Cryptovaluta in cybercriminaliteit:

Een onderzoek naar het gebruik van cryptovaluta's bij verschillende vormen van cybercriminaliteit en de bijbehorende financiële schade

Door

Rens W.H. Hooyman

S5005043

Masterscriptie

MSc Sociologie van Criminaliteit en Veiligheid

Faculteit Gedrags- en Maatschappijwetenschappen

Rijksuniversiteit Groningen

Begeleider: Prof. Dr. René Veenstra

Referent: Dr. Mark Huisman

09-07-2023

rijksuniversiteit groningen

POLITIE

Samenvatting

De coronapandemie heeft geleid tot een verschuiving van traditionele criminaliteit naar cybercriminaliteit. Cryptovaluta's spelen een rol in cybercriminaliteit, maar het is onbekend in hoeverre het gebruik van cryptovaluta's verschilt per vorm van cybercriminaliteit. Bovendien is er weinig bekend over de financiële schade van het gebruik van cryptovaluta's in cybercriminaliteit.

Het doel van dit onderzoek is om de invloed van de coronapandemie op het gebruik van cryptovaluta's te achterhalen, evenals de verschillen in het gebruik van cryptovaluta's tussen de verschillende vormen van cybercriminaliteit. Daarnaast beoogt dit onderzoek inzicht te krijgen in de financiële schade veroorzaakt door het gebruik van cryptovaluta's. De onderzoeksvraag luidt: *Welke invloed heeft de coronapandemie op het gebruik van cryptovaluta's in cybercriminaliteit en hoe verschilt de financiële schade van het gebruik van cryptovaluta's tussen de vormen van cybercriminaliteit?* De belangrijkste hypothesen zijn dat de coronapandemie heeft geleid tot een toename van het gebruik van cryptovaluta's en dat het gebruik van cryptovaluta's heeft bijgedragen aan een stijging van de financiële schade in cybercriminaliteit.

Om de onderzoeksvraag te beantwoorden is er gebruik gemaakt registraties van slachtoffers en verdachten afkomstig uit politiegegevens. Hieruit zijn alle registraties afkomstig uit 2019 tot en met 2022 die in BlueIntel zijn gecategoriseerd als cybercriminaliteit geselecteerd. Om de hypothesen te testen zijn een logistische- en (lineaire) regressieanalyse uitgevoerd.

Allereerst tonen de resultaten van dit onderzoek aan dat de kans op het gebruik van cryptovaluta's significant hoger is in 2021 en 2022 in vergelijking met 2019 en 2020. Bovendien is de kans op het gebruik van cryptovaluta's in 2019 en 2020 verwaarloosbaar. Ten tweede blijkt uit het onderzoek dat de kans op het gebruik van cryptovaluta's aanzienlijk hoger is bij Ddos en ransomware dan bij de andere vormen van cybercriminaliteit. Ten derde komt in het onderzoek naar voren dat in de periode 2021 en 2022 de kans op het gebruik van cryptovaluta's in cybercriminaliteit significant lager is wanneer Ddos of ransomware aanwezig is. Ten vierde laat het onderzoek zien dat het gebruik van cryptovaluta's de financiële schade van cybercriminaliteit aanzienlijk verhoogt. Hierbij veroorzaakt het gebruik van cryptovaluta's in Ddos gemiddeld de grootste financiële schade. Bovendien neemt de gemiddelde financiële schade voor elke vorm van cybercriminaliteit jaarlijks toe. Ten vijfde toont het onderzoek aan dat het effect van het gebruik van cryptovaluta's op de financiële schade wordt verzwakt door de aanwezigheid van ransomware en hacken. Tot slot wordt het effect van 'tijd in jaren' op de financiële schade extra versterkt door het gebruik van cryptovaluta's.

De conclusie is dat de kans op het gebruik van cryptovaluta's in cybercriminaliteit steeg tijdens de coronapandemie. Bovendien laten de resultaten zien dat het gebruik van cryptovaluta's heeft bijgedragen aan de stijging van de financiële schade van cybercriminaliteit.

Belangrijke beperkingen van dit onderzoek zijn mogelijke onderrapportage en selectiviteit bij politieregistraties. Bovendien richt dit zich alleen op hacken, phishing, Ddos en ransomware. Toekomstig onderzoek kan zich richten op andere vormen van cybercriminaliteit om een completer beeld te krijgen van het gebruik van cryptovaluta's. Daarnaast is het belangrijk om vervolgonderzoek te verrichten naar de specifieke factoren die verantwoordelijke zijn voor de verschillen in het gebruik van cryptovaluta's tussen de verschillende vormen van cybercriminaliteit. Op basis van de resultaten wordt aanbevolen om bewustwording van het gebruik van cryptovaluta's binnen de politie te vergroten, samenwerking met wisselkantoren voor cryptovaluta te bevorderen en vervolgonderzoek uit te voeren naar Ddos en ransomware om de oorzaken van de verschillen in het gebruik van cryptovaluta's te begrijpen.

Voorwoord

De interesse voor dit onderzoek is gewekt door de opmerkelijke verschuiving van traditionele vormen van criminaliteit naar online criminaliteit. In dit moderne tijdperk, waarin technologie een integraal onderdeel is geworden van ons dagelijks leven, worden we geconfronteerd met nieuwe mogelijkheden en uitdagingen. Cybercriminaliteit is aanzienlijk gegroeid en cryptovaluta's hebben een geheel nieuwe dimensie toegevoegd aan cybercriminaliteit.

Deze masterscriptie, getiteld "Cryptovaluta's in Cybercriminaliteit", richt zich op het onderzoeken van de verschillen in het gebruik van cryptovaluta's tussen de verschillende vormen van cybercriminaliteit, evenals de financiële schade die ermee gepaard gaat. Dit onderzoek is uitgevoerd als afronding van de master Sociologie van Criminaliteit en Veiligheid.

Ik wil graag mijn oprechte waardering uitspreken voor de begeleiding en waardevolle feedback die ik heb ontvangen van Prof. Dr. René Veenstra en Dr. Mark Huisman van de Rijksuniversiteit Groningen gedurende het onderzoek. Hun expertise en toewijding hebben een cruciale rol gespeeld bij het vormgeven van dit onderzoek.

Daarnaast wil ik ook mijn dankbaarheid uitspreken naar Martijn Krijsen, Gerard Wolters en Jildau Borwell van het Team Cybercrime Noord-Nederland. Zonder hun inzet en medewerking zou dit onderzoek niet mogelijk zijn geweest. Hun waardevolle bijdrage en betrokkenheid hebben enorm bijgedragen aan het verkrijgen van de benodigde gegevens en inzichten.

Rens Hooyman

Groningen, 9 juli 2023

Inhoudsopgave

1. Inleiding

De digitalisering van de maatschappij heeft geleid tot een verschuiving van criminaliteit (Odinot et al., 2018). Traditionele georganiseerde criminaliteit heeft zijn weg gevonden naar het internet, resulterend in een aanzienlijke toename van cybercriminaliteit in de afgelopen jaren (Odinot et al., 2018). Cybercriminaliteit omvat diverse vormen van criminaliteit waarbij de ICT-infrastructuur zelf het doelwit is, en waarbij ICT wordt ingezet om dit doel te bereiken (Leukfeldt et al., 2018). De stijgende trend in cybercriminaliteit wordt ondersteund door statistieken waaruit blijkt dat het aantal geregistreerde gevallen van cybercriminaliteit in de periode van 2019 tot en met 2022 is verdrievoudigd (Cybercrimeinfo, 2023).

De verschuiving in criminaliteit is versterkt door de coronapandemie (Europol, 2020). Tijdens deze periode werden werknemers gedwongen om vanuit huis te werken, wat het lastiger maakte voor traditionele vormen criminaliteit, zoals zakkenrollerij en woningeninbraak (CBS, 2021). De coronapandemie heeft ook geleid tot een toename van het aantal mensen dat online actief was, wat resulteerde in een groter aantal potentiële slachtoffers (Europol, 2020). Aangezien mensen op afstand toegang hadden tot bedrijfsinformatie en -middelen, werden bedrijven en individuen die voorheen niet veel online actief waren kwetsbare doelwitten voor cybercriminelen, omdat ze weinig ervaring hadden met online veiligheid (Europol, 2020).

Een opkomende trend in criminaliteit is het gebruik van cryptovaluta's (Kruisbergen et al., 2018). Onderzoek van Chainanalysis toont aan dat het gebruik van cryptovaluta's in 2021 een recordbedrag heeft bereikt van 12,3 miljard euro, wat een stijging van 45% is ten opzichte van het voorgaande jaar (Cybercrimeinfo, 2022). Het gebruik van cryptovaluta's is om twee redenen aantrekkelijk voor cybercriminelen. Ten eerste bieden cryptovaluta's cybercriminelen de mogelijkheid om anoniem transacties uit te voeren, waardoor het voor opsporingsdiensten moeilijker wordt hen te traceren (Politie, 2020). Ten tweede kunnen cryptovaluta's snel en zonder tussenkomst van centrale organisaties worden verplaatst, waardoor de opbrengsten uit illegale activiteiten kunnen worden verborgen (Politie, 2020).

De opkomst van cryptovaluta's werd door veel mensen gezien als een kans om extra inkomsten te genereren, wat vaak resulteerde in onervaren investeerders die zonder enige voorkennis in cryptovaluta's stapten. Het gebrek aan kennis maakte hen een kwetsbaar doelwit voor cybercriminelen, wat heeft geleid tot een toename van oplichtingspraktijken. Mensen die weinig kennis hebben over cryptovaluta's en de bijbehorende risico's, zijn zich vaak niet bewust dat ze slachtoffer kunnen worden van criminaliteit. Criminelen kunnen deze personen makkelijk misleiden door hen onder valse voorwendselen te overtuigen om cryptovaluta's naar een specifiek adres te sturen. Het aantal oplichtingspraktijken waarbij cryptovaluta's werd gebruikt, is gestegen van 30 in 2020 naar 282 in 2022 (Botha et al., 2023).Het gebruik van cryptovaluta's in criminaliteit is een

zorgwekkende ontwikkeling. Het relatief anonieme karakter van cryptovaluta's bemoeilijkt de taak van opsporingsdiensten om de identiteit van daders te achterhalen, waardoor criminelen in staat zijn om straffeloos criminele handelingen te verrichten (Van Huijsee et al., 2021). Dit draagt bij aan de groei van cybercriminaliteit, aangezien cybercriminelen de risico's voor henzelf laag inschatten door het gebruik van cryptovaluta's.

Cybercriminaliteit vormt een groeiend maatschappelijk probleem en heeft een aanzienlijke impact op de Nederlandse samenleving. Uit gegevens blijkt dat 13 procent van de Nederlandse bevolking in 2019 slachtoffer is geworden van cybercriminaliteit (CBS, 2020a). Slachtoffers melden dat ze zowel emotionele als financiële schade ondervinden als gevolg van cybercriminaliteit (Akkermans et al., 2022).

Hoewel het bekend is dat cryptovaluta's een faciliterende rol spelen in cybercriminaliteit, is er momenteel nog weinig kennis beschikbaar over de verschillen in het gebruik van cryptovaluta's tussen diverse vormen van cybercriminaliteit en of de coronapandemie invloed heeft gehad op het gebruik ervan. Bovendien richt de bestaande literatuur over financiële schade zich voornamelijk op cybercriminaliteit in het algemeen, waardoor er weinig bekend is over de specifieke financiële schade veroorzaakt door het gebruik van cryptovaluta's in cybercriminaliteit. Om dit hiaat in kennis aan te pakken, zal dit onderzoek gebruik maken van landelijke registraties van slachtoffers en verdachten van de Nederlandse politie. Hierdoor wordt getracht om het 'wetenschappelijke gat' met betrekking tot het gebruik van cryptovaluta's in cybercriminaliteit te dichten. Dit onderzoek beoogt inzicht te verschaffen in de verschillen in het gebruik van cryptovaluta's tussen de verschillende vormen van cybercriminaliteit en of de financiële schade die daarmee gepaard gaat, varieert. De resultaten van dit onderzoek kunnen door opsporingsdiensten worden benut om effectievere strategieën te ontwikkelen voor preventie en bestrijding van cybercriminaliteit, met als doel het verminderen ervan.

De onderzoeksvraag luidt: *"Welke invloed heeft de coronapandemie op het gebruik van cryptovaluta's in cybercriminaliteit en hoe verschilt de financiële schade van het gebruik van cryptovaluta's tussen de vormen van cybercriminaliteit?"*

Om de onderzoeksvraag te beantwoorden zal kwantitatief onderzoek worden verricht. Het onderzoek maakt gebruik van landelijke registraties van slachtoffers en verdachten van de Nederlandse politie. De populatie voor dit onderzoek bestaat uit alle registraties van gedigitaliseerde- en cybercriminaliteit tussen 2019 en 2022. Deze registraties zullen worden geanalyseerd met behulp van een logistische en (lineaire) regressieanalyse.

De structuur van het onderzoek is als volgt: hoofdstuk 2 biedt een beschrijving van de theoretische achtergrond van het gebruik van cryptovaluta’s in cybercriminaliteit. Hoofdstuk 3 presenteert de methodologie, onderzoeksopzet en beschrijft de dataselectie en -verzameling. In hoofdstuk 4 worden de resultaten gepresenteerd. Ten slotte worden in hoofdstuk 5 de discussie, conclusie en aanbevelingen van het onderzoek gepresenteerd.

2. Theorie

2.1 Cryptovaluta's en cybercriminaliteit

Het criminele gebruik van cryptovaluta's neemt toe, aangezien deze steeds vaker worden geaccepteerd als betaalmiddel voor illegale goederen en diensten (Kenthineni & Cao, 2020). Cryptovaluta's zijn vormen van digitaal geld die gebruik maken van blockchain technologie om transacties uit te voeren (Politie, 2022). De blockchain is het gedecentraliseerde geldsysteem achter cryptovaluta's, dat geen tussenkomst van derde partijen zoals banken vereist om transacties te voltooien (Bele, 2021). In feite is niemand eigenaar van het systeem achter cryptovaluta's.

Binnen de context van cybercriminaliteit maken cybercriminelen op twee manieren gebruik van cryptovaluta's: als middel voor de facilitering van cybercriminaliteit en als doelwit van cybercriminaliteit (Reddy & Minnaar, 2018). Bij het gebruik van cryptovaluta's als faciliterend middel kunnen twee categorieën worden onderscheiden: het gebruik van cryptovaluta's om cybercriminaliteit te faciliteren en om criminele geldstromen te verhullen (Schrama et al., 2022).

Cryptovaluta's spelen een cruciale rol in cybercriminaliteit, aangezien ze betalingen faciliteren voor criminele transacties (Europol, 2020). De betrouwbaarheid, onomkeerbaarheid en relatieve anonimiteit van cryptovalutatransacties hebben geleid tot hun frequente gebruik door cybercriminelen bij bijvoorbeeld ransomware aanvallen en andere vormen van afpersing (Europol, 2020). Daarnaast fungeren cryptovaluta's als betaalmiddel op het Darkweb, waar illegale goederen en diensten kunnen worden verhandeld tegen betaling in cryptovaluta's (Schrama et al., 2022). Een voorbeeld van aankopen op het Darkweb zijn 'tools' die worden gebruik om cybercriminaliteit uit te voeren. Bovendien worden op het Darkweb ook 'cybercriminaliteit als dienst' aangeboden (Europol, 2020). Dit houdt in dat cybercriminaliteit wordt aangeboden in ruil voor betaling (Masschelein, 2019). Cybercriminaliteit als dienst draagt bij aan de toename van cybercriminaliteit, omdat het criminelen zonder geavanceerde technische kennis in staat stelt om cybercriminaliteit te plegen (Europol, 2020).

Bovendien worden cryptovaluta's vaak gebruik om illegaal verkregen geld te verbergen (Schrama et al., 2022). Cryptovaluta's kunnen worden verzonden naar specifieke mixers om hun herkomst te verhullen (Schrama et al., 2022). Deze mixers mengen de cryptovaluta's van verschillende personen, waardoor de herkomst van de cryptovaluta's wordt verborgen. Om gebruik te maken van deze mixerdienst moeten criminelen een commissie betalen (Schrama et al., 2022).

Vanwege de toenemende acceptatie van cryptovaluta's zijn ze steeds vaker het doelwit van cybercriminelen. Aanvallen op wisseldiensten, crypto bewaarportemonnees van individuen en bedrijven komen steeds vaker voor, zoals in 2019 waarbij tien hackaanvallen op wisseldiensten plaatsvonden en tweehonderdveertig miljoen aan cryptovaluta's werd buitgemaakt. Cybercriminelen richten zich op wisseldiensten omdat ze de cryptovaluta's van hun klanten opslaan. Er zijn enkele phishingcampagnes om toegang te krijgen tot de privésleutels van crypto bewaarportemonnees van individuen en bedrijven, waarmee ze de opgeslagen cryptovaluta's kunnen stelen.

Het bezit van cryptovaluta's is uitsluitend mogelijk in de online omgeving, waardoor fysiek bezit niet mogelijk is (Bele, 2021). De online omgeving verschilt op verschillende manieren van de fysieke omgeving. Er zijn zes kenmerkende mechanismen die deels verklaren hoe het gebruik van internet kan leiden tot crimineel gedrag (Van Huijstee et al., 2021). Deze mechanismen: alledaagsheid, verbindingen en netwerken, groeicapaciteit en bestendigheid, escalatie, virtuele realiteit en wanorde beschrijven hoe mensen in de online omgeving minder snel de gevolgen van hun acties kunnen overzien en minder snel ethisch te handelen in vergelijking met de fysieke omgeving (Van Huijstee et al., 2021).

Het gebruik van cryptovaluta's komt overeen met het mechanisme wanorde. De anonimiteit en wetteloosheid rondom cryptovaluta's dragen bij aan online immoreel gedrag. De relatieve anonimiteit van cryptovaluta's stelt cybercriminelen in staat om ongestraft criminele handelingen te verrichten, terwijl slachtoffers ook anoniem kunnen blijven. Deze anonimiteit leidt ertoe dat daders de risico's laag inschatten en eerder immoreel online gedrag vertonen. Daarnaast is er nog geen duidelijke regelgeving omtrent het gebruik van cryptovaluta's wat voor onduidelijkheid zorgt en overtredingen ongestraft laat. Het grenzeloze karakter van cryptovaluta's maakt internationale samenwerking nodig voor opsporing en berechting, maar dit is beperkt door gebrek aan invloed en uitleveringsverdragen. Tot slot ontbreken er normen over hoe cryptovaluta's moeten worden behandeld, wat leidt tot onduidelijkheid en een gebrek aan maatregelen tegen misbruik (Bele, 2021; Van Huijstee et al., 2022; Valgaeren & Linnemann, 2017; Bergen & Wijnen, 2017)

2.2 Het gebruik van cryptovaluta's en de coronapandemie

De routine-activiteitentheorie stelt dat criminaliteit plaatsvindt wanneer er sprake is van (1) een geschikt doelwit, (2) een gemotiveerde dader en (3) een gebrek of afwezigheid van geschikte toezichthouders (Cohen & Felson, 1979). Deze voorwaarden moeten allemaal vervuld zijn voor criminaliteit om plaats te vinden. Hoewel de theorie oorspronkelijk is ontwikkeld voor fysieke criminaliteit, is deze ook van toepassing op cybercriminaliteit, omdat dezelfde voorwaarden een rol kunnen spelen. De uitbraak van de coronapandemie heeft enkele veranderingen teweeggebracht die van invloed kunnen zijn op deze voorwaarden.

De routine-activiteitentheorie biedt een verklaring voor het toenemende gebruik van cryptovaluta's in cybercriminaliteit tijdens de coronapandemie. Ten eerste heeft de coronapandemie geleidt tot een toename van geschikte doelwitten. Door de economische gevolgen van de pandemie zijn sommige mensen in financiële moeilijkheden gekomen. Om extra geld te verdienen zijn velen zonder enige voorkennis in de wereld van cryptovaluta's gestapt (Botha et al., 2023). Deze individuen hebben vaak beperkte kennis over cryptovaluta's en de bijbehorende risico's, waardoor ze zich minder bewust zijn van de mogelijkheid om slachtoffer te worden van cybercriminaliteit (Botha et al., 2023). Ze kunnen gemakkelijk worden misleid door cybercriminelen die hen onder valse voorwendselen cryptovaluta's laten verzenden naar specifieke adressen (Botha et al., 2023).

Ten tweede heeft de coronapandemie geleid tot een toename van online activiteiten. Als gevolg van fysieke beperkingen werd thuiswerken de norm en waren mensen afhankelijk van online toegang tot informatie en middelen van bedrijven (Europol, 2020). Individuen die voorheen niet veel online actief waren, werden kwetsbaar voor cybercriminelen vanwege hun gebrek aan ervaring in online veiligheid (Europol, 2020). Dit heeft geresulteerd in een groter aantal potentiële doelwitten voor cybercriminaliteit.

Ten slotte heeft het grensoverschrijdende karakter van cryptovaluta's geleid tot een gebrek aan geschikte toezichthouders. Het feit dat cryptovaluta's grensoverschrijdend zijn, zorgt voor onduidelijkheid over welke autoriteiten verantwoordelijk zijn voor het opsporen en handhaven van crimineel gebruik ervan en bemoeilijkt de samenwerking tussen opsporingsdiensten (Van Huijstee et al., 2021). Tijdens de coronapandemie lag de focus van landen mogelijk niet primair op de bestrijding van cybercriminaliteit met betrekking tot cryptovaluta's. Het gebrek aan internationale samenwerking kan dus de toename van het gebruik van cryptovaluta's in cybercriminaliteit verklaren.

Al met al lijkt de coronapandemie het gebruik van cryptovaluta's in cybercriminaliteit te hebben gestimuleerd, voornamelijk vanwege de toename van potentiële slachtoffers en het gebrek aan adequaat toezicht. Op basis hiervan kan de volgende hypothese worden geformuleerd:
H1: Het gebruik van cryptovaluta's in cybercriminaliteit is toegenomen door de coronapandemie.

2.3. De financiële schade en het gebruik van cryptovaluta's tijdens de coronapandemie

De impact op de Nederlandse samenleving wordt gemeten aan de hand van de financiële schade die slachtoffers hebben geleden. Uit het 'Jaarbeeld Cybercriminaliteit 2021' van de Dienst Regionale Informatie Organisatie (DRIO) van de politie-eenheid Rotterdam blijkt dat in 2021 landelijk 32.429 Nederlanders slachtoffer zijn geworden van cybercriminaliteit (DRIO, 2021). Het totale schadebedrag als gevolg van cybercriminaliteit in datzelfde jaar bedroeg 116,4 miljoen euro, wat neerkomt op een gemiddelde schade van 3.589 euro per slachtoffer (DRIO, 2021). De financiële schade varieert afhankelijk van het type cybercriminaliteit. Bankhelpdeskfraude (33,7%), phishing (21,1%) en betaalverzoekfraude (13,3%) dragen het meest bij aan het totale schadebedrag (DRIO, 2021).

De aangiftebereidheid van slachtoffers speelt een essentiële rol bij het bepalen van de financiële schade voor de samenleving. De aangiftebereidheid van slachtoffers van cybercriminaliteit is aanzienlijk lager dan die van slachtoffers van traditionele vormen van cybercriminaliteit (Weijer et al., 2020). Slechts één op de zeven slachtoffers van cybercriminaliteit is bereid om aangifte te doen bij de politie. Met name bij delicten zoals ransomware, hacken en ddos-aanvallen is de aangiftebereidheid laag (Weijers et al., 2020). Slachtoffers geven aan dat ze geen aangifte doen omdat ze 'het zelf oplossen' of het gevoel hebben dat 'de politie er niks aan doet' (Weijers et al., 2020).

Het niet doen van aangifte kan om twee redenen leiden tot een hogere financiële schade voor de samenleving: onderschatting van de omvang van cybercriminaliteit en belemmering in de opsporing. Ten eerste leidt het niet doen van aangifte tot een toename van het 'dark number'. Het dark number verwijst naar de criminaliteit die wel heeft plaatsgevonden, maar niet bekend is en geregistreerd is bij de politie (Aljumily, 2017). Politiegegevens zijn gebaseerd op geregistreerde criminaliteit, wat betekent dat een lagere bereidheid om aangifte te doen resulteert in een onderbelichting van cybercriminaliteit (Politie, z.d.-a). Dit kan leiden tot verkeerde prioriteiten bij de politie, waar kostbare middelen elders worden ingezet terwijl cybercriminaliteit blijft bestaan.

