,9
	Particulier en bedrijf	2	,5	,5	5,4
	Bedrijf en overheidsinstantie	2	,5	,5	6,0
	Geen	347	94,0	94,0	100,0
	Total	369	100,0	100,0	

Tabel 9.5: De frequentieverdeling van de nieuwe variabele "particulier doelwit"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Niet particulier	353	95,7	95,7	95,7
	Wel particulier	16	4,3	4,3	100,0
	Total	369	100,0	100,0	

Ten derde is de variabele gemaakt die het totaal aantal gebruikte strategieën laat zien. Dit is een optelsom van de vier binaire variabelen die het gebruiken van neutralisatietechnieken, reputatieverwijzingen, een klantenservice en kortingen/promoties weerspiegelen. De frequentieverdeling van deze nieuwe variabele wordt gegeven in tabel 9.6.

Tabel 9.6: De frequentieverdeling van de nieuwe variabele "totaal aantal strategieën"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	,00	103	27,9	27,9	27,9
	1,00	106	28,7	28,7	56,6
	2,00	90	24,4	24,4	81,0
	3,00	52	14,1	14,1	95,1
	4,00	18	4,9	4,9	100,0
	Total	369	100,0	100,0	

Tot slot zijn er vier binaire variabelen gemaakt die ieder de aanwezigheid van een bepaald type aanbieder aanduiden. De oorspronkelijke variabele bevat elf individuele categorieën met daarin individuele typeringen per aanbieder, maar ook gecombineerde typen. Vanwege de gecombineerde typen, die worden weergegeven in de frequentieverdeling in tabel 9.7, was het niet mogelijk om de aanbiedertypen onderling met elkaar te vergelijken. De oorspronkelijke variabele is daarom opgesplitst in vier binaire variabelen voor de categorieën "crimineel", "ondernemer", "expert" en "mentor". Ieder van deze variabelen weergeeft of het type aanbieder in de advertentie wel of geen specifiek type is. Deze nieuwe variabelen sluiten elkaar dus onderling niet uit, omdat een advertentie nog steeds mee kan tellen bij meerdere binaire variabelen. De frequentieverdelingen van de nieuwe variabelen worden weergegeven in tabellen 9.8 tot en met 9.11.

Tabel 9.7: De frequentieverdeling van de oorspronkelijke variabele "type aanbieder"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Crimineel	51	13,8	13,8	13,8
	Crimineel en expert	25	6,8	6,8	20,6
	Crimineel en mentor	13	3,5	3,5	24,1
	Crimineel en ondernemer	36	9,8	9,8	33,9
	Expert	54	14,6	14,6	48,5
	Expert en mentor	6	1,6	1,6	50,1
	Expert en ondernemer	29	7,9	7,9	58,0
	Mentor	11	3,0	3,0	61,0
	Mentor en ondernemer	12	3,3	3,3	64,2
	Niet mogelijk te bepalen	14	3,8	3,8	68,0
	Ondernemer	118	32,0	32,0	100,0
	Total	369	100,0	100,0	

Tabel 9.8: De frequentieverdeling van de nieuwe variabele "crimineel"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	244	66,1	66,1	66,1
	Ja	125	33,9	33,9	100,0
	Total	369	100,0	100,0	

Tabel 9.9: De frequentieverdeling van de nieuwe variabele "ondernemer"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	174	47,2	47,2	47,2
	Ja	195	52,8	52,8	100,0
	Total	369	100,0	100,0	

Tabel 9.10: De frequentieverdeling van de nieuwe variabele "expert"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	255	69,1	69,1	69,1
	Ja	114	30,9	30,9	100,0
	Total	369	100,0	100,0	

Tabel 9.11: De frequentieverdeling van de nieuwe variabele "mentor"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	327	88,6	88,6	88,6
	Ja	42	11,4	11,4	100,0
	Total	369	100,0	100,0	

Vervolgens zijn de bivariate statistieken getoetst. Dit is afhankelijk van de typen variabelen gedaan aan de hand van Chi kwadraattoetsen met het Phi coëfficiënt en de Cramer's V, via Pearsons correlaties en Spearmans correlaties. Deze syntax wordt weergegeven in tabel 9.12.