Ten tweede belemmert het niet doen van aangifte de opsporing en vervolging van cybercriminelen. Een strafrechtelijk onderzoek kan pas worden gestart na het indienen van een aangifte (Politie, z.d.-a). Een lagere bereidheid om aangifte te doen beperkt te mogelijkheid om de geleden financiële schade via een strafrechtelijk onderzoek te verhalen op de daders, wat de financiële schade voor de samenleving verhoogt.

Het anonieme karakter van cryptovaluta's draagt bij aan een lagere bereidheid van slachtoffers om aangifte te doen. De anonimiteit van cryptovaluta's stelt cybercriminelen in staat om delicten te plegen en ermee weg te komen zonder te worden geïdentificeerd of vervolgd door opsporingsdiensten (Van Huijstee et al., 2021). Dit versterkt het gevoel van slachtoffers dat daders niet kunnen worden opgespoord en gestraft. Als gevolg hiervan ervaren slachtoffers machteloosheid, wat hun bereidheid om aangifte te doen verminderd.

Er is beperkte regelgeving en een tekort aan opsporingscapaciteit voor cybercriminaliteit vanwege de prioritering van andere zaken (Boekhoorn, 2019). Het gebruik van cryptovaluta's is nog relatief nieuw, waardoor opsporingsdiensten moeite hebben om de ontwikkelingen bij te houden (Schrama et al., 2022). Dit gebrek aan capaciteit en vermogen om cybercriminelen die gebruik maken van cryptovaluta's op te sporen, kan leiden tot een afname van het vertrouwen in de opsporing en het gevoel dat de politie actie onderneemt.

Ondanks de aangiftebereidheid van slachtoffers van cybercriminaliteit doorgaans lager is dan die van traditionele vormen van criminaliteit, heeft de coronapandemie mogelijk op twee manieren de aangiftebereidheid vergroot (Kruisbergen et al., 2021). Ten eerste werd vanaf april 2020 de mogelijkheid geboden om online aangifte te doen, wat de drempel voor het indienen van een aangifte heeft verlaagd (Kruisbergen et al., 2021). Het is namelijk minder tijdrovend om online aangifte te doen in vergelijking met fysiek naar het politiebureau te gaan (Weijer et al., 2020). Dit heeft geleid tot een toename van het aantal slachtoffers van cybercriminaliteit dat daadwerkelijk aangifte heeft gedaan.

Ten tweede heeft de coronapandemie geleid tot een toename van cybercriminaliteit waardoor mensen cybercriminaliteit steeds meer als 'normaal' zijn gaan beschouwen (Moors et al., 2022). Deze trend is zichtbaar in het aantal geregistreerde gevallen van cybercriminaliteit bij de politie. In 2020 is het aantal registraties van cybercriminaliteit verdubbeld ten opzichte van 2019 (Moors et al., 2022). Deze bevindingen worden ook bevestigd in de Veiligheidsmonitor van 2021 (Moors et al., 2022). Ongeveer 49 procent van de slachtoffers heeft in 2021 melding gemaakt bij een instantie wat hen is overkomen, en 19 procent heeft aangifte gedaan bij de politie (CBS, 2022b). In vergelijking met andere vormen van cybercriminaliteit doen slachtoffers van phishing het vaakst aangifte bij de politie (CBS, 2022b). Er lijkt zelfs sprake te zijn van een zekere 'normalisering'; naarmate cybercriminaliteit steeds normaler wordt beschouwd, neemt de bereidheid om aangifte te doen toe (Moors et al., 2022). De groei van cybercriminaliteit is versterkt door de coronapandemie en het lijkt erop dat deze trend de komende jaren niet zal afnamen (Moors et al., 2022).

Al met al blijkt dat de aangifte bereidheid van slachtoffers van cybercriminaliteit over het algemeen lager is dan die van traditionele vormen van criminaliteit. Het gebruik van cryptovaluta's lijkt bij te dragen aan een verhoogde financiële schade voor de samenleving, vanwege het anonieme karakter dat de aangiftebereidheid onder slachtoffers vermindert. Deze lagere aangiftebereidheid resulteert in minder mogelijkheden om de financiële schade op de daders te verhalen en leidt tot een onderbelichting van cybercriminaliteit, waarbij kostbare middelen elders worden ingezet. Op basis hiervan is de volgende hypothese opgesteld:
H2: De financiële schade voor de samenleving is toegenomen door het gebruik van cryptovaluta's in cybercriminaliteit.

2.4. Leeftijd

De 'leeftijd-criminaliteit curve' kan verklaren waarom jongeren vaker cryptovaluta's gebruiken bij cybercriminaliteit (Moffitt, 2018). Deze theorie onderscheidt twee groepen: de 'life-course persistent' en de 'adolescence-limited' groep. In de life-course persistent groep vertonen mensen aanhoudend crimineel gedrag vanaf hun kindertijd tot volwassentijd (Moffitt, 2018). Daarentegen vertonen mensen in de adolescence-limited groep tijdelijk crimineel gedrag dat afneemt naarmate ze ouder volwassen worden (Moffitt, 2018). Er zijn verschillende redenen waarom de adolescence-limited groep stopt met crimineel gedrag. Allereerst kunnen nieuwe verbindingen ontstaan naarmate mensen ouder worden, zoals het stichten van een gezin of het krijgen van een baan (Moffitt, 2018). Bovendien suggereert Moffit dat mensen naarmate ze ouder worden beter in staat zijn om hun impulsen te controleren en zich meer te richten op de toekomst (Moffitt, 2018). Ten slotte kunnen mensen naarmate ze ouder worden afstand nemen van delinquente vrienden, waardoor ze niet langer beïnvloed worden door hun criminele omgeving (Moffitt, 2018).

Er zijn verschillende ontwikkelingspaden waarlangs zowel jongeren als volwassenen interesse kunnen ontwikkelen in cybercriminaliteit. Wat betreft jongeren kunnen er drie verschillende ontwikkelingspaden worden onderscheiden die leiden tot interesse in cybercriminaliteit. Allereerst raken jongeren puur uit nieuwsgierigheid geïnteresseerd in cybercriminaliteit (Matthijsse et al., 2021). In een onderzoek van Matthijsse et al (2021) gaven negen van de veertien geïnterviewde jonge daders aan veel interesse te hebben in de werking van ICT. Deze jongeren zijn opgegroeid in het digitale tijdperk, waarin het internet en computers een prominente rol spelen in het dagelijks leven (CBS, 2021). Ze zijn benieuwd 'hoe ver ze kunnen gaan', zonder dat er een financieel motief lijkt te spelen (Matthijsse et al., 2021). Deze jonge daders lijken niet bewust de regels te willen overtreden, maar worden gedreven door nieuwsgierigheid en opwinding.

Ten tweede raken veel jonge daders geïnteresseerd in cybercriminaliteit via gaming (Matthijsse et al., 2021). De interesse in cybercriminaliteit ontstaat vaak binnen de gamewereld, doordat ze zelf slachtoffer worden van hacks door medespelers en daardoor nieuwsgierig worden of ze dit zelf ook kunnen doen (Matthijsse et al., 2021). In eerste instantie vinden de eerste cyberdelicten plaats binnen de gameomgeving, maar vervolgens verplaatsen ze zich naar de 'echte' wereld.

Tot slot ontwikkelen jongeren interesse voor cybercriminaliteit in de fysieke omgeving, zoals op school (Matthijsse et al., 2021). Hierbij is het verkrijgen van status en het uithalen van kattenkwaad het belangrijkste motief voor het plegen van cyberdelicten (Matthijsse et al., 2021). Het is echter belangrijk om op te merken dat de verschillende manieren waarop interesse in cybercriminaliteit kan ontstaan, elkaar kunnen overlappen (Matthijsse et al., 2021).

Niet alle daders van cybercriminaliteit starten echter op jonge leeftijd (Matthijsse et al., 2021). Wat de manieren waarop volwassen interesse kunnen ontwikkelen voor cybercriminaliteit betreft, kunnen twee verschillende situaties worden onderscheiden. Ten eerste kunnen daders van traditionele vormen van criminaliteit de overstap maken naar cybercriminaliteit. Daarnaast is het ook mogelijk dat traditionele vormen van criminaliteit worden gedigitaliseerd (Matthijsse et al., 2021).

Ten tweede kunnen volwassen daders van traditionele vormen van criminaliteit zich bezighouden met een cyberdelict in het kader van een klassiek delict (Matthijsse et al., 2021). In dergelijke gevallen gaat het voornamelijk om laagdrempelige vormen van cybercriminaliteit waarvoor geen complexe technische kennis vereist is, zoals het raden van wachtwoorden (Matthijsse et al., 2021).

Al met al kunnen zowel jongeren als volwassen daders betrokken zijn bij cybercriminaliteit. Er wordt echter verwacht dat jongeren meer geneigd zijn tot het plegen van cybercriminaliteit, aangezien over het algemeen meer cybercriminaliteit plaatsvindt tijdens de adolescentie (Moffitt, 2018). Naast deze verwachting wordt er ook aangenomen dat jongeren eerder geneigd zijn om cryptovaluta's te gebruiken bij het plegen van cybercriminaliteit, vanwege hun digitale kennis vaardigheden en kennis over het gebruik van cryptovaluta's in vergelijking met volwassenen (CBS, 2020). De hypotheses luiden als volgt:

H3: Jongeren plegen meer cybercriminaliteit dat ouderen.

H4: Jongeren maken meer gebruik van cryptovaluta's in cybercriminaliteit dan ouderen.

2.5. Geslacht

De zelfcontrole theorie van Gottfredson en Hirschi (1990) kan een verklaring bieden waarom mannen eerder geneigd zijn om cryptovaluta's te gebruiken bij cybercriminaliteit. Een lage zelfcontrole is de neiging van individuen om kortetermijnbevrediging na te streven zonder rekening te houden met de langetermijngevolgen van hun acties (Junger et al., 1995). Personen met een hoge zelfcontrole zijn beter in staat om hun emoties, impulsen en gedachten te reguleren en zich te richten op de langetermijngevolgen (Gottfredson & Hirschi, 1990). Daarentegen zijn personen met een lage zelfcontrole eerder geneigd om sociale regels te overtreden en vertonen zij vaker crimineel gedrag (Gottfredson & Hirschi, 1990).

Het niveau van zelfcontrole varieert tussen individuen, maar over het algemeen lijken mannen een lagere zelfcontrole te hebben dan vrouwen (Gibson et al., 2010). Dit betekent dat mannen mogelijk impulsiever reageren, zich sneller richten op het behalen van kortetermijndoelen en minder aandacht besteden aan langetermijngevolgen van hun acties. Cybercriminaliteit biedt een mogelijkheid om op korte termijn snel veel geld te verdienen, zonder dat daders zich voldoende bewust zijn van de mogelijke ernstige gevolgen van hun handelingen.

Daarnaast varieert ook de gevoeligheid voor status tussen individuen, maar over het algemeen zijn mannen gevoeliger voor status dan vrouwen (Rutenfrans, 1989). Vrouwen hechten over het algemeen meer waarde aan relaties en hechten meer belang aan anderen dan mannen (Rutenfrans, 1989). Het verkrijgen en behouden van status gaat vaak gepaard met competitie (Dijkstra & Veenstra, 2019). Om succesvol te zijn in competitieve situaties, is het vaak nodig om op te vallen. Mannen hebben meer de neiging om zowel op positieve als negatieve wijze af te wijken van de norm (Rutenfrans, 1989). Een negatieve manier om op te vallen en status te verwerven, is door betrokken te raken bij delinquent gedrag. Dit betekent dat mannen sneller geneigd kunnen zijn om crimineel gedrag te vertonen om status te verkrijgen.

Tot slot hebben mannen vaak meer mogelijkheden om betrokken te raken bij cybercriminaliteit dan vrouwen (Leek, 2022). Dit geldt ook voor de cryptowereld, waar mannen een dominante rol spelen. Zo bezitten mannen bijvoorbeeld 75% van alle cryptovaluta's (AFM, 2021). Op basis hiervan kunnen de volgende hypotheses worden geformuleerd:

H5: Mannen plegen meer cybercriminaliteit dan vrouwen.

H6: Mannen gebruiken meer cryptovaluta's in cybercriminaliteit dan vrouwen.

3. Methodologie

3.1 Research design

Dit onderzoek is kwantitatief van aard waarbij gebruik is gemaakt van een secundaire dataset afkomstig van de Nederlandse politie. Het doel van dit onderzoek was om inzicht te krijgen in het gebruik van cryptovaluta's in de verschillende vormen van cybercriminaliteit en de bijbehorende financiële schade. Deze dataset bevatte landelijke registraties van slachtoffers en verdachten van cybercriminaliteit waarbij het eventuele gebruik van cryptovaluta's bekend is. Slachtofferregistraties zijn geschikt om het gebruik van cryptovaluta's in cybercriminaliteit en de financiële schade van het gebruik ervan te onderzoeken, omdat zij informatie verstrekken over de vorm van cybercriminaliteit, het slachtoffer, geleden financiële schade en gebruik van cryptovaluta's. De registraties van de verdachten worden in dit onderzoek gebruikt om de leeftijd en geslacht van de cybercriminelen te onderzoeken. Door gebruik te maken van landelijke registraties kon er een beter beeld worden geschetst over het landelijke gebruik van cryptovaluta's in cybercriminaliteit. De onderzoekseenheden zijn de individuen die tussen 2019 en 2022 slachtoffer of verdachte waren van cybercriminaliteit

3.2 Dataverzameling

Voor dit onderzoek is er gebruik gemaakt van data uit BlueIntel. BlueIntel is een programma van de Nederlandse politie waarin informatie uit verschillende politieregistraties eenduidig wordt samengebracht om een nationaal beeld van cybercriminaliteit te ontwikkelen. De informatie in BlueIntel is in twee stappen tot stand gekomen.

Allereerst werden de registraties uit de Basis Voorziening Handhaving (BVH) gescand en aangevuld met informatie van partners en andere bronnen om de belangrijkste vormen van cybercriminaliteit inzichtelijk te krijgen (Borwell et al., 2020). BVH is het registratiesysteem van de politie waarin de aangiften en meldingen door burgers, bedrijven en andere instanties van misdrijven of overtredingen worden vastgelegd (Borwell et al., 2020). De registraties in BVH hebben een maatschappelijke klasse (MK) toebedeeld gekregen. Voor cybercriminaliteit bestaat de MK F90. In de praktijk blijkt echter dat meldingen van cybercriminaliteit niet altijd tot deze MK worden toebedeeld, omdat cybercriminaliteit vaak wordt gepleegd in combinatie met een ander delict (Borwell et al., 2020).

MK F90 geeft een onvolledig beeld van cybercriminaliteit binnen de politieregistraties. Hierdoor zijn met behulp van de Landelijke Cyber Query (LCQ) de vrije tekstvelden van de registraties in BVH geanalyseerd. De LCQ is een zoekvraag binnen de BVH-registraties bestaande uit trefwoorden die betrekking hebben op cybercriminaliteit in enge zin (Borwell et al., 2020). Voor het categoriseren van de met LCQ opgehaalde registraties worden hoofd- en subcategorieën gebruikt.

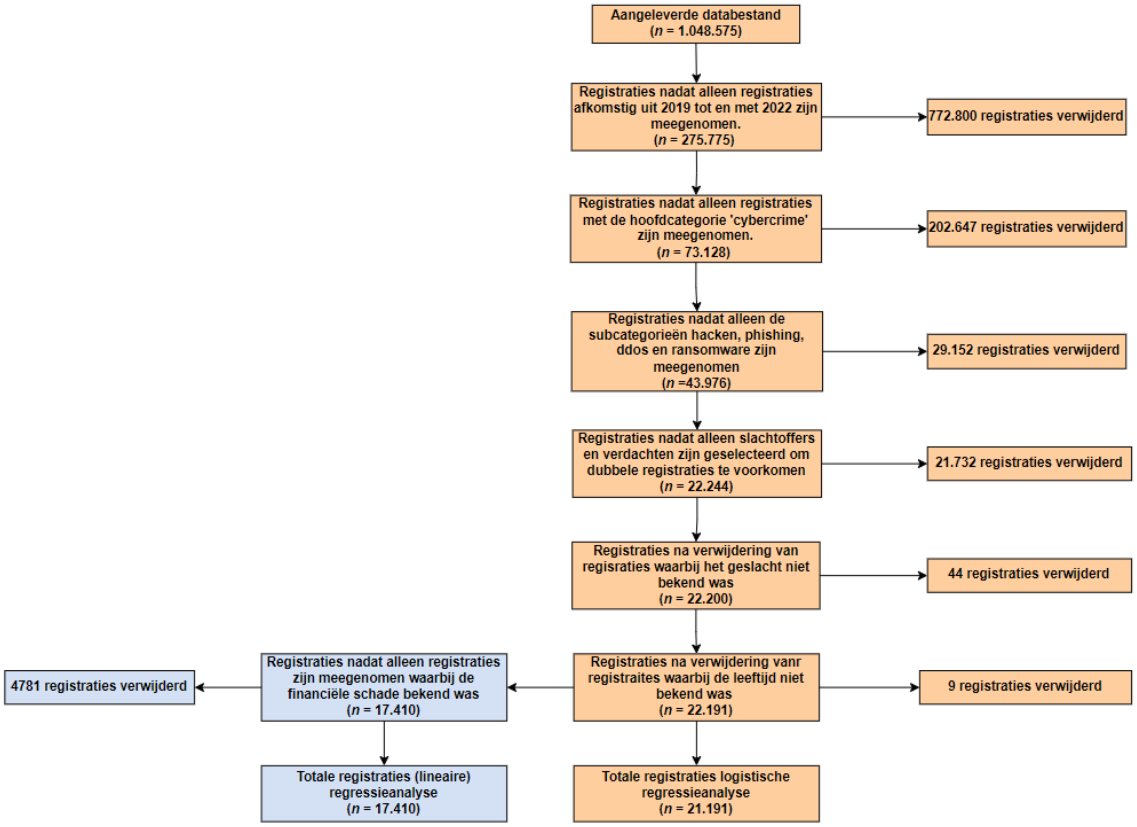
Hierbij zijn de hoofdcategorieën gebaseerd op het motief van de dader (Borwell et al., 2020). Hacktivisme, persoonsgerichte delicten, fraude/oplichting en afpersing/chantage zijn voorbeelden van hoofdcategorieën. Deze hoofdcategorieën zijn weer onderverdeeld in subcategorieën. De subcategorieën zijn gebaseerd op de gebruikte modus operandi. Bij fraude/oplichting kan het bijvoorbeeld gaan om helpdeskfraude.

Ten tweede zijn naar aanleiding van de gescande BVH-registraties de belangrijkste thema's geïdentificeerd en geselecteerd voor een verdiepende analyse (Borwell et al., 2020). In de analyse is specifiek de omvang, ontwikkeling en schade onderzocht. Het doel van deze verdiepende stap is om inzicht te krijgen in de grootte van cybercriminaliteit. Om dit te doen zijn er naast de BVH-registraties ook externe bronnen zoals wetenschappelijke literatuur en rapportages meegenomen.

Met behulp van BlueIntel zijn alle landelijke registraties van slachtoffers en verdachten waarbij er enige vorm van cybercriminaliteit bekend was verzameld. Deze registraties zijn aangeleverd door de data scientist van het cybercrimeteam van de politie Noord-Nederland. Hier was bewust voor gekozen omdat diegene meer ervaring had met het ophalen van informatie binnen de politiesystemen. Dit verhoogt tevens de validiteit van het onderzoek. Alle registraties werden vanuit BlueIntel geëxporteerd naar een Excelbestand en bestond in totaal uit 1.048.575 registraties. Deze registraties bevatten informatie over het jaartal, meldingsclassificatie, hoofd- en subcategorie, vorm van cybercriminaliteit, financiële schade, cryptogebruik, betrokkenen, begin- en geboortedatum, geslacht en leeftijd van de slachtoffers en verdachten.

3.3 Dataselectie

Om de onderzoeksvraag te kunnen beantwoorden is er een aantal selecties toegepast. Het aangeleverde databestand bestond uit 1.048.575 registraties. Allereerst zijn de registraties uit andere jaren dan 2019 tot en met 2022 of waarvan het jaartal niet bekend was verwijderd. Vervolgens zijn alleen de registratie met de maatschappelijke klasse 'cybercrime' meegenomen in dit onderzoek. Verder richtte dit onderzoek zich alleen op de hacken, phishing, ddos en ransomware wat betekent dat alle registraties die niet onder deze subcategorieën vallen zijn verwijderd uit het onderzoek. Tevens zijn alle registraties die niet betrekking hadden op het slachtoffer of de verdachte verwijderd uit de dataset. Deze selectie is uitgevoerd om dubbele registraties te voorkomen. Ook de registraties waarbij het geslacht niet bekend was zijn verwijderd. Tot slot zijn de registraties waarbij de leeftijd negatief of onbekend was verwijderd uit de dataset. Voor de (lineaire) regressieanalyse zijn de registraties waarbij de financiële schade niet bekend was verwijderd uit de dataset.. Figuur 1 geeft de dataselectie weer door middel van een stroomschema.



Figuur 1 **Flowchart met de selectie van de registraties**

3.4 Operationalisatie

Gebruik van cryptovaluta's

In dit onderzoek is het gebruik van cryptovaluta's de afhankelijke variabele in de logistische regressieanalyse. Aan de hand van deze variabele kan een eventuele verandering met betrekking tot het gebruik van cryptovaluta's door de coronapandemie worden onderzocht. Daarnaast geeft de variabele inzicht of het gebruik van cryptovaluta's verschilt tussen de verschillende vormen van cybercriminaliteit. Deze afhankelijke variabele is dichotoom van aard waarbij de volgende coderingen zijn gebruikt: geen gebruik gemaakt van cryptovaluta's = 0, wel gebruik gemaakt van cryptovaluta's = 1.

Vorm van cybercriminaliteit

Cybercriminaliteit in enge zin heeft betrekking op criminaliteit waarbij de computer of de software het doelwit is van criminelen (Van Erp et al., 2013). Cybercriminaliteit neemt in de praktijk verschillende verschijningsvormen aan waardoor in dit onderzoek specifiek op vier verschillende vormen van cybercriminaliteit wordt ingezoomd. Deze vormen van cybercriminaliteit zijn hacken, ddos-aanval, ransomware en phishing. In het databestand worden deze vormen van cybercriminaliteit aangegeven als subcategorieën. Er is bewust voor deze vormen van cybercriminaliteit gekozen, omdat zij de grootste dreiging zijn voor de maatschappij. Voor deze variabele zijn drie dummyvariabelen aangemaakt waarbij phishing dient als referentiegroep. Voor de eerste dummyvariabele wordt de volgende codering gebruikt: 1 = hacken, 0 = anders. In de tweede dummyvariabele is de volgende codering van toepassing: 1 = Ddos, 0 = anders. Tot slot wordt in de derde dummyvariabele de codering 1 = ransomware, 0 = anders, gebruikt.

Tijd in jaren

In de data is een variabele aanwezig die informatie geeft over het jaar waarin het cyberdelict heeft plaatsgevonden. Aan de hand van deze variabele kan er worden onderzocht welke invloed de coronapandemie heeft gehad op het gebruik van cryptovaluta's in cybercriminaliteit. Voor deze onafhankelijke variabele zijn drie dummyvariabelen aangemaakt waarbij 2019 dient als referentiegroep. Het jaar 2019 is gekozen als referentiegroep, omdat dit het jaar voorafgaand aan de coronapandemie is waardoor de verschillen tussen de jaren eenvoudiger met elkaar kunnen worden vergeleken. Voor de eerste dummyvariabele wordt de volgende codering gebruikt: 0 =2019, 1 = 2020 of later. In de tweede dummyvariabele is de codering 0 = 2019 en 2020, 1 = 2021 en 2022. Tot slot wordt in de derde dummyvariabele de volgende codering gebruikt: 0 = 2021 of eerder, 1 = 2022.

Financiële schade

De dataset bevat een variabele die informatie geeft over het schadebedrag van het slachtoffer en wordt in dit onderzoek gebruikt om de financiële schade op de samenleving te onderzoeken. In dit onderzoek is de financiële schade de afhankelijke variabele in de (lineaire) regressieanalyse en continu van aard. De variabele geeft inzicht of de financiële schade voor de samenleving verschilt tussen verschillende vormen van cybercriminaliteit. Het hoogste schadebedrag heeft een waarde van 5,7 miljoen euro en het laagste is dat er geen financiële schade is geleden. De variabele financiële schade is opgedeeld in verschillende intervallen. Voor een financiële schade tot 5.000 euro wordt een interval van 100 euro gehanteerd. Voor een financiële schade tussen 5.000 en 10.000 wordt een interval van 1.000 gebruikt. Voor een financiële schade tussen 10.000 en 100.000 euro wordt een interval van 10.000 euro gebruikt. Voor een financiële schade tussen 100.000 en 1.000.000 euro wordt een interval van 100.000 euro gebruikt. Ten slotte wordt voor schadebedragen tussen 1.000.000 en 5.000.000 een interval van 1.000.000 euro gebruikt. Registraties met een financiële schade hoger dan 5.000.000 euro vallen in de laatste categorie.

Geslacht

Voor de verschillende vormen van cybercriminaliteit wordt in de data informatie weergegeven over het geslacht van de verdachte. Hierbij kan de verdacht het mannelijke- of vrouwelijke geslacht aannemen. De variabele is gehercodeerd naar een dummyvariabele waarbij 0 = man en 1 = vrouw.

Leeftijd

Omdat er wordt verwacht dat jongeren sneller gebruikt zullen maken van cryptovaluta's in cybercriminaliteit, wordt er in dit onderzoek gecontroleerd voor leeftijd. In de data is een variabele aanwezig die informatie geeft over de leeftijd van het slachtoffer tijdens het delict. De leeftijd is berekend door de datum van het delict min de geboortedatum te doen. Er zijn geen wijzigingen aangebracht voor deze variabele.

3.5 Analyseplan

Voorafgaand aan de hypothesetoetsing worden de bivariate- en univariate statistieken beschreven om inzicht te geven in de verdeling van de variabelen en hun onderlinge samenhang. De samenhang tussen twee categorische variabelen wordt berekend met de Cramer's *V*. Voor de samenhang tussen een continue en een categorische variabele wordt een eenweg ANOVA gebruikt. De samenhang tussen twee continue variabelen wordt bepaald aan de hand van de Pearson's correlatie.

Allereerst zal er een logistische regressieanalyse in SPSS worden uitgevoerd om te achterhalen of de coronapandemie invloed had op het gebruik van cryptovaluta's in cybercriminaliteit. Een logistische regressieanalyse is geschikt, omdat de afhankelijke variabele – het gebruik van cryptovaluta's – dichotoom van aard is. In de logistische regressieanalyse zijn de onafhankelijke variabelen hiërarchisch toegevoegd. Allereerst werd in Model 1 de afhankelijke variabele 'gebruik van cryptovaluta's' samen met de onafhankelijke variabele 'tijd in jaren' toegevoegd. In Model 2 werden de dummyvariabelen van de onafhankelijke variabele 'vorm van cybercriminaliteit' toegevoegd aan het bestaande model. Ten derde werd in Model 3 de relevante interacties toegevoegd. Gezien de variabele 'tijd in jaren' en 'vorm van cybercriminaliteit' beide bestaan uit drie dummyvariabelen, resulteerde dit in negen interactievariabelen. Tot slot zijn in Model 4 de variabelen leeftijd en geslacht toegevoegd. De logistische regressieanalyse is gebaseerd op registraties van slachtoffers en verdachten. Deze registraties zijn geschikt voor de logistische regressieanalyse, omdat zij beide een indicatie geven over het gebruik van cryptovaluta's

Ten tweede wordt er een (lineaire) regressieanalyse uitgevoerd om de financiële impact van het gebruik van cryptovaluta's in de verschillende vormen van cybercriminaliteit te achterhalen. Er wordt een (lineaire) regressieanalyse uitgevoerd, omdat de afhankelijke variabele – financiële schade – continu van aard is. In Model 1 zijn de afhankelijke variabele 'financiële schade' en de onafhankelijke variabele 'tijd in jaren' toegevoegd. Ten tweede werd in Model 2 de onafhankelijke variabele 'vorm van cybercriminaliteit' toegevoegd. Vervolgens werd in Model 3 de onafhankelijke variabele 'gebruik van cryptovaluta's' toegevoegd. In Model 4 worden de interacties aan het model toegevoegd. Hierbij bestaat de eerste interactie uit 'het gebruik van cryptovaluta's' en 'vorm van cybercriminaliteit'. Dit wordt gedaan omdat er verwacht wordt dat het effect van het gebruik van cryptovaluta's op de financiële schade afhankelijk is van de vorm van cybercriminaliteit. De tweede interactie bestaat uit 'het gebruik van cryptovaluta's en 'tijd in jaren'. Ook dit wordt gedaan omdat het effect van het gebruik van cryptovaluta's op de financiële schade afhankelijk kan zijn van de vorm van cybercriminaliteit. Tot slot werden in Model 4 de variabele geslacht en leeftijd. Ook de (lineaire) regressieanalyse is gebaseerd op registraties van slachtoffers en verdachten, omdat voor beide registraties de financiële schade bekend is. Tot slot zullen de hypotheses met betrekking tot geslacht en leeftijd worden getoetst door middel van de logistische regressieanalyse en beschrijvende statistieken.

4. Resultaten

4.1 Beschrijvende statistieken

4.1.1. Univariate statistieken

Tabel 1 geeft de univariate statistieken weer voor de categorische en dichotome variabelen. Tabel 2 toont dezelfde statistieken, maar dan voor de continue variabele. Tabel 3 bevat de beschrijvende statistieken van de oorspronkelijke variabelen.

Uit Tabel 1 blijkt dat de meeste cybercriminaliteit plaatsvond in 2021. Het aantal geregistreerde gevallen van cybercriminaliteit steeg van 2.172 in 2019 (9,8%) naar 7.631 in 2021 (34,4%) en daalde vervolgens naar 7.180 registraties in 2022 (32,2%). Hierbij verwijzen de percentages naar het aandeel cybercriminaliteit in het desbetreffende jaar ten opzichte van het totale aantal registraties.

Tabel 1 toont aan dat er in 2019 bij 23 registraties (1,06%) bekend was dat er cryptovaluta's werden gebruikt. Dit percentage vertegenwoordigt het aandeel van het gebruik van cryptovaluta's in cybercriminaliteit voor dat specifieke jaar. In 2020 waren er 42 registraties met cryptovaluta's (0,80%). Het aantal registraties waarbij cryptovaluta's werden gebruikt steeg vervolgens in 2021 naar 134 registraties (1,76%). Het aandeel van het gebruik van cryptovaluta's was het hoogst in 2022, met 148 bekende registraties waarbij cryptovaluta's zijn gebruikt (2,06%).

Uit Tabel 1 blijkt dat het gebruik van cryptovaluta's relatief het laagst is bij phishing. Bij phishing zijn er 286 registraties bekend waarbij er cryptovaluta's zijn gebruikt, wat neerkomt op 1,34% van alle geregistreerde phishing incidenten. Ook voor hacken geldt dat er relatief weinig cryptovaluta's worden gebruikt. Zo zijn er in hacken slechts 9 registraties bekend waarbij er cryptovaluta's zijn gebruikt, wat neerkomt op 1,68% van alle geregistreerde hackincidenten. Daarentegen is het gebruik van cryptovaluta's in Ddos en ransomware relatief hoger. In Ddos zijn er 23 registraties bekend waarbij er cryptovaluta's zijn gebruikt, wat neerkomt op 21,30% van alle Ddos-incidenten. Bij ransomware zijn er 29 registraties bekend waarbij er cryptovaluta's zijn gebruikt, wat neerkomt op 13,49% van alle ransomware-incidenten.

Verder blijkt uit Tabel 1 dat mannen meer betrokken zijn bij cybercriminaliteit waarbij cryptovaluta's zijn gebruikt. Het aandeel van mannen als slachtoffer of verdachte bij dergelijke cybercriminaliteit bedraag 2,32%. Voor vrouwen ligt dit aandeel aanzienlijk lager, namelijk op slechts 0,67%.

Tabel 1
Beschrijvende statistieken categorische variabelen

Variabele				Gebruik van cryptovaluta's (*N* = 347)	
		Aantal	Percentage	Aantal	Percentage
Tijd in Jaren	0 = 2019	2.172	9,8%	23	1,06%
	1 = 2020	5.208	23,4%	42	0,80%
	2 = 2021	7.631	34,4%	134	1,76%
	3 = 2022	7.180	32,4%	148	2,06%
Vorm van cybercriminaliteit	1 = Hacken	535	2,4%	9	1,68%
	2 = Phishing	21.333	96,1%	286	1,34%
	3 = Ddos	108	0,5%	23	21,30%
	4 = Ransomware	215	1,0%	29	13,49%
Geslacht	0 = man	12.032	54,2%	279	2,32%
	1 = vrouw	10.159	45,8%	68	0,67%

Tabel 2
Beschrijvende statistiek continue variabelen

Variabele					Wel cryptogebruik (N = 347)			
	Aantal	Gemiddelde (st. dev)	Min	Max	Aantal	Gemiddelde (st. dev)	Min	Max
Financiële schade	12.271	5837,98 (60581,181)	0	5.700.000	194	59.075,08 (146846,597)	0	500.000
Leeftijd	22.191	49,57 (18,703)	8	95	347	41,55 (16,490)	17	82

4.1.2 Bivariate statistieken

Tabel 3 toont aan dat er een associatie bestaat tussen de afhankelijke variabele, het gebruik van cryptovaluta's, en alle onafhankelijke variabelen die zijn opgenomen in de logistische regressieanalyse. De associatie tussen het gebruik van cryptovaluta's en de vorm van cybercriminaliteit (V = ,147; p < ,001; N = 22.116) is het sterkst. Het is belangrijk op te merken dat de verdeling van het gebruik van cryptovaluta's verschilt. Het valt op dat er meer cryptovaluta's worden gebruik in Ddos (21,30%) en ransomware (12,49%) vergeleken met phishing (1,34%) en hacken (1,68%). Zie Tabel 1 voor de verdeling van het gebruik van cryptovaluta's tussen de verschillende vormen van cybercriminaliteit. Het is echter belangrijk op te merken dat de associatie tussen deze variabelen als zwak kan worden beschouwd, aangezien de associatie lager is dan 0,15.

Tabel 3
Samenhang tussen opgenomen variabelen

		1.	2.	3.	4.	5.	6.
1..	Gebruik van cryptovaluta's	-	,040**[A]	,147**[A]	,055**[B]	,066**[A]	,110**[B]
2.	Tijd in jaren	-	-	,049**[A]	,155**[B]	,031**[A]	,000[B]
3.	Vorm van cybercriminaliteit	-	-	-	,032**[B]	,075**[A]	,000[B]
4	Leeftijd	-	-	-	-	,063**[B]	,016[C]
5.	Geslacht	-	-	-	-	-	,032**[B]
6.	Financiële schade	-	-	-	-	-	-

**Significant bij tweezijdige p < ,001; [A] Berekend met Cramer's V, [B] Berekend met ANOVA F-toets, [C] Berekend met Pearson's correlatie

Tabel 3 toont aan dat naast de vorm van cybercriminaliteit, het gebruik van cryptovaluta's ook een relatief sterkere associatie vertoont met de afhankelijke variabele, financiële schade, in de (lineaire) regressieanalyse ($\sqrt{R^2}$ =,110; p < ,001; N = 22.116). Ook hier is het belangrijk op te merken dat gaat om een relatief zwakke associatie, aangezien de correlatie lager is dan 0,15. Dit betekent dat een verandering in één variabele geen voorspellende waarde heeft voor de andere variabele.

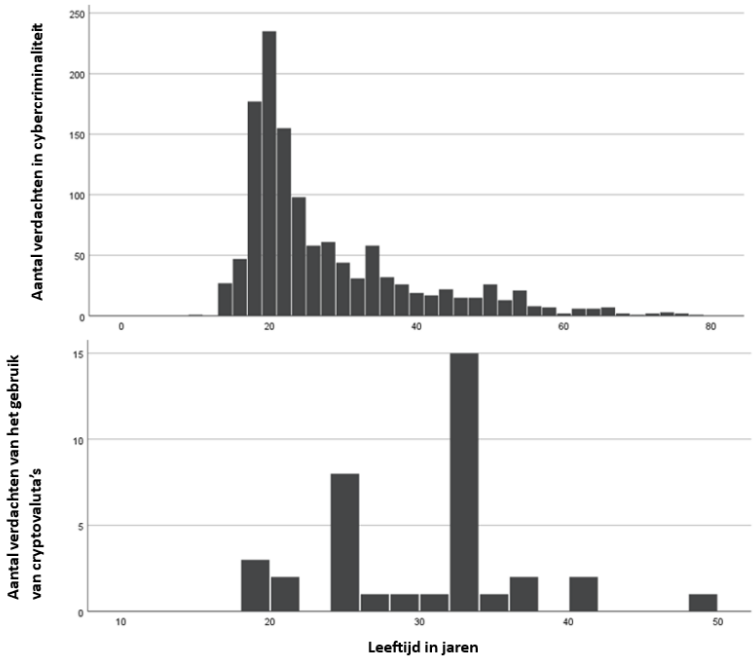
Verder toont Tabel 3 aan dat de afhankelijke variabele, financiële schade, in de (lineaire) regressieanalyse samenhangt met het geslacht ($\sqrt{R^2}$ = ,032; p < ,001; N = 22.116). De andere variabelen in de (lineaire) regressieanalyse vertonen geen samenhang met de financiële schade.

De resultaten in Tabel 3 geven de mate van samenhang tussen de variabelen weer. Aangezien enkele van de variabelen categorisch van aard zijn en bestaan uit vier categorieën, is het belangrijk om inzicht te krijgen in de verdeling tussen deze variabelen. De onderlinge verdeling van de categorische variabele wordt weergegeven in Tabel 4 en 5.

4.1.3. Gebruik van cryptovaluta's en leeftijd

In deze paragraaf worden de hypothesen over geslacht getoetst aan de hand van registraties van verdachten. De bovenste grafiek in Figuur 2 laat zien dat de meeste registraties van verdachten betrekking hebben op jongeren. Op basis van deze gegevens kan geconcludeerd worden dat er ondersteuning is gevonden voor de hypothese: "*jongeren plegen meer cybercriminaliteit dat ouderen"*

De onderste grafiek uit Figuur 2 laat zien dat de meeste verdachten die gebruik hebben gemaakt van cryptovaluta's tussen de 20 en 35 jaar oud zijn, wat als relatief jong beschouwd kan worden. Op basis van deze gegevens kan geconcludeerd worden dat er ondersteuning is gevonden voor de hypothese: "*jongeren maken meer gebruik van cryptovaluta's in cybercriminaliteit dan ouderen"*. Een gedetailleerde beschrijving van het gebruik van cryptovaluta's door verdachten is te vinden in Bijlage VII..

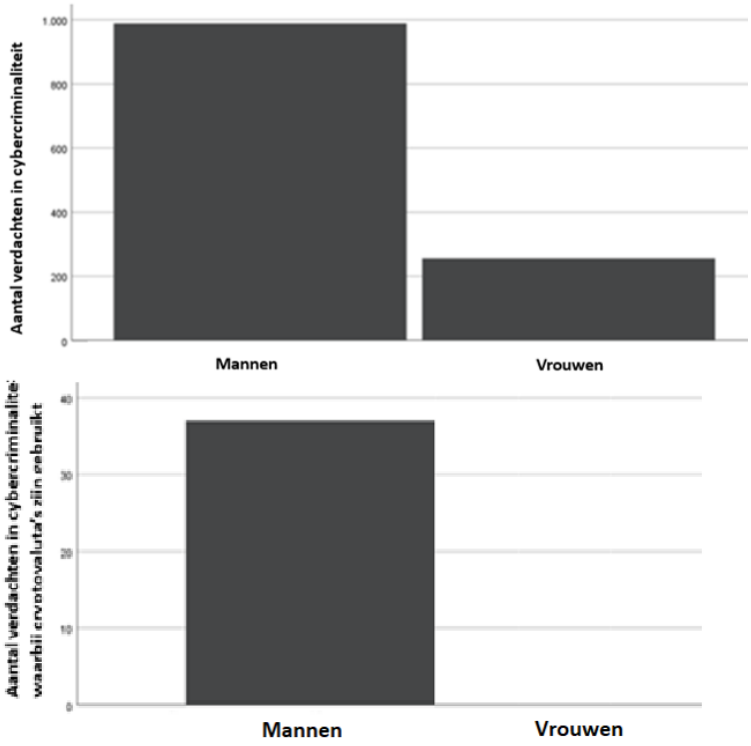


Figuur 2 **Leeftijd van de verdachten in cybercriminaliteit en cybercriminaliteit waarbij gebruik is gemaakt van cryptovaluta's**

4.1.4. Gebruik van cryptovaluta's en geslacht

In deze paragraaf worden de hypothesen over leeftijd getoetst aan de hand van registraties van verdachten. In de bovenste grafiek in Figuur 3 is te zien dat het aandeel mannelijk verdachten aanzienlijk groter is dan dat van vrouwen. Op basis van deze gegeven kan er worden gesteld dat er ondersteuning is gevonden voor de hypothese: "*Mannen plegen meer cybercriminaliteit dan vrouwen"*

In de onderste grafiek in Figuur 3 is er te zien dat in alle gevallen van cybercriminaliteit waarbij cryptovaluta's zijn gebruikt mannen verdacht worden. Op basis van deze gegevens kan er worden gesteld dat er ondersteuning is gevonden voor de hypothese: "*mannen maken meer gebruik van cryptovaluta's in cybercriminaliteit dan vrouwen".* Een volledige beschrijving van het gebruik van cryptovaluta's en geslacht is te vinden in Bijlage VIII.



Figuur 3 **Het geslacht van verdachten in cybercriminaliteit en waarbij er gebruik is gemaakt van cryptovaluta's**

4.2 Logistische regressieanalyse

In deze paragraaf worden de resultaten van de logistische regressie weergegeven. In deze logistische regressieanalyse zijn alleen de interacties tussen Ddos en de periode 2021 en 2022, ransomware en de periode 2021 en 2022 en ransomware en 2022 meegenomen. Deze interacties zijn opgenomen vanwege hun relatief lage standaardfout en significante resultaten. De resultaten van de volledige logistische regressieanalyse zijn te vinden in Bijlage IV.

4.2.1. Hypothesetoetsing

De eerste hypothese: *het gebruik van cryptovaluta's in cybercriminaliteit is toegenomen door de coronapandemie,* wordt getoetst aan de hand van de resultaten van Model 1 in de logistische regressieanalyse. Om de hypothese te toetsen, worden de odds-ratio's en bijbehorende *p*-waarden geanalyseerd. De odds-ratio in Model 1 geeft de verhouding weer van de kans op het gebruik van cryptovaluta's tijdens de jaren die vertegenwoordigd zijn in de dummyvariabelen, in vergelijking met de jaren die dat niet zijn. Hierbij fungeert 2019 als referentievariabele, aangezien dit het jaar is voorafgaand aan de coronapandemie.

Tijd in jaren

Er werd verwacht dat de coronapandemie het gebruik van cryptovaluta's in cybercriminaliteit zou verhogen. De pandemie begon in 2020, met de strengste maatregelen die werden genomen in 2021. Model 1 toont aan dat de kans op het gebruik van cryptovaluta's in cybercriminaliteit in 2021 en 2022 significant hoger is ten opzichte van 2019 en 2020 (b = 1,299; p < ,001; OR = 3,665). Deze resultaten ondersteunen de hypothese dat de coronapandemie het gebruik van cryptovaluta's in cybercriminaliteit heeft verhoogd. Er is echter geen significante toename in 2022 ten opzichte van 2019, 2020 en 2021 (b = ,185; p = ,149; OR = 1,203).

Model 1 toont aan dat er in de jaren 2020, 2021 en 2022 nog geen significante verhoging was van de kans op het gebruik van cryptovaluta's in cybercriminaliteit (b = -,271; p = ,451; OR = ,763). De resultaten ondersteunen echter wel de hypothese voor de jaren 2021 en 2022 in vergelijking met 2020 en 2019

Vorm van cybercriminaliteit

De resultaten in Model 2 tonen aan dat de kans op het gebruik van cryptovaluta's verschilt voor de verschillende vormen van cybercriminaliteit. De odds-ratio in dit model kan worden geïnterpreteerd als de verhouding van de kans op het gebruik van cryptovaluta's in vergelijking met phishing. Allereerst toont Model 2 aan dat de kans op het gebruik van cryptovaluta's voor hacken niet hoger is vergeleken met phishing (*b* = -,162; *p* = ,721 ; *OR* = ,850), na controle voor de andere variabelen uit Model 2. Het is echter belangrijk op te merken dat het gaat om een niet significant resultaat. Model 2 geeft echter een ander resultaten voor ddos en ransomware. In Model 2 is te zien dat de kans op het gebruik van cryptovaluta's aanzienlijk hoger is bij Ddos vergeleken met phishing (*b* = 4,060 ; *p* <,001; *OR* = 57,998), na controle voor de andere variabelen uit Model 2. Dit betekent dat de odds op het gebruik van cryptovaluta's 57,998 keer hoger is voor Ddos dan voor phishing. De kans op het gebruik van cryptovaluta's is ook voor ransomware aanzienlijk hoger dan voor phishing (*b* = 2,887; *p* <,001 = ; *OR* = 17,940).

Interacties

Model 3 toont aan dat er sprake is van een negatieve interactie tussen de variabelen Ddos en de periode 2021 en 2022 (*b* = -4,643; *p* < ,001; *OR* = ,010). Ddos op zichzelf verhoogt de kans op het gebruik van cryptovaluta's in cybercriminaliteit (*b* = 6,280; *p* < ,001; *OR* = 533,679). De negatieve interactiecoëfficiënt van -4,643 geeft aan dat de interactie tussen Ddos en de periode 2021 en 2022 een negatief effect hebben op de log-odds van het gebruik van cryptovaluta's in cybercriminaliteit. Het suggereert dat het effect van Ddos op het gebruik van cryptovaluta's in de periode 2021 en 2022 significant lager is in vergelijking met 2020 en 2019.

De odds-ratio van 0,010 geeft aan dat de odds op het gebruik van cryptovaluta's sterk verminderd worden wanneer zowel Ddos aanwezig is als de periode 2021 en 2022. Oftewel, in de periode 2021 en 2022 is de kans op het gebruik van cryptovaluta's in cybercriminaliteit significant lager wanneer Ddos aanwezig is.

Verder toont Model 3 aan dat er sprake is van een negatieve interactie tussen de variabelen ransomware en de periode 2021 en 2022 (*b* = -2,924; *p* < ,001; *OR* = ,054). Ransomware op zichzelf verhoogt de kans op het gebruik van cryptovaluta's in cybercriminaliteit (*b* = 4,929; *p* < ,001; *OR* =138,282). De negatieve interactiecoëfficiënt van -2,924 geeft aan dat de interactie tussen ransomware en de periode 2021 en 2022 een negatief effect kan hebben op de log-odds van het gebruik van cryptovaluta's in cybercriminaliteit. Het suggereert dat het effect van ransomware op het gebruik van cryptovaluta's in de periode 2021 en 2022 significant lager is in vergelijking met 2020 en 2019.

De odds-ratio van 0,054 geeft aan dat de odds op het gebruik van cryptovaluta's in cybercriminaliteit sterk verminderd worden wanneer zowel ransomware aanwezig is als de periode 2021 en 2022. Oftewel, in de periode 2021 en 2022 is de kans op het gebruik van cryptovaluta's in cybercriminaliteit significant lager wanneer ransomware aanwezig is.

Verder is het belangrijk om op te merken dat er geen sprake is van een positieve interactie tussen ransomware en 2022, maar dat de interactie relatief dichtbij het significantieniveau ligt. Dit betekent dat er geen sterk bewijs is om te concluderen dat er geen sprake is van een interactie tussen ransomware en 2022.