Tabel 9.12: De syntax van de bivariate statistieken

```
CROSSTABS
  /TABLES=Gebruik_her BY Platform_her Taal_her Groepsgevoel_dummy Toon_her Moeilijkheidsgraad_her
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ PHI
  /CELLS=COUNT
  /COUNT ROUND CELL.

CORRELATIONS
  /VARIABLES=Gebruik_her Totaal_aantal_woorden Aantal_dienstenproducten
  /PRINT=TWOTAIL NOSIG FULL
  /MISSING=PAIRWISE.

CROSSTABS
  /TABLES=Gebruik_her BY is_crimineel is_ondernemer is_expert is_mentor Reputatie_her
    Klantenservice_her Kortingen_her
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ PHI
  /CELLS=COUNT
  /COUNT ROUND CELL.

CROSSTABS
  /TABLES=Platform_her BY Taal_her Groepsgevoel_dummy Toon_her Moeilijkheidsgraad_her is_crimineel
    is_ondernemer is_expert is_mentor Reputatie_her Klantenservice_her Kortingen_her
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ PHI
  /CELLS=COUNT
  /COUNT ROUND CELL.

CORRELATIONS
  /VARIABLES=Platform_her Totaal_aantal_woorden Aantal_dienstenproducten
  /PRINT=TWOTAIL NOSIG FULL
  /MISSING=PAIRWISE.

CORRELATIONS
  /VARIABLES=Taal_her Totaal_aantal_woorden Aantal_dienstenproducten
  /PRINT=TWOTAIL NOSIG FULL
  /MISSING=PAIRWISE.

CROSSTABS
  /TABLES=Taal_her BY Groepsgevoel_dummy Toon_her Moeilijkheidsgraad_her is_crimineel
is_ondernemer
    is_expert is_mentor Reputatie_her Klantenservice_her Kortingen_her
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ PHI
  /CELLS=COUNT
```

```
  /COUNT ROUND CELL.

CORRELATIONS
  /VARIABLES=Totaal_aantal_woorden Aantal_dienstenproducten Groepsgevoel_dummy Toon_her
    is_crimineel is_ondernemer is_expert is_mentor Reputatie_her Klantenservice_her Kortingen_her
  /PRINT=TWOTAIL NOSIG FULL
  /MISSING=PAIRWISE.

NONPAR CORR
  /VARIABLES=Totaal_aantal_woorden Moeilijkheidsgraad_her
  /PRINT=SPEARMAN TWOTAIL NOSIG FULL
  /MISSING=PAIRWISE.

CORRELATIONS
  /VARIABLES=Aantal_dienstenproducten Groepsgevoel_dummy Toon_her is_crimineel is_ondernemer
    is_expert is_mentor Reputatie_her Klantenservice_her Kortingen_her
  /PRINT=TWOTAIL NOSIG FULL
  /MISSING=PAIRWISE.

NONPAR CORR
  /VARIABLES=Aantal_dienstenproducten Moeilijkheidsgraad_her
  /PRINT=SPEARMAN TWOTAIL NOSIG FULL
  /MISSING=PAIRWISE.

CROSSTABS
  /TABLES=Groepsgevoel_dummy BY Toon_her Moeilijkheidsgraad_her is_crimineel is_ondernemer
    is_expert is_mentor Reputatie_her Klantenservice_her Kortingen_her
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ PHI
  /CELLS=COUNT
  /COUNT ROUND CELL.

CROSSTABS
  /TABLES=Toon_her BY Moeilijkheidsgraad_her is_crimineel is_ondernemer is_expert is_mentor
    Reputatie_her Klantenservice_her Kortingen_her
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ PHI
  /CELLS=COUNT

CROSSTABS
  /TABLES=Moeilijkheidsgraad_her BY is_crimineel is_ondernemer is_expert is_mentor Reputatie_her
    Klantenservice_her Kortingen_her
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ PHI
  /CELLS=COUNT
  /COUNT ROUND CELL.

CROSSTABS
  /TABLES=is_crimineel BY is_ondernemer is_expert is_mentor Reputatie_her Klantenservice_her
    Kortingen_her
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ PHI
```

```
  /CELLS=COUNT
  /COUNT ROUND CELL.

CROSSTABS
  /TABLES=is_ondernemer BY is_expert is_mentor Reputatie_her Klantenservice_her Kortingen_her
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ PHI
  /CELLS=COUNT
  /COUNT ROUND CELL.

CROSSTABS
  /TABLES=is_expert BY is_mentor Reputatie_her Klantenservice_her Kortingen_her
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ PHI
  /CELLS=COUNT
  /COUNT ROUND CELL.

CROSSTABS
  /TABLES=is_mentor BY Reputatie_her Klantenservice_her Kortingen_her
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ PHI
  /CELLS=COUNT
  /COUNT ROUND CELL.

CROSSTABS
  /TABLES=Reputatie_her BY Klantenservice_her Kortingen_her
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ PHI
  /CELLS=COUNT
  /COUNT ROUND CELL.

CROSSTABS
  /TABLES=Klantenservice_her BY Kortingen_her
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ PHI
  /CELLS=COUNT
  /COUNT ROUND CELL.
```

Tot slot is er een logistische regressieanalyse uitgevoerd en zijn er assumpties gecontroleerd. Dit wordt weergegeven in tabel 9.13.

Tabel 9.13: De syntax van de logistische regressieanalyse en assumptiecontrole

```
LOGISTIC REGRESSION VARIABLES Gebruik_her
  /METHOD=ENTER Platform_her Totaal_aantal_woorden Aantal_dienstenproducten
  /METHOD=ENTER Groepsgevoel_dummy Toon_her Doelwit_particulier_dummy Delict_gecompliceerd
    Delict_beide
  /METHOD=ENTER is_crimineel is_ondernemer is_expert is_mentor Reputatie_her Klantenservice_her
    Kortingen_her
  /SAVE=COOK LEVER DFBETA SRESID DEV
  /PRINT=GOODFIT
```

```
  /CRITERIA=PIN(0.05) POUT(0.10) ITERATE(20) CUT(0.5).

REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA COLLIN TOL
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT Woorden_techniek1
  /METHOD=ENTER Gebruik_her Delict_gecompliceerd Delict_beide Groepsgevoel_dummy Toon_her
    Doelwit_particulier_dummy Reputatie_her Klantenservice_her Kortingen_her is_crimineel is_mentor
    is_expert is_ondernemer Platform_her Taal_her Totaal_aantal_woorden Aantal_dienstenproducten.

DESCRIPTIVES VARIABLES=LEV_1
  /STATISTICS=MEAN.
```