Op basis van de resultaten van de logistische regressieanalyse in Tabel 4 zijn de voorspelde kansen berekend. Een gedetailleerd overzicht van de berekeningen is te vinden in Bijlage VIII. Zie Figuur 4 voor een visuele weergave van de voorspelde kansen.

Figuur 4 **Overzicht voorspelde kansen op het gebruik van cryptovaluta's voor 2021 en 2022, Ddos, ransomware en de interactie**

Figuur 4 toont aan dat de kans op het gebruik van cryptovaluta's in ransomware en Ddos hoger is in vergelijking met hacken en phishing. De relatief hoge kans op het gebruik van cryptovaluta's voor Ddos en ransomware kan worden verklaard door het aandeel in het gebruik van cryptovaluta's. Zoals blijkt in Figuur 6, is het aandeel van het gebruik van cryptovaluta's aanzienlijk groter bij Ddos in de periode 2019 en 2020. Bovendien is te zien dat de kans op het gebruik van cryptovaluta's over het algemeen groter is in de periode 2021 en 2022. Dit is echter niet het geval voor de kans op het gebruik van Ddos in 2019 en 2020 (21,45%). Ten slotte kan er worden geconcludeerd dat de kans op het gebruik van cryptovaluta's in de loop van de tijd is toegenomen.

Geslacht

De resultaten van Model 4 laten zien dat vrouwen een lagere kans hebben om betrokken te zijn bij cybercriminaliteit waarbij cryptovaluta's worden gebruikt (b = -2,270; p <,001; OR = ,103),na controle voor de andere variabelen uit Model 4. Op basis van deze bevindingen kan geconcludeerd worden dat er ondersteuning is gevonden voor de hypothese: *Mannen zijn meer betrokken bij cybercriminaliteit waarbij cryptovaluta's worden gebruikt dan vrouwen.*

Leeftijd

De resultaten van Model 4 tonen aan dat de kans op betrokkenheid bij cybercriminaliteit waarbij cryptovaluta's worden gebruikt afneemt naarmate iemand ouder wordt (*b* = -,036; *p* <,001; *OR* = ,965), na controle voor de andere variabelen uit Model 4. Op basis van deze bevindingen kan geconcludeerd worden dat er ondersteuning is gevonden voor de hypothese: *Jongeren zijn meer betrokken bij cybercriminaliteit waarbij cryptovaluta's worden gebruikt dat ouderen*.

4.2.2. Modelevaluatie

Allereest bestaat de dataset uit onafhankelijke waarnemingen, omdat er slechts één registratie bekend is per delict. Verder moet er bij de logistische regressieanalyse worden getoetst of de modellen voldoende aansluiten bij de data. Dit wordt beoordeeld aan de hand van de Deviance en Hosmer-Lemeshow test. Een lagere Deviance geeft aan dat het model beter bij de data past. Tabel 4 toont aan dat de Deviance significant afneemt bij elk nieuw model, wat betekent dat de nieuwe modellen beter aansluiten bij de data.

In dit onderzoek wordt er gebruik gemaakt van een grote dataset met 21.116 registraties. Dit betekent dat de Hosmer-Lemeshow test niet wordt geanalyseerd voor de modelevaluatie, omdat zelf kleine verschillen snel een significant resultaat kunnen opleveren. Hierbij is het belangrijk om op te merken dat de geobserveerde- en verwachte aantallen met elkaar overeenkomen. Op basis van de Deviance kan er worden geconcludeerd dat elk nieuwe model beter in staat is om het gebruik van cryptovaluta's te verklaren.

Tabel 4
Resultaten logistische regressieanalyse

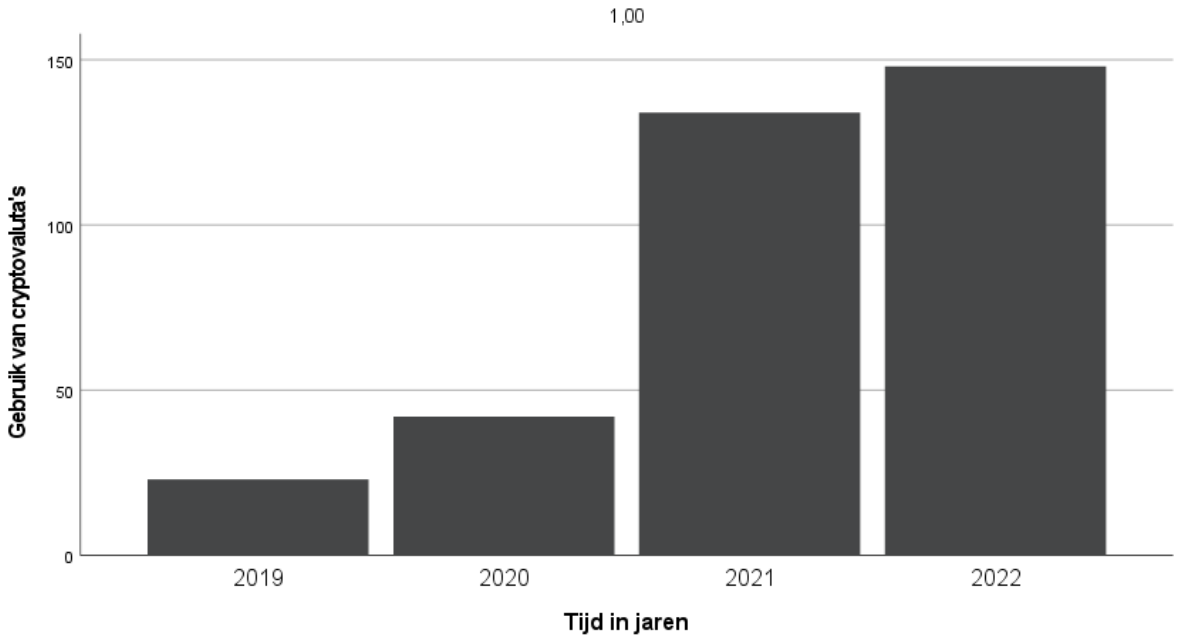
	Model 1			Model 2			Model 3			Model 4		
	b (SE)	Odds-ratio	*p*	*b* (SE)	Odds-ratio	*p*	*b* (SE)	Odds-ratio	*p*	*b* (SE)	Odds-ratio	*p*
Constante	-5,188 (,289)	,006	<,001	-5,975 (,317)	,003	<,001	-7,578 (,547)	,001	<,001	-5,679 (,563)	,003	<,001
2020 of later	-,271 (,360)	,763	,451	,058 (,370)	1,059	,876	,419 (,399)	1,520	,294	,582 (,410)	1,789	,155
2021 of 2022	1,299 (,233)	3,665	<,001	1,610 (,246)	5,001	<,001	2,957 (,465)	19,242	<,001	3,056 (,466)	21,235	<,001
2022	,185 (,128)	1,203	,149	,184 (,131)	1,201	,161	,104 (,134)	1,109	,438	,150 (,135)	1,162	,267
HackenR				-,162 (,455)	,850	,721	-,172 (,455)	,842	,705	-,493 (,459)	,611	,282
Ddos				4,060 (,279)	57,998	<,001	6,280 (,519)	533,679	<,001	5,414 (,527)	224,593	<,001
Ransomware				2,887 (,218)	17,940	<,001	4,929 (,587)	138,282	<,001	4,730 (,591)	113,311	<,001
Ddos * 2021 en 2022							-4,643 (,902)	,010	<,001	-4,616 (,917)	,010	<,001
Ransomware * 2021 en 2022							-2,924 (,759)	,054	<,001	-2,893 (,768)	,055	<,001
Geslacht (1 = vrouw; 0 = man)										-2,270 (,229)	,103	<,001
Leeftijd										-,036 (,004)	,965	<,001
Deviance	2957,832			2733,417			2682,363			2406,492		
X2-toets	71,505		<,001	224,414		<,001	51,054		<,001	275,871		<,001
N	22.116			22.116			22.116			22.116		

4.3. Bivariate toetsing

4.3.1. Coronapandemie en het gebruik van cryptovaluta's

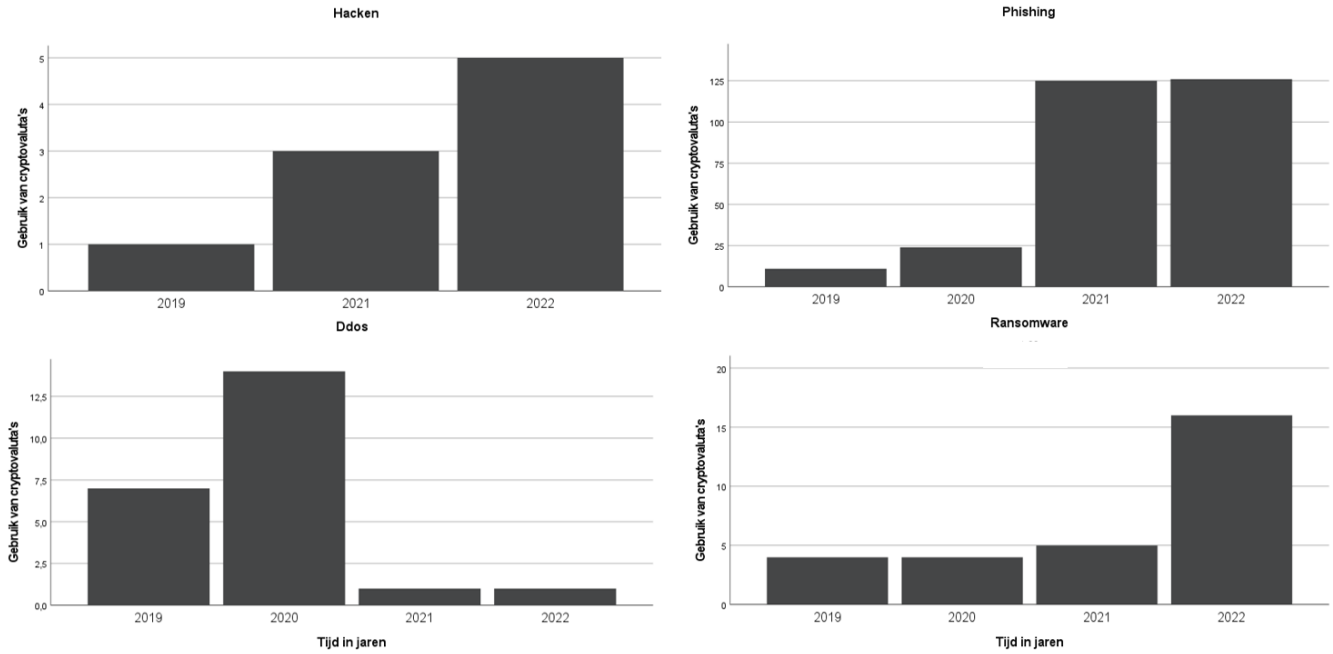
Om voorafgaande resultaten te ondersteunen, worden in deze paragraaf beschrijvende statistieken gepresenteerd met betrekking tot het gebruik van cryptovaluta's in cybercriminaliteit. Een gedetailleerde beschrijving van het gebruik van cryptovaluta's in cybercriminaliteit en de ontwikkeling voor geslacht en leeftijd is te vinden in Bijlage VI.

De bevindingen die aantonen dat het gebruik van cryptovaluta's in cybercriminaliteit is toegenomen door de coronapandemie worden ondersteund door de resultaten in Figuur 5. In deze figuur wordt 2019 beschouwd als het referentiejaar vóór de coronapandemie. Het aantal geregistreerde gevallen van cybercriminaliteit waarbij cryptovaluta's zijn gebruikt, is jaarlijks gestegen. In 2020 is het gebruik van cryptovaluta's met 82,61% gesteken ten opzichte van 2019. In 2021 is het gebruik van cryptovaluta's met 219,05% gestegen ten opzichte van 2020. In 2022 steeg het gebruik van cryptovaluta's met 10,45% ten opzichte van 2021. De meest significante stijging van het gebruik van cryptovaluta's in cybercriminaliteit vond plaats tussen 2020 en 2021, wat overeenkomt met de tijdslijn van de coronapandemie. Raadpleeg Figuur 5 voor een visuele weergave van het gebruik van cryptovaluta's in cybercriminaliteit



Figuur 5 **De ontwikkeling van het gebruik van cryptovaluta's van 2019 tot en met 2022**

Gemiddeld genomen werd in 1,56 van de registraties over de vier jaar cryptovaluta's gebruikt. De sterkste stijging is te zien van 2020 naar 2021. Zowel in absolute getallen als in percentages, komt deze stijging overeen met de tijdlijn van de coronapandemie. Op basis van deze resultaten kan er geconcludeerd worden dat het gebruik van cryptovaluta's in cybercriminaliteit is toegenomen door de coronapandemie. Raadpleeg Tabel 1 voor het aandeel van cybercriminaliteit waarbij cryptovaluta's zijn gebruikt.



Figuur 6 De ontwikkeling van het gebruik van cryptovaluta's van 2019 tot en met 2022 voor de verschillende vormen van cybercriminaliteit

Uit Figuur 6 blijkt dat er verschillen zijn in de ontwikkeling van het gebruik van cryptovaluta's bij verschillende vormen van cybercriminaliteit. Tussen 2019 en 2022 is het aantal registraties van hack-, phishing- en ransomware delicten waarbij cryptovaluta's zijn gebruikt toegenomen. Bij hacken is het gebruik van cryptovaluta's gestegen van 1 registratie in 2019 naar 5 registraties in 2022. In 2020 waren er geen hackregistraties bekend waarbij cryptovaluta's zijn gebruikt. Het aantal phishingregistraties waarbij cryptovaluta's zijn gebruikt, is gestegen van 11 in 2019 naar 126 in 2022. De sterkste stijging in het gebruik van cryptovaluta's bij phishing vond plaats tussen 2020 en 2021, waarbij het aantal registraties steeg van 24 in 2020 naar 125 in 2021. Ook voor ransomware is een toename te zien in het gebruik van cryptovaluta's. Het aantal ransomwareregistraties is gestegen van 4 in 2019 naar 16 in 2022. De sterkste stijging vond plaats tussen 2021 en 2022, waarbij het aantal registraties toenam van 5 in 2021 naar 16 in 2022.

In tegenstelling tot de andere vormen van cybercriminaliteit is het gebruik van cryptovaluta's bij ddos-aanvallen gedaald. In Figuur 6 is te zien dat het aantal registraties waarbij cryptovaluta's zijn gebruikt is verdubbeld van 7 in 2019 naar 14 in 2020 om vervolgens weer te dalen naar 1 registratie in zowel 2021 als 2022.

4.4. Lineaire regressieanalyse

In Tabel 5 worden de resultaten van de (lineaire) regressieanalyse weergegeven, waarbij financiële schade de afhankelijke variabele is.

4.4.1. Hypothesetoetsing

De tweede hypothese "*de financiële schade voor de samenleving is toegenomen door het gebruik van cryptovaluta's"*, wordt getoetst aan de hand van de resultaten van Model 3. Om de hypothese te testen worden de hellingen (*b*) en bijhorende *p*-waarden geëvalueerd. De resultaten van Model 3 in Tabel 5 tonen aan dat het gebruik van cryptovaluta's leidt tot een significante stijging van de financiële schade (b = 18,995; p <,001). Dit impliceert dat de financiële schade van cybercriminaliteit toeneemt wanneer er cryptovaluta's worden gebruikt. Op basis van deze resultaten kan geconcludeerd worden dat er ondersteuning is gevonden voor de hypothese dat het gebruik van cryptovaluta's heeft bijgedragen aan een gemiddelde toename van de financiële schade gedurende de periode van 2019 tot 2022 voor alle vormen van cybercriminaliteit.

Tijd in jaren

Model 1 toont aan dat de financiële schade van cybercriminaliteit per jaar significant toeneemt (b = 1,905; p < ,001). Dit betekent dat voor elke toename van één jaar de financiële schade gemiddeld met 1,905 eenheden stijgt. Bijvoorbeeld, in 2019 was de gemiddelde financiële schade tussen 1200 en 1299,99 euro (b = 13,015; p = ,000). Met een jaarlijkse toename van 1,905 eenheden, lag de financiële schade in 2020 tussen 1300 en 1399,99 euro. In 2021 bedroeg de gemiddelde financiële schade tussen 1500 en 1599,99 euro. Tot slot, in 2022 was de financiële schade tussen de 1700 en 1799,99 euro.

Vorm van cybercriminaliteit

Model 2 toont aan dat de financiële schade verschilt voor de verschillende vormen van cybercriminaliteit. De gemiddelde financiële schade van phishing wordt in 2019 geschat tussen de 1100 en 1199,99 euro (b = 12,982; p = ,000). Uit de resultaten blijkt dat de gemiddelde financiële schade voor hacken significant lager is in vergelijking met phishing (b = -12,337; p < ,001). Dit betekent dat de financiële schade als gevolg van hacken naar schatting gemiddeld 12,337 eenheden lager ligt in de periode van 2019 tot 2022 in vergelijking met phishing. Als er bijvoorbeeld naar het jaar 2019 wordt gekeken, bedroeg de schade als gevolg van hacken tussen 0,05 en 99,99 euro.

Verder laat Model 2 zien dat de gemiddelde financiële schade van Ddos significant hoger is dan die van phishing (b = 10,684; p < ,001). Dit betekent dat de financiële schade als gevolg van Ddos naar schatting gemiddeld 10,684 eenheden hoger ligt in de periode van 2019 tot 2022 in vergelijking met phishing. Als er bijvoorbeeld naar het jaar 2019 wordt gekeken, bedroeg de schade als gevolg van Ddos tussen 2200 en 2299,99 euro.

Bovendien toont Model 2 aan dat de gemiddelde financiële schade van ransomware significant hoger is dan die van phishing (b = 4,318; p = ,036). Dit bekent dat de financiële schade als gevolg van ransomware naar schatting gemiddeld 4,318 eenheden hoger ligt in de periode van 2019 tot 2022 in vergelijking met phishing. Als er bijvoorbeeld naar het jaar 2019 wordt gekeken, bedroeg de schade als gevolg van ransomware tussen 1600 en 1699,99 euro. Het is belangrijk op te merken dat de financiële schade van de verschillende vormen van cybercriminaliteit specifiek betrekking heeft op situaties waarbij geen cryptovaluta's zijn gebruikt.

Interacties

Allereest toont Model 5 dat er sprake is van een positieve interactie tussen 'het gebruik van cryptovaluta's en 'tijd in jaren' (b = 3,203; p = ,029). Om het interactie effect beter te begrijpen is het belangrijk om eerst naar de afzonderlijke variabelen te kijken. Model 5 toont aan dat de gemiddelde financiële schade per jaar stijgt wanneer er geen gebruik wordt gemaakt van cryptovaluta's (b = 1,853; p <,001). Dit betekent dat elk jaar de gemiddelde financiële schade met 1,853 eenheden stijgt, wanneer er geen gebruik wordt gemaakt van cryptovaluta's.

Verder blijkt uit Model 5 dat het gebruik van cryptovaluta's in 2019 een aanzienlijke toename van de gemiddelde financiële schade als gevolg van phishing heeft veroorzaakt (b = 12,943; p <,001). Dit impliceert dat in 2019 de gemiddelde financiële schade als gevolg van phishing met 12,943 eenheden stijgt wanneer cryptovaluta's worden gebruikt.

De interactie toont aan dat het gebruik van cryptovaluta's significant verband houdt met een aanzienlijke stijging van de gemiddelde financiële schade per jaar (b = 3,203; p = ,029). Dit impliceert dat de gemiddelde financiële schade jaarlijks 3,203 eenheden extra stijgt wanneer er gebruik wordt gemaakt van cryptovaluta's in vergelijking met situaties waarin ze niet worden gebruikt (b = 1,853; p < ,001). Op basis van deze resultaten kan geconcludeerd worden dat het gebruik van cryptovaluta's de gemiddelde financiële schade versterkt.

Ten tweede wijst Model 4 op een negatieve interactie tussen het gebruik van cryptovaluta's en ransomware (b = -27,654; p < ,001). Om het interactie effect beter te begrijpen is het belangrijk om eerst naar de afzonderlijke variabelen te kijken. Model 4 laat zien dat de gemiddelde financiële schade als gevolg van ransomware stijgt in vergelijking met phishing, wanneer er geen gebruikt wordt gemaakt van cryptovaluta's (b = 5,540; p = ,012).

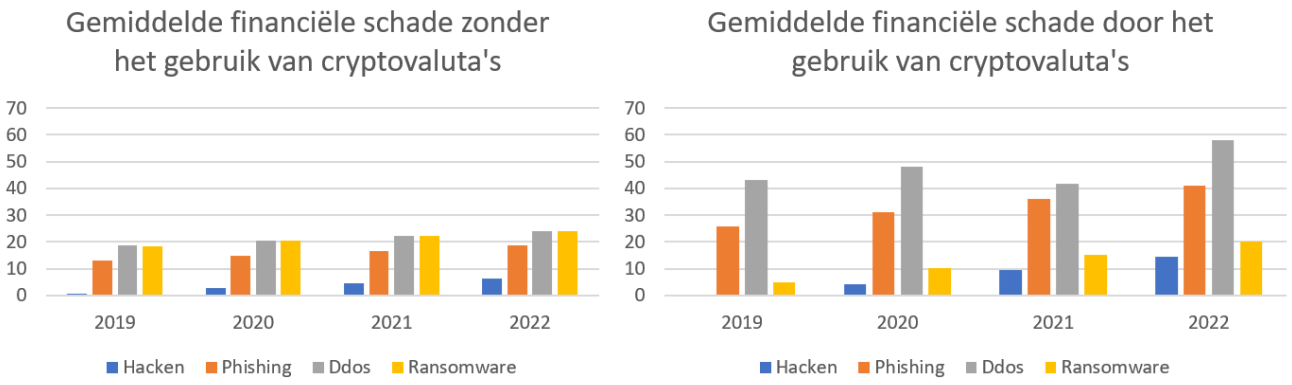
Verder blijkt uit Model 4 dat het gebruikt van cryptovaluta's in 2019 een aanzienlijke toename van de gemiddelde financiële schade als gevolg van phishing heeft veroorzaakt (b = 20,268; p < ,001). Dit impliceert dat in 2019 de gemiddelde financiële schade als gevolg van phishing met 20,268 eenheden stijgt wanneer cryptovaluta's worden gebruikt.

Model 4 toont aan dat de aanwezigheid ransomware aanzienlijk de toename van de gemiddelde financiële schade door het gebruik van cryptovaluta's verzwakt (b = -27,654; p < ,001). Dit impliceert dat de gemiddelde financiële schade van het gebruik van cryptovaluta's in ransomware, in vergelijking met het gebruik van cryptovaluta's in phishing, met 27,654 eenheden afneemt. Op basis van deze resultaten kan geconcludeerd worden dat het gebruik van cryptovaluta's in ransomware de gemiddelde financiële schade verzwakt.

De interactie toont aan dat de relatie tussen het gebruik van cryptovaluta's en de financiële schade wordt beïnvloed door ransomware. De resultaten van de interactie geven aan dat het effect van het gebruik van cryptovaluta's op de financiële schade wordt verzwakt bij de aanwezigheid van ransomware. Op basis van de resultaten in Model 4 kunnen er geen conclusies worden getrokken over de andere interacties, omdat deze niet significant zijn.

Tot slot is er echter in Model 6 wel sprake van een negatieve interactie tussen het gebruik van cryptovaluta's en hacken (b = -17, 255; p = ,047). Om het interactie effect beter te begrijpen is het belangrijk om eerst naar de afzonderlijke variabele te kijken. Uit Model 6 blijkt dat het gebruik van cryptovaluta's in 2019 een aanzienlijke toename van de gemiddelde financiële schade als gevolg van phishing heeft veroorzaakt (b = 13,329; p < ,001). De interactie toont aan dat de gemiddelde financiële schade van het gebruik van cryptovaluta's als gevolg van hacken in 2019 aanzienlijk lager is in vergelijking met phishing (b = -17,255; p = ,047). Dit impliceert dat de gemiddelde financiële schade als gevolg van het gebruik van cryptovaluta's bij hacken 17,255 eenheden lager ligt dan de financiële schade van het gebruik van cryptovaluta's in phishing. De aanwezigheid van hacken verzwakt het effect van het gebruik van cryptovaluta's in phishing in 2019.

Op basis van de resultaten van de (lineaire) regressieanalyse in Tabel 5 zijn de voorspelde kansen berekend. Een gedetailleerd overzicht van de berekeningen is te vinden in Bijlage VIII. Zie Figuur 7 voor een visuele weergave van de voorspelde scores.



Figuur 7 **Voorspelde scores voor de gemiddelde financiële schade voor de verschillende vormen van cybercriminaliteit**

Figuur 7 biedt ondersteuning voor de hypothese dat het gebruik van cryptovaluta's aanzienlijk bijdraagt aan de gemiddelde financiële schade van cybercriminaliteit. Het gebruik van cryptovaluta's in hacken en ransomware veroorzaakt relatief weinig financiële schade. In 2019 is er zelfs helemaal geen financiële schade veroorzaakt door het gebruik van cryptovaluta's in hacken. Het is belangrijk op te merken dat het gebruik van cryptovaluta's in Ddos gemiddeld de grootste financiële schade met zich meebrengt. Bovendien neemt de gemiddelde financiële schade door het gebruik van cryptovaluta's in het algemeen jaarlijks toe voor alle vormen van cybercriminaliteit.

Daarentegen veroorzaakt het gebruik van cryptovaluta's in ransomware gemiddeld genomen geen grotere financiële schade gedurende de periode van 2019 tot en met 2022, in vergelijking met situaties waarin er geen cryptovaluta's zijn gebruikt.

In situaties waarin er geen cryptovaluta's zijn gebruikt brengen Ddos en ransomware gemiddeld ongeveer evenveel financiële schade met zich mee. Ook phishing veroorzaakt ongeveer dezelfde mate van financiële schade. Daarentegen veroorzaakt hacken gemiddeld weinig financiële schade.

4.4.2. Modelevaluatie

Bij de (lineaire) regressieanalyse is het belangrijk om de kwaliteit van de verschillende modellen te beoordelen. Een manier om dit te doen is door middel van de proportie verklaarde variantie (R^2). In Tabel 5 is te zien dat de R^2-waarde toeneemt per model, wat betekent dat het nieuwe model meer variantie verklaart dan het vorige model. Het is echter opmerkelijk dat de R^2-waarde bijna gelijk blijft voor Model 4 en -5. Dit suggereert dat Model 4 en 5 nauwelijks extra variantie verklaren ten opzichte van Model 3. In dit onderzoek wordt Model 4 en 5 daarom van lagere kwaliteit beschouwd in vergelijking met de andere modellen.

Ten tweede kan de kwaliteit van de modellen worden beoordeeld aan de hand van de *F*-veranderingstoets. Deze toets vergelijkt de verklaarde variantie tussen het nieuwe- en het oude model, waarbij de nulhypothese stelt dat er geen significante toename is in de proportie verklaarde variantie. Uit Tabel 5 blijkt dat elk model een significante F-veranderingsscore heeft, wat impliceert dat het model in staat is om de variantie in de afhankelijke variabele adequaat te verklaren op basis van onafhankelijke variabelen. Op basis hiervan kan geconcludeerd worden dat de modellen in de lineaire regressieanalyse voldoende van kwaliteit zijn.

Vervolgens is het belangrijk op te merken dat er voldaan wordt aan de assumptie van onafhankelijke waarnemingen en homoscedasticiteit. Echter, worden de assumpties van lineariteit en een normale verdeling van de standaardfouten geschonden. Daarnaast zijn er in totaal zes registraties verwijderd uit de dataset. Van deze registraties zijn vijf beoordeeld als uitbijter op basis van de residuen en één registratie is verwijderd vanwege een (te) extreme Cook's Distance. Tot slot is er geen sprake van multicollineariteit tussen de onafhankelijke variabelen.

Tabel 5

Resultaten (lineaire) regressieanalyse

	Model 1		Model 2		Model 3			Model 4		Model 5		Model 6		
	b (SE)	*p**	*b* (SE)	*p**	*b* (SE)	*p**	*VIF*	*b* (SE)	*p**	*b* (SE)	*p**	*b* (SE)	*p**	*VIF*
Constante	13,015 (,319)	,000	12,982 (,319)	,000	12,926 (,317)	<,000		12,896 (,317)	,000	12,959 (,318)	,000	6,701 (,488)	<,001	
Tijd in jaren	1,905 (,150)	<,001*	1,986 (,150)	<,001*	1,880 (,149)	<,001*	1,006	1,887 (,149)	<,001*	1,853 (,150)	<,001*	1,300 (,150)	<,001*	1,047
Hacken			-12,337 (1,264)	<,001*	-12,448 (1,256)	<,001*	1,001	-12,177 (1,268)	<,001*	-12,168 (1,268)	<,001*	-10,449 (1,250)	<,001*	1,027
Ddos			10,684 (2,964)	<,001*	6,881 (2,954)	,020*	1,009	5,607 (3,306)	,090	5,589 (3,306)	,091	7,126 (3,257)	,029*	1,267
Ransomware			4,318 (2,063)	,036*	1,963 (2,054)	,339	1,007	5,540 (2,201)	,012*	5,522 (2,201)	,012*	4,169 (2,168)	,054	1,159
Gebruik van cryptovaluta's					18,995 (1,221)	<,001*	1,014	20,268 (1,280)	<,001*	12,943 (3,582)	<,001*	13,329 (3,524)	<,001*	8,726
Gebruik van cryptovaluta's * Hacken								-13,492 (8,796)	,125	-14,480 (8,806)	,100	-17,255 (8,668)	,047*	1,046
Gebruik van cryptovaluta's * Ddos								4,920 (7,333)	,502	11,497 (7,924)	,147	10,152 (7,798)	,193	1,524
Gebruik van cryptovaluta's * Ransomware								-27,654 (6,111)	<,001*	-26,448 (6,135)	<,001*	-26,800 (6,038)	<,001*	1,218
Gebruik van cryptovaluta's * Tijd in jaren										3,203 (1,462)	,029*	3,490 (1,440	,015*	8,329
Geslacht												-2,381 (,290)	<,001*	1,012
Leeftijd												,169 (,008)	<,001*	1,041

R^2	,009		,016		,029		,030		,031		,061	
R-change	,009		,005		,014		,001		,000		,031	
F-change	161,025	<,001*	37,717	<,001*	241,825	<,001*	7,729	<,001*	4,729	,029*	283,241	<,001*
Df-change	1		3		1		3		1		2	
residual	17.396		17.393		17.392		17.389		17.388		17.386	

*significant bij p <,05 , N = 17.397, Afhankelijke variabele: financiële schade;

5. Discussie en conclusie

Het doel van dit onderzoek was om te achterhalen of er verschil zit in het gebruik van cryptovaluta's tussen de verschillende vormen van cybercriminaliteit en of de financiële schade van het gebruik ervan verschilt tussen de verschillende vormen van cybercriminaliteit. Verder diende het onderzoek om te achterhalen welke invloed de coronapandemie heeft gehad op het gebruik van cryptovaluta's in cybercriminaliteit. Gezien verschillen in het gebruik van cryptovaluta's tussen de verschillende vormen van cybercriminaliteit en de invloed van de coronapandemie hierop niet eerder is onderzocht, draagt het bij aan de wetenschappelijke literatuur. Gebaseerd op voorgaande literatuur werd er verwacht dat de coronapandemie het gebruik van cryptovaluta's in cybercriminaliteit heeft verhoogd en daarmee ook de financiële schade van het gebruik ervan. Verder werd verwacht dat er meer cybercriminaliteit werd gepleegd door mannen en jongeren en dat zij daarbij ook meer gebruik maakten van cryptovaluta's dan vrouwen. De onderzoeksvraag is beantwoord met gegevens afkomstig van politieregistraties.

5.1. Theoretische implicaties

Cryptovaluta's worden door cybercriminelen op twee manieren gebruikt: als middel voor de facilitering van cybercriminaliteit en als doelwit van cybercriminaliteit (Reddy & Minnaar, 2018). Tot op heden was het echter nog niet duidelijk in hoeverre het gebruik van cryptovaluta's verschilt tussen de verschillende vormen van cybercriminaliteit. Dit onderzoek werpt nieuw licht op deze kwestie en toont aan dat het gebruik van cryptovaluta's aanzienlijk groter is bij Ddos en ransomware in vergelijking met phishing en hacken.

Daarnaast werd op basis van de routine-activiteiten-theorie gesuggereerd dat het gebruik van cryptovaluta's zou toenemen als gevolg van de coronapandemie. De resultaten van dit onderzoek ondersteunen deze verwachting, omdat de kans op het gebruik van cryptovaluta's aanzienlijk groter is in 2021 en 2022 ten opzichte van 2019 en 2020. Het is mogelijk dat de effecten van de verandering in het gebruik van cryptovaluta's nog niet zichtbaar waren in 2020, omdat het enige tijd kan duren voordat deze effecten meetbaar worden.

Slachtoffers van cybercriminaliteit hebben gemeld dat zij financiële schade hebben geleden als gevolg van cybercriminaliteit (Akkermans et al., 2022). Het is echter niet bekend in hoeverre het gebruik van cryptovaluta's bijdraagt aan deze financiële schade. Dit onderzoek toont aan dat het gebruik van cryptovaluta's aanzienlijk bijdraagt aan de financiële schade van cybercriminaliteit.

Al met al bieden deze bevindingen een waardevolle aanvulling op de bestaande literatuur omtrent cybercriminaliteit, en dragen ze zij aan een beter begrip van de rol en impact van cryptovaluta's binnen dit domein.

5.2. Praktische implicaties

Dit onderzoek kan bijdragen aan de ontwikkeling van effectieve maatregelen of strategieën om het gebruik van cryptovaluta's in cybercriminaliteit te bestrijden. Door inzicht te krijgen de verschillen van het gebruik van cryptovaluta's tussen de verschillende vormen van cybercriminaliteit, kan de Nederlandse politie gerichte maatregelen treffen om deze uitingsvorm van cybercriminaliteit tegen te gaan.

Dit onderzoek draagt bij aan de vergroting van het bewustzijn en begrip van het gebruik van cryptovaluta's in cybercriminaliteit. Het heeft inzicht verschaft in de verschillen in het gebruik van cryptovaluta's tussen de verschillende vormen van cybercriminaliteit. Bovendien heeft het onderzoek aangetoond dat het gebruik van cryptovaluta's aanzienlijk bijdraagt aan de financiële schade. Deze bevindingen kunnen leiden tot een verhoogd bewustzijn van dat cryptovaluta's een belangrijke rol spelen in cybercriminaliteit.

5.3. Limitatie onderzoek en toekomstig onderzoek

In dit onderzoek is er gebruik gemaakt van politieregistraties. Deze registraties zijn gebaseerd op gevallen die daadwerkelijk gemeld worden bij de politie. Het gebruik maken van politieregistraties kan verschillende beperkingen opleveren bij het uitvoeren van het onderzoek. Allereerst is het mogelijk dat er sprake kan zijn van onderrapportage bij cybercriminaliteit. Slachtoffers van cybercrime doen namelijk minder snel aangifte dan slachtoffers van traditionele vormen van criminaliteit (Weijer & Leukfeldt, 2020). Dit kan voor onderrapportage zorgen waarbij het werkelijke aantal cybercriminaliteit hoger ligt dan wat bekend is bij de politie. In de criminologie wordt de criminaliteit dat niet bij de politie bekend is genoemd als 'dark number'.

Ten tweede is de vastlegging van cybercriminaliteit afhankelijk van de classificatie die door een politieanalist aan een specifiek delict wordt toegewezen. Ondanks de ontwikkeling van vaste protocollen om een correcte classificatie aan een delict toe te wijzen, kan het voorkomen dat de classificatie per analist kan verschillen. Dit kan leiden tot een vertekend beeld van de aard en omvang van cybercriminaliteit. Een vertekend beeld kan ontstaan doordat bepaalde vormen van cybercriminaliteit mogelijk verkeerd worden geclassificeerd of over het hoofd worden gezien, terwijl andere mogelijk worden uitvergroot of onjuist toegewezen. Dit kan de analyse van bepaalde trends van cybercriminaliteit belemmeren.

Tot slot richtte dit onderzoek op vier specifieke vormen van cybercriminaliteit : hacken, phishing, ddos en ransomware. Hierdoor werden andere vormen van cybercriminaliteit niet meegenomen in het onderzoek. Aangezien de focus beperkt was tot slechts deze vier vormen, geeft het onderzoek geen alomvattend beeld van het gebruik van cryptovaluta's in alle vormen van cybercriminaliteit.

Het gebruik maken van politieregistraties biedt echter ook aanzienlijke voordelen. Politieregistraties leveren waardevolle inzichten op met betrekking tot het gebruik van cryptovaluta's in cybercriminaliteit. Dit onderzoek maakte gebruik van landelijke politieregistraties waardoor er inzicht is verkregen in het gebruik van cryptovaluta's in cybercriminaliteit voor de gehele populatie.

Politieregistraties worden opgesteld volgens gestandaardiseerde protocollen, waardoor de gegevens vaak goed gestructureerd worden vastgelegd. Ondanks enige mogelijkheid tot selectiviteit bij de analyse, is het mogelijk om de gegevens te analyseren en te vergelijken. Het gebruik van politiegegevens heeft het in dit onderzoek mogelijk gemaakt om het gebruik van cryptovaluta's in cybercriminaliteit gedurende de verschillende jaren te onderzoeken.

In dit onderzoek werd specifiek gekeken naar het gebruik van cryptovaluta's in hacken, phishing, Ddos en ransomware. Om een volledig inzicht te krijgen in de totale impact van het gebruik van cryptovaluta's en om te bepalen of de financiële schade verschilt tussen de verschillende vormen van cybercriminaliteit, is het belangrijk om in een vervolgonderzoek alle andere vormen van cybercriminaliteit mee te nemen. Voorbeelden hiervan zijn identiteitsfraude, malware of defacing. Door alle vormen van cybercriminaliteit te onderzoeken in een vervolgonderzoek, kan er een alomvattend beeld worden verkregen van het gebruik van cryptovaluta's in cybercriminaliteit

Verder kan een vervolgonderzoek zicht richten op de specifieke factoren die verantwoordelijk zijn voor de verschillen in het gebruik van cryptovaluta's tussen de verschillende vormen van cybercriminaliteit. Het is belangrijk om te begrijpen hoe en waarom deze verschillen zijn ontstaan, omdat dit inzicht kan bieden in de aard en dynamiek van cybercriminaliteit.

5.4. Conclusie

5.4.1. Het gebruik van cryptovaluta's

In dit onderzoek stond de volgende onderzoeksvraag centraal: "Welke invloed heeft de coronapandemie op het gebruik van cryptovaluta's in cybercriminaliteit en hoe verschilt de financiële schade van het gebruik van cryptovaluta's tussen de vormen van cybercriminaliteit?" Op basis van de routine-activiteiten-theorie werd gesuggereerd dat de coronapandemie het gebruik van cryptovaluta's in cybercriminaliteit heeft verhoogd (Cohen & Felson, 1979). Daarnaast werd verwacht dat het gebruik van cryptovaluta's de financiële schade van cybercriminaliteit zou verhogen. Om de onderzoeksvraag te beantwoorden werden registraties van slachtoffers en verdachten uit politieregistraties gebruikt.

De resultaten laten zien dat in 2021 en 2022 de kans op het gebruik van cryptovaluta's significant hoger was dan in 2019 en 2020. De coronapandemie begon in 2020 en eindigde in 2022, waarbij de zwaarste maatregelen werden getroffen in 2021. Het is mogelijk dat de effecten van de verandering in het gebruik van cryptovaluta's nog niet zichtbaar waren in 2020, omdat het enige tijd kan duren voordat deze effecten meetbaar worden. Gezien de aanzienlijke toename van het gebruik van cryptovaluta's in cybercriminaliteit in 2021 en 2022 ten opzichte van 2019 en 2020, kan worden geconcludeerd dat er ondersteuning is gevonden voor de verwachting dat het gebruik van cryptovaluta's in cybercriminaliteit tijdens de coronapandemie is toegenomen.

Bovendien blijkt dat de kans op het gebruik van cryptovaluta's in cybercriminaliteit verschilt tussen de verschillende vormen van cybercriminaliteit. De kans op het gebruik van cryptovaluta's is lager bij hacken in vergelijking met phishing, terwijl de kans hoger is bij Ddos en ransomware. Het is belangrijk op te merken dat in de periode van 2021 en 2022 de kans op het gebruik van cryptovaluta's sterk verminderd wordt wanneer Ddos of ransomware aanwezig is. Een mogelijke verklaring voor dit resultaat is dat bij phishing, in tegenstelling tot Ddos en ransomware, er vaak geen gebruik wordt gemaakt van cryptovaluta's als betaalmiddel. Een bekend voorbeeld hiervan is vriend-in-nood phishing via Whatsapp, waarbij het slachtoffer vaak zelf geld overboekt naar de persoon die zogenaamd in 'nood' verkeert. (Cybercrimeinfo, z.d.) Daarnaast is er bij hacken niet altijd sprake van een financieel motief. Hoewel dit vaak wel het geval is, kan het bijvoorbeeld ook voorkomen dat een netwerk wordt gehackt door een groep die het niet eens is met het beleid van een bepaalde organisatie (Scheffel, 2022).

Ten slotte is de kans op betrokkenheid bij cybercriminaliteit waarbij cryptovaluta's zijn gebruik aanzienlijk groter voor mannen dan voor vrouwen. Daarnaast hebben jongeren een grotere kans dan ouderen om betrokken te raken bij cybercriminaliteit waarbij cryptovaluta's zijn gebruikt.

5.4.2. Financiële schade

Het gebruik van cryptovaluta's in cybercriminaliteit leidt tot een aanzienlijke toename van de financiële schade. Bovendien neemt de gemiddelde financiële schade door het gebruik van cryptovaluta's voor alle vier de vormen van cybercriminaliteit jaarlijks toe. Op basis van deze resultaten kan er worden geconcludeerd dat er ondersteuning is gevonden voor de verwachting dat het gebruik van cryptovaluta's de financiële schade voor de samenleving verhoogt. Het is belangrijk op te merken dat het gebruik van cryptovaluta's in Ddos gemiddeld de meeste financiële schade met zich meebrengt. Bovendien blijkt dat het effect van het gebruik van cryptovaluta's op de financiële schade wordt verzwakt door de aanwezigheid van hacken of ransomware. Aan de andere kant wordt het effect van 'tijd in jaren' op de financiële schade versterkt door het gebruik van cryptovaluta's.

Daarnaast zijn er conclusies getrokken met betrekking tot de algemene financiële schade als gevolg van cybercriminaliteit. Uit de onderzoeksresultaten blijkt dat de financiële schade jaarlijks is toegenomen in de periode 2019 tot en met 2022. Bovendien varieert de financiële schade afhankelijk van de vorm van cybercriminaliteit. Hacken veroorzaakt over het algemeen minder financiële schade in vergelijking met phishing, terwijl Ddos en ransomware een hogere financiële schade met zich meebrengen.

5.5. Aanbevelingen

Uit het onderzoek is gebleken dat de kans op het gebruik van cryptovaluta's aanzienlijk groter is in Ddos en ransomware vergeleken met de andere vormen van cybercriminaliteit. Deze bevinding hebben belangrijke implicaties voor de aanpak van cybercriminaliteit. Daarom wordt er aanbevolen om speciale aandacht te besteden aan de preventie en bestrijding van cybercriminaliteit waarbij cryptovaluta's worden gebruikt, met nadruk op Ddos en ransomware.

Allereerst wordt er aanbevolen om binnen de politieorganisatie de bewustwording rondom het gebruik van cryptovaluta's te vergroten. Uit het onderzoek is namelijk gebleken dat cryptovaluta's zijn gebruikt in 22,30% van de Ddos-registraties 13,49% van de ransomware registraties. Daarom wordt het aanbevolen om trainingen en voorlichtingscampagnes te organiseren om binnen de politieorganisatie een beter begrip van de risico's van het gebruik van cryptovaluta's te bevorderen.

Ten tweede wordt er aangeraden om nauw samen te werken met wisselkantoren van cryptovaluta's. In het onderzoek kwam namelijk naar voren dat de financiële schade van cybercriminaliteit aanzienlijk wordt verhoogd door het gebruik van cryptovaluta's. Een goede samenwerking met wisselkantoren van cryptovaluta's zorgt ervoor om illegaal verkregen verdiensten te traceren en in beslag te nemen. Het in beslag nemen van deze illegaal verkregen verdiensten kan de financiële schade verminderen.

Tot slot wordt het aanbevolen om verder onderzoek te verrichten naar het gebruik van cryptovaluta’s in Ddos en ransomware. Dit kan leiden tot nieuwe inzichten in de variatie van het gebruik van cryptovaluta’s tussen de verschillende vormen van cybercriminaliteit. De resultaten van dit vervolgonderzoek zullen bijdragen aan een beter begrip van het gebruik van cryptovaluta’s in cybercriminaliteit.

Referenties

AFM. (2021). *Attitudes van cryptobezitters*. AFM. Geraadpleegd op 8 april 2023, van www.afm.nl

Akkermans, M., Kloosterman, R., Moons, E., Reep, C., & Van der Aa, M. T. (2022, 28 februari). *4. Traditionele criminaliteit*. Centraal Bureau voor de Statistiek. https://www.cbs.nl/nl-nl/longread/rapportages/2022/veiligheidsmonitor-2021/4-traditionele-criminaliteit#:~:text=Het%20gaat%20hier%20om%20criminaliteit,inbraak%20en%20diefstal%2C%20en%20vernieling.

Aljumily, R. (2017b). Quantitative Criminology: Bayesian Statistics for Measuring the "Dark Figure" of Crime. *Social Science Research Network*. https://doi.org/10.2139/ssrn.2999280

Bele, J. L. (2021). Cryptocurrencies as facilitators of cybercrime. *SHS web of conferences*, *111*, 01005. https://doi.org/10.1051/shsconf/202111101005

Boekhoorn, P. (2019, oktober). *De aanpak van cybercrime door regionale eenheden van de politie - van intake van cybercrime naar opsporing en vervolging*. BBSO. Geraadpleegd op 20 mei 2023, van https://zoek.officielebekendmakingen.nl/blg-924272.pdf

Borwell, J., Schuppers, K., Rooyakkers, J., & Harteveld, A. (2020). Het cybercrimebeeld van de Nederlandse politie: Van algemeen beeld naar verdiepende analyse en aanpak. *Cahiers Politiestudies*, *3*(56), 39-62.

Botha, J. G., Botha, D., & Leenen, L. (2023). An Analysis of Crypto Scams during the Covid-19 Pandemic: 2020-2022. *Proceedings of the . . . international conference on information warfare and security*, *18*(1), 36–48. https://doi.org/10.34190/iccws.18.1.1087

Centraal Bureau voor de Statistiek. (2020, maart 23). Meer jongeren digitaal vaardig. *Centraal Bureau voor de Statistiek*. https://www.cbs.nl/nl-nl/nieuws/2020/13/meer-jongeren-digitaal-vaardig

Centraal Bureau voor de Statistiek. (2020a, 18 december). *Hoe zit het met cybercrime? - Nederland in cijfers 2020*. Hoe zit het met cybercrime? - Nederland in cijfers 2020 | CBS. https://longreads.cbs.nl/nederland-in-cijfers-2020/hoe-zit-het-met-cybercrime

Centraal Bureau voor de Statistiek. (2021, 28 februari). Scherpe daling traditionele vormen van criminaliteit. *Centraal Bureau voor de Statistiek*. https://www.cbs.nl/nl-nl/nieuws/2021/09/scherpe-daling-traditionele-vormen-van-criminaliteit

Centraal Bureau voor de Statistiek. (2022b, februari 28). *Veiligheidsmonitor 2021*. Geraadpleegd op 22 mei 2023, van https://www.cbs.nl/nl-nl/publicatie/2022/09/veiligheidsmonitor-2021

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review, 44(4), 588–608. https://doi.org/10.2307/2094589

CyberCrimelnfo. (2022, 12 januari). *Cryptogeld gelinkt aan criminelen bereikte een record bedrag van 12,3 miljard euro in 2021*. Geraadpleegd op 15 mei 2023, van https://www.ccinfo.nl/cybercrime/crypto-crime/nieuws-crypto-crime/815184_cryptogeld-gelinkt-aan-criminelen-bereikte-een-record-bedrag-van-12-3-miljard-euro-in-2021

CyberCrimelnfo. (18 januari,2023). *Cybercrime verdrievoudigd sinds 2019 blijkt uit de misdaadcijfers van 2022*. CyberCrimelnfo.nl | De Bibliotheek Van Cybercrime En Darkweb. Geraadpleegd op 15 mei 2023, van https://www.ccinfo.nl/cybercrime/1161094_cybercrime-verdrievoudigd-sinds-2019-blijkt-uit-de-misdaadcijfers-van-2022

CyberCrimelnfo. (z.d.). *Vriend-in-nood-fraude (VIN fraude) | Cybercrimeinfo.nl*. CyberCrimelnfo| De bibliotheek van Cybercrime en Darkweb. Geraadpleegd op 7 juli 2023, van https://www.ccinfo.nl/cybercrime/vriend-in-nood-fraude-vin-fraude#:~:text=Bij%20vriend%2Din%2Dnoodfraude%20krijgt,slinkse%20wijze%20geld%20wil%20aftroggelen.

Dijkstra, J. K., & Veenstra, R. (2019). Jongeren, leeftijdsgenoten en criminaliteit. *Tijdschrift voor criminologie*, *61*(3), 280–292. https://doi.org/10.5553/tvc/0165182x2019061003005

DRIO. (2021). *Jaarbeeld cybercrime 2021*. Agora. Geraadpleegd op 11 mei 2023, van https://www.agora.nl

Europol. (2020). *Beyond the pandemic - How COVID-19 will shape the serious and organised crime landscape in the EU*. Geraadpleegd op 18 april 2023, van https://www.europol.europa.eu/publications-events/publications/beyond-pandemic-how-covid-19-will-shape-serious-and-organised-crime-landscape-in-eu

Gibson, C. L., Ward, J. T., Wright, J. P., Beaver, K. M., & Delisi, M. (2010). Where Does Gender Fit in the Measurement of Self-Control? *Criminal Justice and Behavior, 37*(8), 883–903. https://doi.org/10.1177/0093854810369082

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime.* Stanford, CA: Stanford University Press.

Junger, M., Terlouw, G., Van Der Heijden, P., & Rutenfrans, C. (1995). Zelfcontrole, ongevallen en criminaliteit. *Tijdschrift Voor Criminologie*, *37*, 2–21. http://dspace.library.uu.nl/handle/1874/19869

Kenthineni, S., & Cao, Y. (2020). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. *International Criminal Justice Review*, *30*(3), 325–344. https://doi.org/10.1177/1057567719827051

Kruisbergen, E. W., Leukfeldt, R., Kleemans, E. R., Roks, R., Kouwenberg, R., Nabi, S., Fiorito, T. L., & Van Ruitenburg, T. (2018). Georganiseerde criminaliteit en ICT. *Den Haag*. https://repository.tudelft.nl/assets/uuid:576d2a7f-a31d-4019-89b0-07db2d3415a5/Cahier_2018-8_2437_Samenvatting_tcm28-328674.pdf

Kruisbergen, E. W., Haas, M., Van Es, L., & Snijders, J. (2021). De pandemie als criminologisch experiment. *Justitiële verkenningen*, *47*(3), 9–34. https://doi.org/10.5553/jv/016758502021047003002

Leukfeldt, R., Notté, R., & Malsch, M. (2018). *Slachtofferschap van online criminaliteit: Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van*

cybercrime en gedigitaliseerde criminaliteit. WODC. Geraadpleegd op 5 april 2023, van https://repository.wodc.nl/bitstream/handle/20.500.12832/2355/2839_Volledige_Tekst_tcm28-368216.pdf?sequence=1&isAllowed=y

Masschelein, J. (2019). *Cybercriminaliteit als een dienst: Een onderzoek naar de aankoop en verkoop van cybercriminele diensten*. Universiteit Gent. Geraadpleegd op 11 mei 2023, van https://libstore.ugent.be/fulltxt/RUG01/002/790/126/RUG01-002790126_2019_0001_AC.pdf

Matthijsse, S., Van Der Wagen, W., Van 't Zand, E., & Fischer, T. (2021). Een kijkje achter de schermen: een kwalitatieve studie over het ontstaan van cybercriminele carrières. *Tijdschrift voor criminologie*, *63*(1), 30–49. https://doi.org/10.5553/tvc/0165182x2021063001002

Moffitt, T. E. (2018). Male antisocial behaviour in adolescence and beyond. *Nature Human Behaviour*, *2*(3), 177–186. https://doi.org/10.1038/s41562-018-0309-4

Moors, H., De Veen, L., & Van De Wijngaert, L. (2022). *Criminaliteit en veiligheid in Almere: ontwikkelingen, perspectieven en opgaven, 2010-2030*.

Odinot, G., De Poot, C. J., & Verhoeven, M. (2018). De aard en aanpak van georganiseerde cybercrime. *WODC*, 11. https://doi.org/10.5553/jv/016758502018044005002

Politie. (2020, 30 oktober). *Rapport Cryptovaluta*. Geraadpleegd op 3 april 2023, van https://agora.portal.politie.local

Politie. (2020a, april). *Nu ook online aangifte van cybercrime*. politie.nl. Geraadpleegd op 22 mei 2023, van https://www.politie.nl/nieuws/2020/februari/4/nu-ook-online-aangifte-van-cybercrime.html

Politie. (2022, augustus 29). *Cryptovaluta*. Agora. Geraadpleegd op 5 april 2023, van https://Agora.portal.politie.local

Politie. (z.d.-b). *Wat moet ik meenemen bij een aangifte en wat gebeurt daarmee?* politie.nl. Geraadpleegd op 20 mei 2023, van https://www.politie.nl/informatie/wat-moet-ik-meenemen-bij-een-aangifte-en-wat-gebeurt-daarmee.html#:~:text=Als%20je%20aangifte%20doet%2C%20verzoek,doet%20de%20politie%20verder%20onderzoek.

Politie. (z.d-a.). *Politiecijfers in CBS-overzicht*. politie.nl. Geraadpleegd op 20 mei 2023, van https://www.politie.nl/informatie/politiecijfers-in-cbs-overzicht.html

Reddy, E., & Minnaar, A. (2018). Cryptocurrency: a tool and target for cybercrime. *African Journal of Criminology & Victimology*, *31*(3).

Rutenfrans, C. (1989). *Criminaliteit en sexe: een verklaring voor de verschillen in het criminele gedrag van vrouwen en mannen*. Geraadpleegd op 11 mei 2023, van https://repository.ubn.ru.nl/handle/2066/113679

Scheffel, M. (2022b, september 27). *Wie zijn die hackers, waarom doen ze het en wat doe je ertegen?* Avantage. Geraadpleegd op 7 juli 2023, van https://www.avantage.nl/blog/hackers-wie-waarom/

Schrama, V., Van de Laarschot, J., Volten, C., & Van Wegberg, R. (2022, 10 november). *Virtuele valuta: Handelingsperspectieven voor data-gedreven opsporing*. Wetenschappelijk Onderzoek- en Documentatiecentrum. Geraadpleegd op 8 april 2023, van https://repository.wodc.nl/handle/20.500.12832/3215

Valgaeren, E., & Linnemann, J. J. (2017, december). *Blockchain ontketend*. Geraadpleegd op 22 april 2023, van https://kvdl.com/uploads/documents/Valgaeren-Linnemann.pdf

Van Den Berg, E. (2022, februari 21). 'Cybercriminelen winnen slag met politie door gebruik van Tron.' *bnr.nl*. https://www.bnr.nl/nieuws/technologie/10468014/cybercriminelen-winnen-slag-met-politie-door-gebruik-van-tron

Van Huijstee, M., Nieuwenhuizen, W., Masson, E., Sanders, M., & Van Boheemen, P. (2021). Online ontspoord : Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland. *Rathenau Instituut*. https://www.rathenau.nl/sites/default/files/2021-07/Rathenau_Instituut_Rapport_Online_ontspoord.pdf

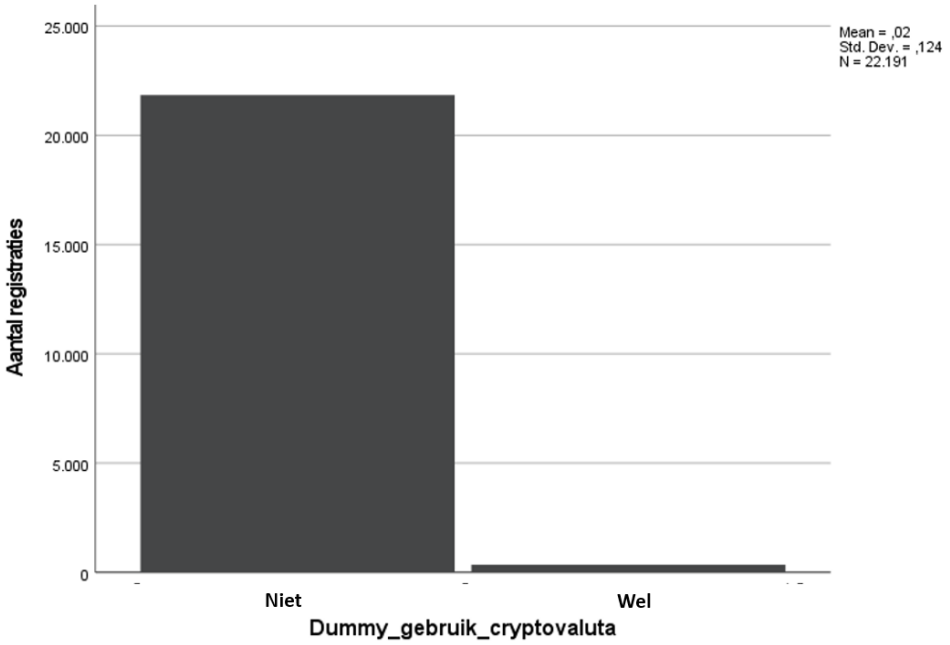
Weijer, S. G. A., Leukfeldt, E. R., & Van Der Zee, S. (2020). *Slachtoffer van online criminaliteit, wat nu?: een onderzoek naar de aangiftebereidheid onder burgers en ondernemers*. SDU uitgevers. https://surfsharekit.nl/public/314d6dd6-00c3-416f-81ae-3f3fbb6e0346

Bijlage I – Beschrijving variabelen

In deze paragraaf zullen allereerst de variabelen die zijn opgenomen in de logistische regressieanalyse worden beschreven. Vervolgens zal de variabele financiële schade, die extra wordt toegevoegd in de (lineaire) regressieanalyse worden beschreven.

Gebruik van cryptovaluta's

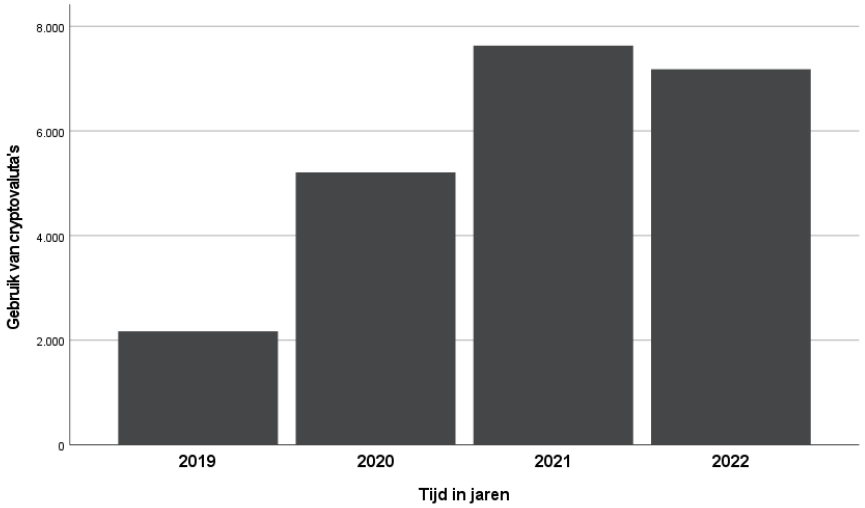
Het gebruik van cryptovaluta's is categorisch van aard waarbij 'Geen gebruik gemaakt van cryptovaluta's' wordt weergegeven aan de hand van de linker staaf in het histogram. Het 'wel gebruik van cryptovaluta's' wordt dus weergegeven in de rechterstaaf van het histogram. In het histogram is te zien dat bij het grootste gedeelte van de registraties van cybercriminaliteit geen cryptovaluta's worden gebruikt. Er zijn 21.844 registraties van cybercriminaliteit waarbij geen cryptovaluta's zijn gebruikt. Dit komt neer op 98,44% van de registraties. Er zijn 347 registraties van cybercriminaliteit waarbij cryptovaluta's zijn gebruikt. Dit komt neer op 1,56% van de registraties van cybercriminaliteit.



Figuur 8 Gebruik cryptovaluta's in cybercriminaliteit in de periode van 2019 tot 2022

Tijd in jaren

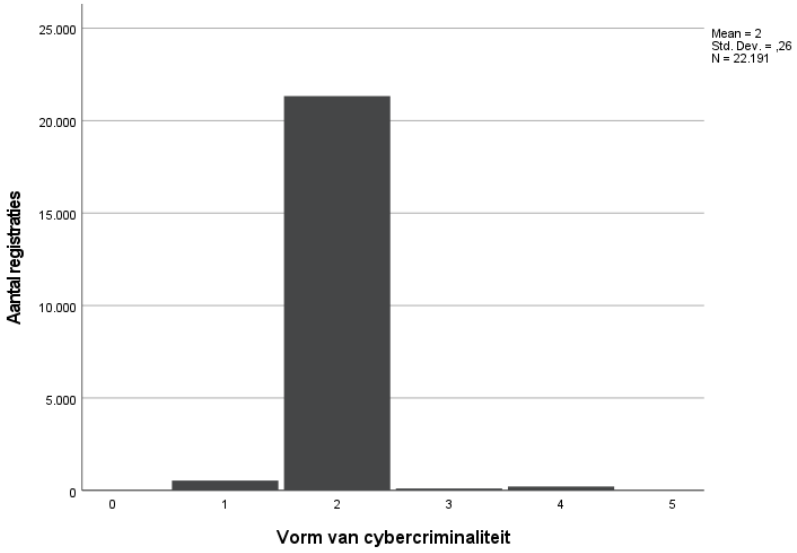
De onafhankelijke variabele – tijd in jaren – is onderverdeeld in de categorieën 2019, 2020, 2021 en 2022. In Figuur 9 is te zien dat de meeste cybercriminaliteit plaatsvond van 2020 tot en met 2022. Hierbij zijn er 3892 registraties van cybercriminaliteit bekend in 2020. In 2021 ligt het aantal op 5991 registraties en in 2022 gaat het om 5542 registraties.



Figuur 9 **Het gebruik van cryptovaluta's weergegeven voor de jaren 2019 tot en met 2022**

Vorm van cybercriminaliteit

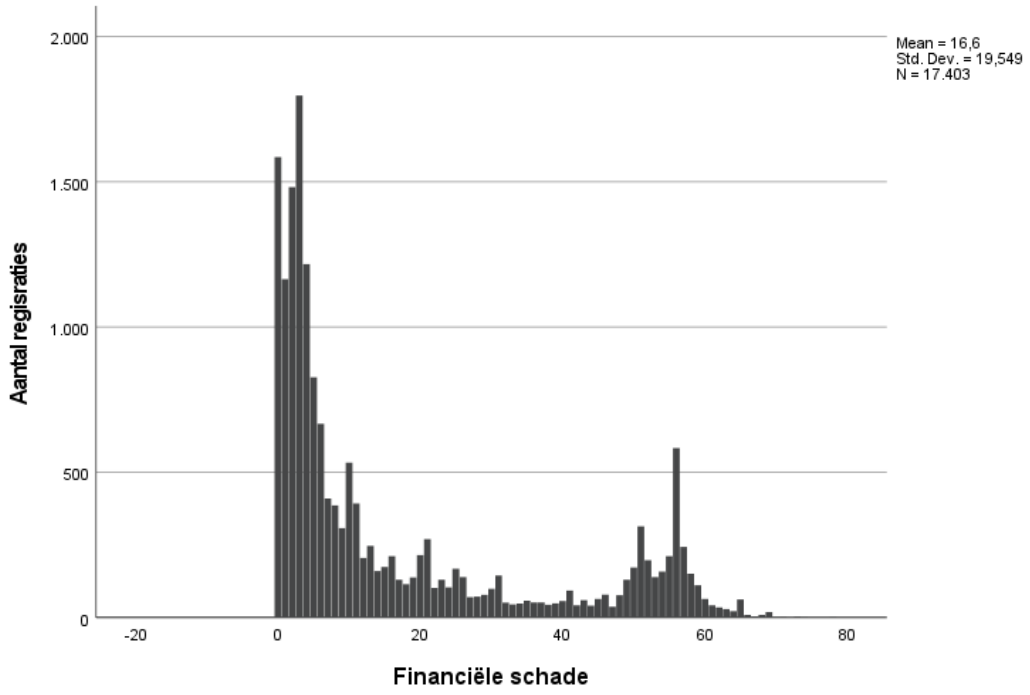
De vorm van cybercriminaliteit bestaat uit vier categorieën: hacken, phishing, ddos en ransomware. In Figuur 10 is te zien dat het grootste gedeelte van alle registraties van cybercriminaliteit vallen onder phishing. Van de in totaal 22.116 registraties van cybercriminaliteit vallen er 21.273 onder phishing, 531 onder hacken, 108 onder ddos en 215 onder ransomware.



Figuur 10 **Het gebruik van cryptovaluta's weergegeven voor hacken, phishing, Ddos en ransomware**

Financiële schade

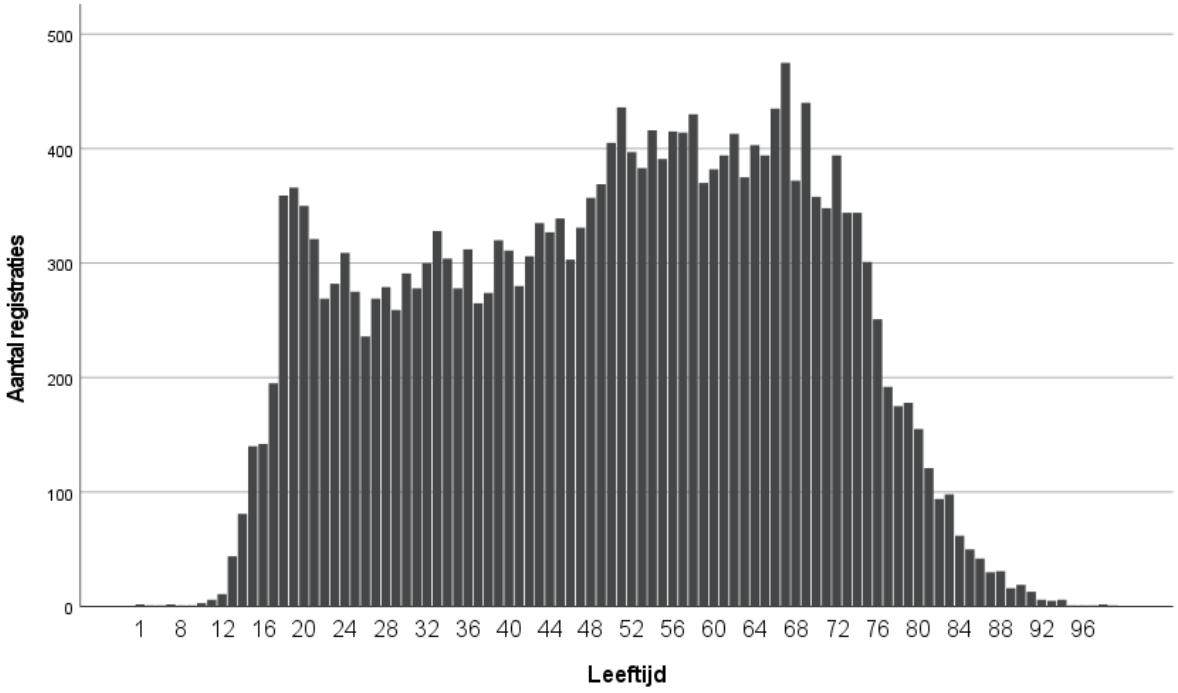
In Figuur 11 wordt de verdeling van de continue variabele financiële schade weergegeven, die als afhankelijke variabele dient in de (lineaire) regressieanalyse. De hoogste financiële schade bedraagt 5,7 miljoen euro, terwijl de minimale financiële schade 0 euro is. De gemiddelde financiële schade is 16.6, wat betekent dat deze zich bevindt op schaal 16. Dit komt overeen met een gemiddelde financiële schade tussen 1600 en 1699,99 euro.



Figuur 11 Financiële schade weergegeven in intervallen voor de registraties van cybercriminaliteit

Leeftijd

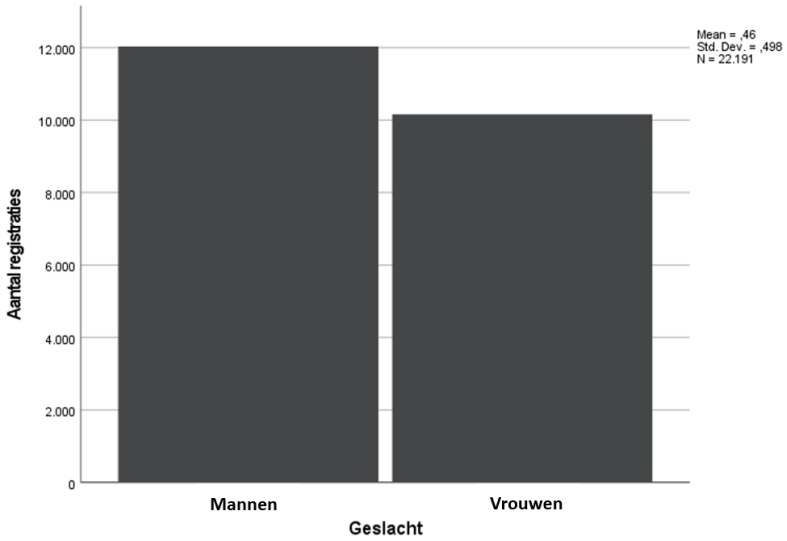
In Figuur 12 wordt de verdeling van de continue variabele leeftijd weergegeven. Hierin is te zien dat leeftijd redelijk normaal verdeeld is. In de dataset is de jongste leeftijd 8 jaar en de oudste 95-. Vanwege extreme waarden zijn twaalf registraties verwijderd. Deze registraties betroffen de leeftijden 1, 3, 6, 7, 96, 97, 98 en 102 jaar. Het eerste kwartiel ligt op 34 jaar en het derde kwartiel op 65 jaar. Dit betekent dat 50 procent van alle registraties zich bevind tussen 34 en 65 jaar.



Figuur 12 De verdeling van leeftijd voor de registraties van slachtoffers en verdachten

Geslacht

De variabele geslacht bestaat uit de categorieën man en vrouw en is nominaal van aard. In Figuur 13 wordt de verdeling van het geslacht voor de registraties van cybercriminaliteit weergegeven. Hierin is te zien dat van de in totaal 22.127 registraties van cybercriminaliteit, 12,015 betrekking hebben op mannen. Dit komt neer op 54,3%. De overige 10.112 registraties hebben betrekking op vrouwen wat neerkomt op 45,7%.



Figuur 13 De verdeling van geslacht voor de registraties van cybercriminaliteit

Bijlage II – Bewerking variabelen

Databewerking Excel

In deze paragraaf wordt er besproken welke coderingen zijn verricht per variabele. Deze coderingen zijn uitgevoerd om de data geschikt te krijgen voor analyses in SPSS.

Het gebruik van cryptovaluta's

In het databestand komt het gebruik van cryptovaluta's terug in de kolom 'kenmerk'. Wanneer er in de registratie gebruik is gemaakt van cryptovaluta's wordt dit aangegeven met de term 'cryptocurrency'. Als er geen gebruik is gemaakt van cryptovaluta's of als het niet bekend is wordt de term 'NA' gehanteerd. Het gebruik van cryptovaluta's is in dit onderzoek de afhankelijke variabele en is dichotoom van aard. Dit houdt in dat de variabele slechts uit twee categorieën bestaat; 0 = geen gebruik gemaakt van cryptovaluta's, 1 = wel gebruik gemaakt van cryptovaluta's. In Excel is een aparte kolom aangemaakt waarin de volgende codering is gebruikt:

=ALS(I11="NA";0;ALS(I11="Cryptocurrency";1;""))

Hierbij verwijst I11 naar de cel waarin is aangegeven of er wel of geen gebruik is gemaakt van cryptovaluta's.

Tijd in jaren

In het databestand wordt het jaar wanneer het delict is gepleegd aangegeven in de kolom 'registratie'. In de registraties geven de eerste vier letters van de laatste cijferreeks het jaar aan wanneer het delict heeft plaatsgevonden. Een voorbeeld van zo'n registratie is PL0100_BVH_201908597. In dit geval heeft het delict plaatsgevonden in 2019. Alle informatie, behalve de laatste cijferreeks, werd verwijderd. Vervolgens is in Excel een aparte kolom aangemaakt waarin werd aangegeven of het om het jaar 2019, 2020, 2021 of 2022 ging. Dit is gedaan door middel van de volgende codering:

=LINKS(A31;4)

Deze codering zorgt ervoor dat alleen de vier linker letters werden weergegeven in de kolom. Hierbij verwijst A31 naar de cel waarin de cijferreeks stond weergegeven. Nu alleen de jaartallen in een kolom staan weergegeven werd de volgende codering toegepast:

=ALS(B31="2019";0;ALS(B31="2020";1;ALS(B31="2021";2;ALS(B31="2022";3;""))))

In de nieuwe kolom werd aan de hand van één cijfer aangegeven in welk jaartal het delict had plaatsgevonden. Hierbij werd de volgende codering gebruikt: 0 = 2019, 1 = 2020, 2 = 2021 en 3 = 2022.

Vorm van cybercriminaliteit

In het databestand wordt aangegeven onder welk soort cybercriminaliteit de registratie valt. De vorm van cybercriminaliteit komt in het databestand terug als 'subcategorie'. Hierbij bestond er al een bestaande subcategorie voor hacken, ransomware en ddos. Dit was echter niet het geval voor phishing. Het databestand bevatte tevens een kolom waarin stond aangegeven of er wel of geen sprake was van phishing. Om het aantal phishingregistraties te achterhalen werden alleen de registraties waarbij er sprake was van phishing geselecteerd. Van de registraties die over bleven zijn de registraties met de subcategorie hacken, ransomware en ddos afgehaald. De overgebleven registraties kregen de subcategorie 'phishing' toegewezen.

In het databestand is een nieuwe variabele aangemaakt waarin de vorm van cybercriminaliteit werd aangegeven door middel van een cijfer. De werd de volgende codering gebruikt: 1 = hacken, 2 = phishing, 3 = ddos en 4 = ransomware. Om deze kolom aan te maken is de volgende formule toegepast:

=ALS(E3531="hacktivisme";1;ALS(E3531="hacken onbekend motief";1;ALS(E3531="phishing";2;ALS(E3531="ddos";3;ALS(E3531="ransomware";4;"")))))

Hierbij verwees E3531 naar de cel waarin de vorm van cybercriminaliteit werd weergegeven. Zie Figuur 11 ter ondersteuning.

Financiële schade

Het databestand wordt, wanneer bekend, het geleden schadebedrag per registratie aangegeven. Het schadebedrag wordt in dit onderzoek beschreven als financiële schade. Voor deze variabele zijn verschillende intervallen gebruikt. Zie de databewerking van SPSS voor een volledige beschrijving.

Geslacht

Het databestand bevatte een kolom waarin het geslacht van de betrokkene werd aangegeven. De betrokkene uit zich in de vorm van de verdachte of dader. Deze variabele is gehercodeerd naar een dummyvariabele waarbij de volgende codering is toegepast: 0 = man en 1 = vrouw.

In het databestand is een nieuwe variabele aangemaakt waarin het geslacht wordt vermeldt aan de hand van bovenstaande codering. Om de variabele aan te maken is de volgende codering toegepast:

=ALS(P3531="man";0;ALS(P3531="vrouw";1;""))

Hierbij verweest P3531 naar de cel waarin het geslacht in de vorm van 'man' en 'vrouw' werd aangegeven. Zie Figuur 14 ter ondersteuning.

Leeftijd

In de dataset was geen variabele aanwezig die informatie gaf over de leeftijd van de betrokkene tijdens het delict. De dataset bevatte echter wel informatie over de geboortedatum van de betrokkene en de begindatum van het delict. De leeftijd van de betrokkene tijdens het delict kon berekend worden door de geboortedatum van de begindatum af te halen. In de dataset is een variabele aangemaakt waarin de leeftijd van de betrokkene werd aangegeven. De variabele is aangemaakt door middel van de volgende formule:

=JAAR(L3531)-JAAR(O3531)-
(ALS(OF(MAAND(L3531)<MAAND(O3531);EN(MAAND(L3531)=MAAND(O3531);DAG(L3531
)<DAG(O3531)));1;0))

Hierbij verwijst L3531 naar de begindatum van het delict en O3531 naar de geboortedatum van de betrokkene. In deze variabele werd de leeftijd in hele getallen weergegeven. Om de resultaten van het onderzoek beter te kunnen interpreteren, is er voor gekozen om leeftijd te verdelen in categorieën. Hierbij werden de volgende coderingen gebruikt: 0 = 0 – 17 jaar, 1 = 18 – 24 jaar, 2 = 25 – 34 jaar, 3 = 35 – 44 jaar, 4 = 45 – 55 jaar en 5 = 55+. In de dataset is een nieuwe variabele aangemaakt waarin staat aangegeven tot welke leeftijdscategorie de registratie behoort. Om de nieuwe variabele aan te maken is de volgende formule gebruikt:

=ALS(R3531>=1;ALS(R3531<=17;0;ALS(R3531<=24;1;ALS(R3531<=34;2;ALS(R3531<=44;3;AL
S(R3531<=54;4;5)))));"")

Hierbij verwijst R3531 naar de cel waarin de leeftijd van de betrokkene staat aangegeven in hele getallen.

De uiteindelijke dataset wordt weergegeven in Figuur 15. Deze dataset is geëxporteerd naar SPSS. Vervolgens zijn, met uitzondering de variabele het gebruik van cryptovaluta's, alle variabelen die geen informatie bevatte in de vorm van cijfers verwijderd uit SPSS.

registratie	soort	hoofdcategorie	subcategorie	hack	phishing	toelichting	benadeelde	schade	schade_vergoed	schade_be	cat_doelwit	cat_expertise
PL0100 BVH 2019108597	Cybercrime	Fraude / Oplichting	Vriend-in-noodfraude	Ja	Nee	Slt krijgt WhatsApp bericht va	Particulier	2000	Onbekend	NA	Burger	NA
PL0100 BVH 2019108597	Cybercrime	Fraude / Oplichting	Vriend-in-noodfraude	Ja	Nee	Slt krijgt WhatsApp bericht va	Particulier	2000	Onbekend	NA	Burger	NA
PL0100 BVH 2019075092	Cybercrime	Overige Cybercrime	Malware onbekend motief	Nee	Nee	E-mail gekregen dat computer	Particulier	NA	NA	NA	Burger	NA
PL0100 BVH 2019076566	Gedigitaliseerde criminaliteit	Fraude / Oplichting	Creditcardfraude	Onbekend	Ja	Slt kreeg mail met link. Drukt	Particulier	NA	NA	NA	Burger	NA
PL0100 BVH 2019090714	Cybercrime	Fraude / Oplichting	Helpdeskfraude (Tech Support Scam)	Ja	Ja	SLT onving eerst 2 mails over	Particulier	398.43	Nee	NA	Burger	NA
PL0100 BVH 2019090714	Cybercrime	Fraude / Oplichting	Helpdeskfraude (Tech Support Scam)	Ja	Ja	SLT onving eerst 2 mails over	Particulier	398.43	Nee	NA	Burger	NA
PL0100 BVH 2019223545	Cybercrime	Fraude / Oplichting	Misbruik accounts voor bestellingen	Ja	Onbekend	Account Wehkamp en BonPri	Particulier	504.45	Onbekend	Bonprix	Burger	NA
PL0100 BVH 2019223545	Cybercrime	Fraude / Oplichting	Misbruik accounts voor bestellingen	Ja	Onbekend	Account Wehkamp en BonPri	Particulier	504.45	Onbekend	Bonprix	Burger	NA
PL0100 BVH 2019223545	Cybercrime	Fraude / Oplichting	Misbruik accounts voor bestellingen	Ja	Onbekend	Account Wehkamp en BonPri	Particulier	504.45	Onbekend	Bonprix	Burger	NA
PL0100 BVH 2019229132	Cybercrime	Fraude / Oplichting	Fraude bankgegevens / internetbankieren	Ja	Ja	Zogenaamde koper op Marktp	Particulier	202.02	Ja	ING	Burger	NA

cat_middelen	cat_organisatie	cat_motivatie	cat_actortype	kenmerk	waarde	voorval	mk	begindatum	einddatum	SRT_OMS	GEBOORTE_DAT	GESLACHT
NA	NA	NA	Oplichters en fraudeurs	NA	NA	PL0100 BVH 4648209	CYBERCRIM	25-4-2019 19:00	26-4-2019 01:00	SLACHTO	24-7-1949	Vrouw
NA	NA	NA	Oplichters en fraudeurs	NA	NA	PL0100 BVH 4648209	CYBERCRIM	25-4-2019 19:00	26-4-2019 01:00	AANGEVE	24-7-1949	Vrouw
NA	NA	NA	Overig/onbekend	NA	NA	PL0100 BVH 4583479	CYBERCRIM	26-3-2019 07:20	26-3-2019 07:20	MELDER	2-9-1946	Man
NA	NA	NA	Oplichters en fraudeurs	NA	NA	PL0100 BVH 4586661	OVERIGE H	26-3-2019 16:00	26-3-2019 16:00	MELDER	22-11-1997	Man
NA	NA	NA	Oplichters en fraudeurs	NA	NA	PL0100 BVH 4614502	FRAUDE ME	10-4-2019 09:15	10-4-2019 09:30	AANGEVE	14-9-1946	Man
NA	NA	NA	Oplichters en fraudeurs	NA	NA	PL0100 BVH 4614502	FRAUDE ME	10-4-2019 09:15	10-4-2019 09:30	SLACHTO	14-9-1946	Man
NA	NA	NA	Oplichters en fraudeurs	NA	NA	PL0100 BVH 4860367	FRAUDE ME	19-7-2019 12:00	23-8-2019 15:00	SLACHTO	25-10-1973	Man
NA	NA	NA	Oplichters en fraudeurs	NA	NA	PL0100 BVH 4860367	FRAUDE ME	19-7-2019 12:00	23-8-2019 15:00	AANGEVE	25-10-1973	Man
NA	NA	NA	Oplichters en fraudeurs	NA	NA	PL0100 BVH 4860367	FRAUDE ME	19-7-2019 12:00	23-8-2019 15:00	SLACHTO	21-4-1973	Vrouw
NA	NA	NA	Oplichters en fraudeurs	NA	NA	PL0100 BVH 4870281	CYBERCRIM	26-8-2019 20:00	26-8-2019 20:00	SLACHTO	31-1-1970	Man

**Noot. Persoonsgegevens zijn verwijderd uit de dataset*

Figuur 14 Voorbeeldweergaven van de aangeleverde dataset in Excel

Registratie	Jaartal	Jaartal_categorie	hoofdcategorie	subcategorie	Vorm_cybercriminaliteit	phishing	schade	kenmerk	Gebruik cryptovaluta
2021002240	2021	3	Fraude / Oplichting	Phishing	1	Ja	325	Cryptocurrency	1
2022085934	2022	3	Fraude / Oplichting	Phishing	2	Ja	1000	Cryptocurrency	1
2021261419	2021	2	Fraude / Oplichting	Phishing	2	Ja	10500	Cryptocurrency	1
2022211259	2022	3	Fraude / Oplichting	Phishing	2	Ja	18818	Cryptocurrency	1
2022211259	2022	3	Fraude / Oplichting	Phishing	2	Ja	18818	Cryptocurrency	1
2022211259	2022	3	Fraude / Oplichting	Phishing	2	Ja	18818	Cryptocurrency	1
2022024421	2022	3	Fraude / Oplichting	Phishing	2	Ja	2249	Cryptocurrency	1
2022024421	2022	3	Fraude / Oplichting	Phishing	2	Ja	2249	Cryptocurrency	1
2022560637	2022	3	Fraude / Oplichting	Phishing	2	Ja	2446.61	Cryptocurrency	1
2022285350	2022	3	Fraude / Oplichting	Phishing	2	Ja	958	Cryptocurrency	1

mk	begindatum	SRT_OMSCHR	Verdachte_of_slachtoffer	GEBOORTE_DAT	GESLACHT	Geslacht_code	Leeftijd	Leeftijd_categorie	
CYBERCRIME	2-1-2021	SLACHTOFFER	1	10-9-1957	Man	0	63	5	
CYBERCRIME	22-3-2022	SLACHTOFFER	1	25-2-2000	Vrouw	1	22	1	
CYBERCRIME	7-8-2021	SLACHTOFFER	1	13-2-1988	Vrouw	1	33	2	
CYBERCRIME	2-7-2022	SLACHTOFFER	1	3-1-1988	Man	0	34	2	
CYBERCRIME	2-7-2022	SLACHTOFFER	1	3-1-1988	Man	0	34	2	
CYBERCRIME	2-7-2022	SLACHTOFFER	1	3-1-1988	Man	0	34	2	
CYBERCRIME	1-10-2021	SLACHTOFFER	1	27-8-1976	Man	0	45	4	
CYBERCRIME	1-10-2021	SLACHTOFFER	1	27-8-1976	Man	0	45	4	
CYBERCRIME	29-11-2022	SLACHTOFFER	1	19-7-1975	Man	0	47	4	
CYBERCRIME	23-10-2022	SLACHTOFFER	1	26-6-1970	Man	0	52	4	

Figuur 15 Voorbeeldweergaven van de uiteindelijke dataset in Excel

Databewerking SPSS

Nadat het bestand vanuit Excel naar SPSS is geëxporteerd, zijn er nog enkele aanpassingen verricht aan de variabelen om ze geschikt te maken voor de analyses. Voor de variabele 'tijd in jaren' en 'vorm van cybercriminaliteit' zijn dummyvariabelen aangemaakt. Vervolgens zijn er interactievariabelen met deze dummyvariabelen aangemaakt.

Tijd in jaren

In het geëxporteerde databestand vanuit Excel is een variabele aanwezig die het jaar wanneer het delict plaatsvond aangaf door middel van een cijfer. Deze variabele bestond uit vier groepen. Om de variabele te kunnen opnemen in de analyses zijn er drie dummyvariabelen aangemaakt waarbij 2019 dient als referentiegroep. Hierbij is de volgende codering toegepast: 0 = 2019, 1 = 2020 of later; 0 = 2019 of 2020, 1 = 2021 of 2022; 0 = 2019, 2020 of 2021, 1 = 2022. Om de dummyvariabelen op te stellen zijn de volgende formules in SPSS gebruikt:

```
RECODE Jaartal_categorie (0=0) (1=1) (2=1) (3=1) INTO Dummy_2020_21_22.
VARIABLE LABELS  Dummy_2020_21_22 '2020 of later'.
EXECUTE.

RECODE Jaartal_categorie (0=0) (1=0) (2=1) (3=1) INTO Dummy_2021_22.
VARIABLE LABELS  Dummy_2021_22 '2021 of 2022'.
EXECUTE.

RECODE Jaartal_categorie (0=0) (1=0) (2=0) (3=1) INTO Dummy_2022.
VARIABLE LABELS  Dummy_2022 '2022'.
EXECUTE.
```

Vorm van cybercriminaliteit

In het geëxporteerde databestand vanuit Excel is een variabele aanwezig die door middel van een cijfer het soort cybercriminaliteit aangaf. Deze variabele bestond uit vier groepen. Om de variabele geschikt te maken voor analyse zijn er drie dummyvariabelen aangemaakt voor deze variabelen waarbij hacken dient als referentiegroep. Voor de eerste dummyvariabele wordt de volgende codering gebruikt: 1 = hacken, 0 = anders. In de tweede dummyvariabele geldt de volgende codering: 1 = Ddos, 0 = anders. Tot slot wordt in de derde dummyvariabele de codering: 1 = ransomware, 0 = anders, gebruikt

RECODE Vorm_cybercriminaliteit (1=1) (2=0) (3=0) (4=0) INTO Dummy_hacken.
EXECUTE.

RECODE Vorm_cybercriminaliteit (3=1) (2=0) (1=0) (4=0) INTO Dummy_ddos.
EXECUTE.

RECODE Vorm_cybercriminaliteit (4=1) (3=0) (2=0) (1=0) INTO Dummy_ransomware.
EXECUTE.

Financiële schade

In de (lineaire) regressieanalyse dient de financiële schade als afhankelijke variabele. De variabele financiële schade is opgedeeld in verschillende intervallen. Voor een financiële schade tot 5.000 euro wordt een interval van 100 euro gehanteerd. Voor een financiële schade tussen 5.000 en 10.000 wordt een interval van 1.000 gebruikt. Voor een financiële schade tussen 10.000 en 100.000 euro wordt een interval van 10.000 euro gebruikt. Voor een financiële schade tussen 100.000 en 1.000.000 euro wordt een interval van 100.000 euro gebruikt. Ten slotte wordt voor schadebedragen tussen 1.000.000 en 5.000.000 een interval van 1.000.000 euro gebruikt. Registraties met een financiële schade hoger dan 5.000.000 euro vallen in de laatste categorie. De intervallen zijn opgesteld door middel van de volgende formule:

RECODE schade (0=0) (0.01=0) (0.02=0) (0.03=0) (0.05 thru 99.99=1) (100 thru 199.99=2) (200 thru 299.99=3) (300 thru 399.99=4) (400 thru 499.99=5) (500 thru 599.99=6) (600 thru 699.99=7) (700 thru 799.99=8) (800 thru 899.99=9) (900 thru 999.99=10) (1000 thru 1099.99=11) (1100 thru 1199.99=12) (1200 thru 1299.99=13) (1300 thru 1399.99=14) (1400 thru 1499.99=15) (1500 thru 1599.99=16) (1600 thru 1699.99=17) (1700 thru 1799.99=18) (1800 thru 1899.99=19) (1900 thru 1999.99=20) (2000 thru 2099.99=21) (2100 thru 2199.99=22) (2200 thru 2299.99=23) (2300 thru 2399.99=24) (2400 thru 2499.99=25) (2500 thru 2599.99=26) (2600 thru 2699.99=27) (2700 thru 2799.99=28) (2800 thru 2899.99=29) (2900 thru 2999.99=30) (3000 thru 3099.99=31) (3100 thru 3199.99=32) (3200 thru 3299.99=33) (3300 thru 3399.99=34) (3400 thru 3499.99=35) (3500 thru 3599.99=36) (3600 thru 3699.99=37) (3700 thru 3799.99=38) (3800 thru 3899.99=39) (3900 thru 3999.99=40) (4000 thru 4099.99=41) (4100 thru 4199.99=42) (4200 thru 4299.99=43) (4300 thru 4399.99=44) (4400 thru 4499.99=45) (4500 thru 4599.99=46) (4600 thru 4699.99=47) (4700 thru 4799.99=48) (4800 thru 4899.99=49) (4900 thru 4999.99=50) (5000 thru 5999.99=51) (6000 thru 6999.99=52) (7000 thru 7999.99=53) (8000 thru 8999.99=54) (9000 thru 9999.99=55) (10000 thru 19999.99=56) (20000 thru 29999.99=57) (30000 thru 39999.99=58) (40000 thru 49999.99=59) (50000 thru 59999.99=60) (60000 thru 69999.99=61) (70000 thru 79999.99=62) (80000 thru 89999.99=63) (90000 thru 99999.99=64) (100000 thru 199999.99=65) (200000 thru 299999.99=66) (300000 thru 399999.99=67) (400000 thru 499999.99=68) (500000 thru 599999.99=69) (600000 thru 699999=70) (700000 thru 799999.99=71) (800000 thru 899999.99=72) (900000 thru 999999.99=73) (1000000 thru 1999999.99=74) (2000000 thru 2999999.99=75) (3000000 thru 3999999.99=76) (4000000 thru 4999999.99=77) (ELSE=78) INTO SCHADE_interval2

Interacties

In de logistische regressieanalyse worden de interacties tussen de dummyvariabelen opgenomen. Voor zowel 'tijd in jaren' als 'vorm van cybercriminaliteit' zijn drie dummyvariabelen aangemaakt. Dit betekent dat er negen interactievariabelen zijn opgesteld voor de logistische regressieanalyse. De interactievariabelen zijn opgesteld door middel van de volgende formules:

```
COMPUTE Interactie_hacken_2020later=Dummy_hacken * Dummy_2020_21_22.
EXECUTE.

COMPUTE Interactie_hacken_20212022=Dummy_hacken * Dummy_2021_22.
EXECUTE.

COMPUTE Interactie_hacken_2022=Dummy_hacken * Dummy_2022.
EXECUTE.

COMPUTE Interactie_ddos_2020later=Dummy_ddos * Dummy_2020_21_22.
EXECUTE.

COMPUTE Interactie_ddos_20212022=Dummy_ddos * Dummy_2021_22.
EXECUTE.

COMPUTE Interactie_ddos_2022=Dummy_ddos * Dummy_2022.
EXECUTE.

COMPUTE Interactie_ransomware_2020later=Dummy_ransomware * Dummy_2020_21_22.
EXECUTE.

COMPUTE Interactie_ransomware_20212022=Dummy_ransomware * Dummy_2021_22.
EXECUTE.

COMPUTE Interactie_ransomware_2022=Dummy_ransomware * Dummy_2022.
EXECUTE.
```

In de (lineaire) regressieanalyse worden allereerst de interacties tussen 'het gebruik van cryptovaluta's en de dummyvariabelen van de verschillende vormen van cybercriminaliteit toegevoegd. Vervolgens

wordt de interactie tussen 'het gebruik van cryptovaluta's' en 'tijd in jaren' toegevoegd. Voor de regressieanalyse zijn de volgend interacties opgesteld:

```
COMPUTE Interactie_cryptohacken=Gebruikcryptovaluta * Dummy_hacken.
EXECUTE.

COMPUTE Interactie_cryptoddos=Gebruikcryptovaluta * Dummy_ddos.
EXECUTE.

COMPUTE Interactie_cryptoransomware=Gebruikcryptovaluta * Dummy_ransomware.
EXECUTE.

COMPUTE Interactie_cryptojaartal=Gebruikcryptovaluta * Jaartal_categorie.
EXECUTE.
```

Bijlage III – Assumptietoetsing

Modelassumptie logistische regressieanalyse

Voorafgaand aan de logistische regressieanalyse zijn de assumpties getest om te controleren of de data geschikt is voor de analyse. De dataset is aangepast zodat de verschillende observaties geen invloed op elkaar hebben en de observaties onafhankelijk van elkaar zijn. Bovendien blijkt de assumptietoetsing dat er sprake is van multicollineariteit tussen 'hacken' en 'het gebruik van cryptovaluta's' in Model 3. Daarnaast is er ook sprake van multicollineariteit tussen de interactie 'hacken' en '2020 of later' in Model 3. Dit betekent dat de resultaten van Model 3 onvoldoende informatie geven over de invloed van het gebruik van cryptovaluta's in cybercriminaliteit. Als gevolg hiervan is de logistische regressieanalyse opnieuw uitgevoerd zonder de variabelen uit Model 3. De resultaten van de oorspronkelijke logistische regressieanalyse worden weergegeven in Bijlage IV. Ten slotte zijn er 64 uitbijters verwijderd uit de dataset. De uitbijters zijn individuele waarnemingen die niet specifiek gekoppeld zijn aan een bepaalde variabele in het model. Het was niet mogelijk om variabelen te hercoderen om de uitbijters in de dataset te behouden, omdat alle waarnemingen binnen een bepaald bereik van de variabele vallen Hieronder volgt de gedetailleerde beschrijving van de assumptietoetsing.

Uitbijters

Allereerst zal het databestand worden geanalyseerd op de aanwezigheid van uitbijters. Uitbijters zijn waarnemingen die significant afwijken van de overige waarnemingen in de dataset en kunnen het gevolg zijn van meetfouten, extreme waarden of echt uitzonderlijke observaties. Wanneer een uitbijter wordt geïdentificeerd, is het belangrijk om de oorzaak van de uitbijter te onderzoeken voordat er een beslissing wordt genomen over hoe ermee om te gaan.

Het is niet aan te raden om een uitbijter te verwijderen op basis van het feit dat het een uitbijter is. Het is essentieel om onderscheid te maken tussen onmogelijke- en onwaarschijnlijke uitbijters. Een onmogelijke uitbijter is een waarneming die duidelijk niet mogelijk is, bijvoorbeeld een negatieve leeftijd of -schadebedrag. In dergelijke gevallen kan de uitbijter veilig worden verwijderd.

Aan de andere kant zijn onwaarschijnlijke waarnemingen weliswaar mogelijk, maar wijken sterk af van de overige waarnemingen. In dit geval kunnen verschillende benaderingen worden overwogen. De waarnemingen kunnen worden getransformeerd om de invloed van de uitbijters te verminderen, maar het is ook mogelijk om de uitbijters in de analyses op te nemen zonder verdere aanpassingen.

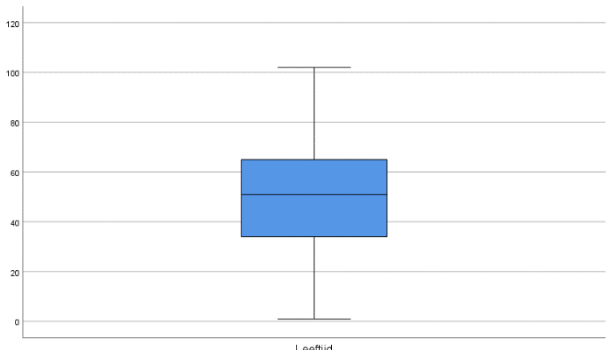
Om de invloed van uitbijters te beoordelen kan de analyse zowel met als zonder uitbijters worden uitgevoerd. Door de resultaten met elkaar te vergelijken kan worden bepaald in hoeverre de uitbijters de resultaten beïnvloeden en welke impact ze hebben op de conclusie van de analyse. Het is

belangrijk om voorzichtig te zijn bij het nemen van beslissingen over uitbijters en om altijd specifieke context van het onderzoek en de aard van de data in overweging te nemen.

Om te achterhalen of de dataset enkele uitbijters bevat voor de continue variabele 'leeftijd' kan er allereerst een boxplot worden opgesteld. De resultaten in Figuur 16 tonen aan dat er geen uitbijters zijn op het gebied van leeftijd. Ondanks de resultaten van de boxplot bevatte leeftijd enkele uitbijters. Deze zijn verwijderd uit de dataset.

Ten tweede kunnen de gestandaardiseerde residuen worden geanalyseerd om te bepalen of de dataset uitbijters bevat. Een waarneming wordt als uitbijter beschouwd wanneer het gestandaardiseerde residu een waarde heeft kleiner dan -3 of groter dan 3. Dit betekent dat de waarneming meer dan drie standaardafwijkingen afwijkt van het gemiddelde van de variabele. De resultaten van de logistische regressieanalyse tonen aan dat er 64 waarnemingen zijn met een gestandaardiseerde residu groter dan 3. De logistische regressieanalyse is opnieuw uitgevoerd zonder deze residuen. Hieruit is gebleken dat de residuen aanzienlijke invloed hadden op de resultaten. Daarom is besloten om de 64 waarnemingen te verwijderen uit de dataset

Voor categorische variabelen zijn uitbijters minder interessant dan voor continue variabelen. Uitbijters worden namelijk geassocieerd met afwijkende waarden die ver buiten een bepaalde range vallen. In het geval van categorische variabelen kunnen waarnemingen echter alleen tot specifieke categorieën behoren waardoor extreme waarden niet mogelijk zijn.



Figuur 16 Boxplot leeftijd

Naast uitbijters is ook onderzocht of de dataset enkele invloedrijke waarnemingen bevat. De Cook's Distance kan worden gebruikt om de invloedrijke punten te identificeren. Wanneer de Cook's Distance groter is dan 1, wordt de waarneming als invloedrijk beschouwd. In de dataset zijn er drie waarnemingen die een Cook's Distance hoger dan 1 hebben. Deze waarnemingen worden echter niet verwijderd uit de dataset, omdat het om invloedrijke waarnemingen gaat en niet om uitbijters. De invloedrijke punten worden beschreven in Tabel 7. De Cook's Distance geeft aan in hoeverre coëfficiënten veranderen wanneer een bepaalde registratie verwijderd. De Leverage daarentegen meet de afstand van een observatie tot het gemiddelde van de geschatte waarden in het regressiemodel. Tabel 7 toont aan dat de drie meest invloedrijke registraties een lage Leverage als Cook's Distance hebben, wat betekent dat deze registraties weinig invloed hebben op de regressiecoëfficiënt. De overige registraties beschikken over een lagere Cook's Distance.

Tabel 7
Overzicht invloedrijke waarnemingen

Waarneming	Residual	Leverage (*h*)	Cook's Distance
1	2,631	,038	1,052
2	2,230	,109	1,015
3	2,788	,021	1,008

Multicollineariteit

Multicollineariteit verwijst naar een hoge correlatie tussen twee of meer onafhankelijke variabelen. In een logistische regressieanalyse leidt multicollineariteit tot minder betrouwbare resultaten, omdat het moeilijk wordt om de individuele bijdrage van een onafhankelijke variabele op de afhankelijke variabele te beoordelen. Multicollineariteit kan worden beoordeeld met behulp van de Variance Inflation Factor (*VIF*). In de logistische regressieanalyse wordt een *VIF*-waarde van 10 of hoger als problematisch beschouwd. Uit de analyse blijkt dat de variabelen in Model 1 en 2 geen problematische multicollineariteit vertonen, aangezien de *VIF*-waarden lager zijn dan 10. Dit geldt echter niet voor Model 3. De analyse toont aan dat er multicollineariteit is tussen 'hacken' en het gebruik van cryptovaluta's (*VIF* = 10,833) in Model 3. Daarnaast is er ook sprake van multicollineariteit tussen de interactie 'hacken' en '2020 of later' op het gebruik van cryptovaluta's (*VIF* = 14,356). Om de multicollineariteit zo goed mogelijk op te lossen zal de interactieterm worden verwijderd. De dummyvariabele 'hacken' wordt echter behouden omdat het een sterke relatie heeft met het onderzoeksdoel.

Onafhankelijke waarnemingen

Voor de logistische regressieanalyse moeten de waarnemingen worden gecontroleerd op de onafhankelijkheid ten opzichte van elkaar. Hierbij worden waarnemingen als onafhankelijk beschouwd wanneer ze geen invloed op elkaar hebben. In dit onderzoek wordt er gebruik gemaakt van politieregistraties. De aangeleverde dataset bestond uit verschillende registratie die betrekking hadden op hetzelfde delict. De verschillende waarnemingen in de dataset zijn zo aangepast dat er per delict één registratie bekend was. Aan de hand van deze aanpassingen kan er worden gesteld dat er wordt voldaan aan de assumptie van onafhankelijk waarnemingen.

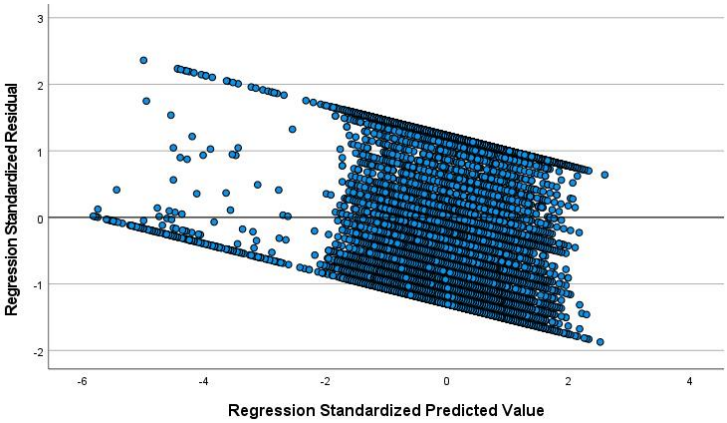
Lineaire regressieanalyse

Voorafgaand aan de (lineaire) regressieanalyse zijn de assumpties getoetst om de betrouwbaarheid van de resultaten te controleren. De dataset is aangepast zodat er geen overlappende registraties zijn met betrekking tot hetzelfde delict. Hierdoor is er geen onderlinge afhankelijkheid tussen de registraties en kan er worden geconcludeerd dat ze onafhankelijk van elkaar zijn en elkaar niet beïnvloeden. Bovendien wordt er voldaan aan de assumptie lineariteit, homoscedasticiteit en normale verdeling van de residuen.

Daarnaast zijn er zes waarnemingen verwijderd uit de dataset. Vijf van deze waarnemingen werden als uitbijter beschouwd vanwege hun gestandaardiseerde residu hoger dan 3. Daarnaast is één invloedrijke waarneming verwijderd op basis van een buitengewoon hoge Cook's Distance. Raadpleeg Tabel 8 voor een overzicht van de verwijderde waarnemingen.

Voorafgaand aan de regressieanalyse moet er worden onderzocht of er wordt voldaan aan de assumpties. Ten eerste moet er worden onderzocht of er wordt voldaan aan de assumptie van onafhankelijke waarnemingen. In dit onderzoek wordt er gebruik gemaakt van slachtoffer- en verdachtenregistraties afkomstig uit politiegegevens. In dit onderzoek wordt er voldaan aan de assumptie van onafhankelijke waarnemingen. Dit is mogelijk gemaakt doordat de waarnemingen zijn aangepast, waarbij per delict slechts één bekend was. Op basis van deze aanpassing kan er worden geconcludeerd dat er wordt voldaan aan de assumptie van onafhankelijke waarnemingen.

Ten tweede moet de assumptie van lineariteit worden onderzocht. Om de assumptie van lineariteit te toetsen moet het gemiddelde van de residuen gelijk zijn aan nul. Dit betekent dat de residuen niet systematisch afwijken van de nullijn. In de residuenplot worden de residuen op de y-as weergegeven en de voorspelde waarden van de onafhankelijke variabelen op de x-as. Het gemiddelde van de residuen wordt weergegeven door middel van de horizontale lijn. Figuur 17 toont aan dat de residuen van linksboven naar rechtsonder lopen. Dit kan wijzen op een mogelijk niet-lineaire verband.

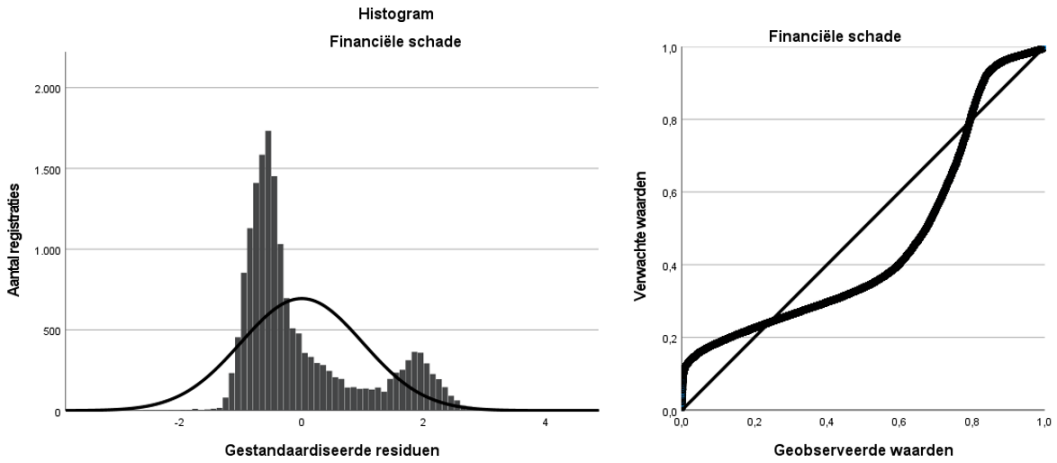


Figuur 17 Residuen plot

Ten derde moet de assumptie van homoscedasticiteit worden onderzocht. Homoscedasticiteit is aanwezig wanneer de conditionele standaarddeviatie constant is. Dit betekent dat de spreiding van de residuen in de residuenplot evenredig verdeeld zijn rond de nullijn. Figuur 17 toont aan dat de residuen ongeveer evenredig zijn verdeeld rond de nullijn. Het is belangrijk op te merken dat de residuen in het linker gedeelte van de plot hogere y-waarden hebben, maar dit patroon omgekeerd is in het rechter gedeelte. Op basis van deze bevindingen kan geconcludeerd worden dat er wordt voldaan aan de assumptie van homoscedasticiteit.

Tot slot moet er worden beoordeeld of de standaardfouten van de afhankelijke variabele – financiële schade – normaal verdeeld zijn. Er kan een histogram en PP-plot worden opgesteld om te controleren of er sprake is van een normale verdeling. In Figuur 18 wordt het histogram en de PP-plot weergegeven. Het histogram toont aan dat er sprake is van een normale verdeling. Het is echter belangrijk om aan te geven dat het niet gaat om een perfecte normale verdeling. Veel van de waarnemingen liggen namelijk links of rechts in de verdeling en bevinden er relatief minder waarnemingen zich in het midden van de verdeling.

Verder laat de PP-plot zien dat de residuen een S-vormig patroon vertonen. Een S-vormig patroon geeft aan dat de residuen afwijken van een perfecte normale verdeling. In een ideale situatie zouden de residuen in een PP-plot langs de diagonaal moeten liggen, wat overeenkomt met een normale verdeling. De S-vorm kan worden veroorzaakt door de verdeling van de residuen in het histogram. In het histogram is namelijk te zien dat veel van de residuen zich aan de linker- of rechterzijde van de verdeling bevinden. Op basis van het S-vormige patroon van de residuen kan geconcludeerd worden dat er niet wordt voldaan aan de assumptie van een normale verdeling van de standaardfouten.



Figuur 18 Histogram en PP-plot van de verwachte- en geobserveerde residuen van de financiële schade

Naast het controleren van de modelassumpties, moet ook de aanwezigheid van multicollineariteit tussen de onafhankelijke variabelen worden onderzocht. Multicollineariteit verwijst naar een hoge mate van samenhang tussen twee of meer onafhankelijke variabelen. Als er sprake is van multicollineariteit in de (lineaire) regressieanalyse, worden de resultaten minder betrouwbaar omdat het moeilijk is om de individuele bijdrage van elke onafhankelijke variabele op de afhankelijke variabele te bepalen. Multicollineariteit wordt beoordeeld aan de hand van de Variance Inflation Factor (*VIF*). Er is sprake van multicollineariteit wanneer een variabele een *VIF*-waarde hoger dan 10 heeft. De resultaten van de (lineaire) regressieanalyse geven aan dat er geen sprake is van multicollineariteit tussen de onafhankelijke variabele in de modellen.

Een methode om uitbijter te identificeren is door de gestandaardiseerde residuen te onderzoeken. Als een waarneming een gestandaardiseerde residuwaarde heeft kleiner dan -3 of groter dan 3, wordt deze beschouwd als een uitbijter. In de dataset werden vijf waarnemingen geïdentificeerd als uitbijters op basis van de residuwaarden. Deze waarnemingen zijn verwijderd uit de dataset. Zie Tabel 8 voor een overzicht van de verwijderde waarnemingen.

Er zijn verschillende manieren om te achterhalen of er invloedrijke punten in de dataset aanwezig zijn. Allereest geeft de Leverage aan in hoeverre een waarneming invloed heeft op geschatte coëfficiënt in de y-richting. Het is belangrijk om aan te geven dat een hoge Leverage waarde niet altijd problematisch hoeft te zijn. Om de leverage te berekenen kan de volgende formule worden gebruikt: Leverage = $hc > 2p / n$ of $3p / n$. Hierbij is p het aantal geschatte parameters en n het aantal registraties in de dataset. In dit onderzoek zijn er 16 parameters en bestaat de steekproef uit 17.403 registraties. Dit betekent dat registraties met een Leverage (h) van ,003 of hoger als invloedrijk kunnen worden gezien. Op basis van de Leverage bevat de dataset 36 invloedrijke registraties.

Ten tweede kan er worden gekeken naar de Cook's Distance (*CD*). Hierbij geeft een grotere Cook's Distance aan dat de registratie een grotere invloed heeft op het model. Wanneer een registratie een Cook's Distance heeft van 1 of hoger, wordt de registratie als problematisch beschouwd. In de dataset zijn geen registraties aanwezig met een Cook's Distance groter dan 1.

Tabel 8

Overzicht van de verwijderde waarnemingen uit de dataset

Waarneming	Standaardized Residual	Studentized Residual	Leverage (*h*)	Cook's Distance	DFFIT
1	3,070	3,074	,002	,004	,041
2	3,070	3,074	,002	,004	,041
3	3,066	3,070	,002	,004	,043
4	3,054	3,058	,002	,004	,039
5	3,042	3,046	,003	,004	,045
6	-,010	-1,961	,999	23650,336	-2100,983

Bijlage IV– Resultaten volledige logistische regressieanalyse

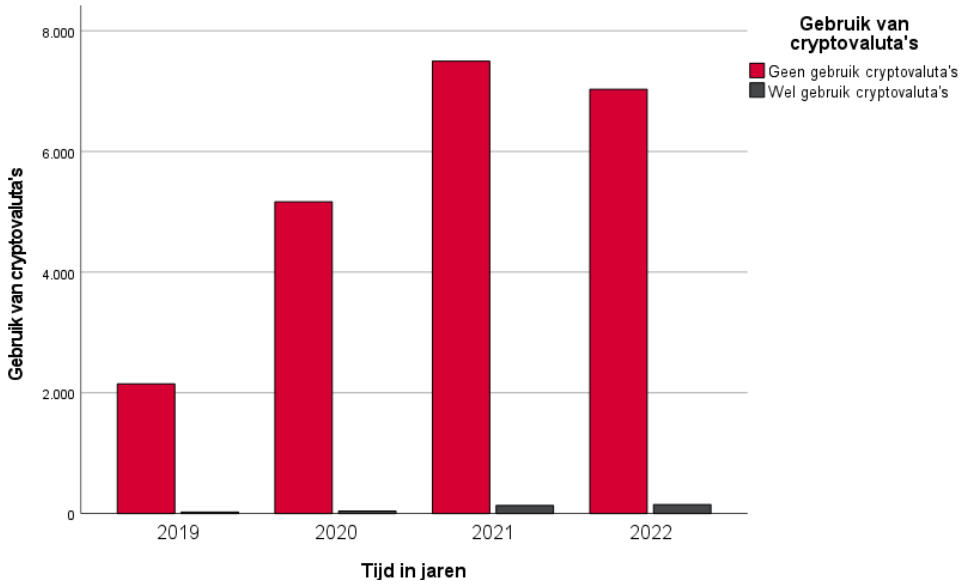
In deze bijlage worden de resultaten van de logistische regressieanalyse weergegeven waarin de interactievariabelen zijn opgenomen.

	Model *1*			Model 2			Model 3			Model 4		
	b (SE)	Odds-ratio	*p*	*b* (SE)	Odds-ratio	*p*	*b* (SE)	Odds-ratio	*p*	*b* (SE)	Odds-ratio	*p*
Constante	-5,188 (,289)	,006	<,001	-5,976 (,317)	,003	<,001	-21,203 (893,180)	,000	,981	-19,193 (837,555)	,000	,982
2020 of later	-,271 (,360)	,763	,451	,057 (,370)	1,059	,877	14,075 (893,180)	1296534,738	,987	14,136 (837,555)	1378373,293	,987
2021 of 2022	1,299 (,233)	3,665	<,001	1,610 (,246)	5,002	<,001	2,931 (,509)	18,748	<,001	3,025 (,510)	20,604	<,001
2022	,185 (,128)	1,203	,149	,183 (,131)	1,201	,161	,100 (,135)	1,105	,459	,154 (,137)	1,166	,262
Dummy hacken				,162 (,455)	,851	,722	17,332 (893,181)	33655880,90	,985	17,285 (837,555)	32105873,74	,984
Dummy Ddos				4,061 (,279)	58,027	<,001	19,817 (893,180)	403870570,80	,982	18,779 (837,555)	143041904,40	,982
Dummy Ransomware				2,888 (,218)	17,949	<,001	18,718 (893,180)	134623523,60	,983	18,541 (837,555)	112759635,10	,982
Interactie Hacken * 2020 of later							-31,407 (3968,937)	,000	,994	-31,564 (3768,863)	,000	,993
Interactie Hacken * 2021 of 2022							13,707 (3885,601)	897558,738	,997	13,676 (3674,620)	870035,961	,997
Interactie Hacken * 2022							-,030 (1,014)	,970	,976	-,203 (1,020)	,816	,842
Interactie Ddos * 2020 of later							-13,516 (893,181)	,000	,988	-13,301 (837,555)	,000	,987
Interactie Ddos * 2021 of 2022							-4,877 (1,194)	,008	<,001	-4,815 (1,211)	,008	<,001
Interactie Ddos * 2022							,475 (1,481)	1,608	,748	,290 (1,507)	1,336	,848

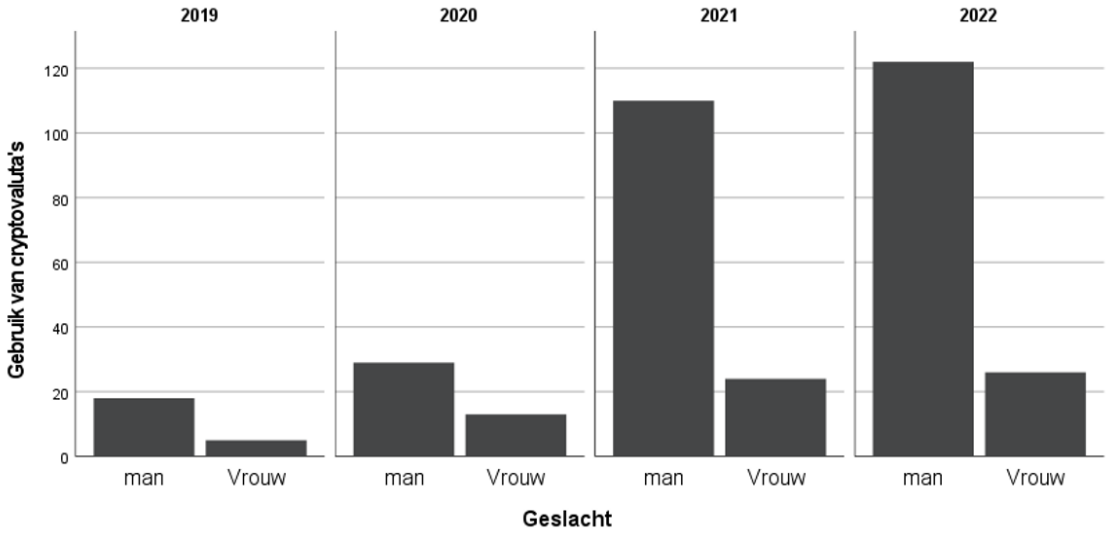
Interactie Ransomware * 2020 of later					-13,965 (893,181)	,000	,988	-14,080 (837,555)	,000	,987
Interactie Ransomware * 2021 of 2022					-2,753 (,869)	,064	,002	-2,625 (,881)	,072	,003
Interactie Ransomware * 2022					,958 (,568)	2,605	,092	,935 (,585)	2,548	,110
Geslacht (1 = vrouw; 0 = man)								-2,270 (,229)	,103	<,001
Leeftijd								-,036 (,004)	,965	<,001
Deviance	2958,107		2733,647		2674,061			2397,070		
X2-toets	71,512	<,001	224,460	<,001	59,586		<,001	276,991		<,001
Hosmer – Lemeshow	,000	-	11,775	,019	,000		-	9,326		,316
N	22.116		22.116		22.116			22.116		

Bijlage V– Grafieken gebruik cryptovaluta's

Voordat het gebruik van cryptovaluta's wordt beschreven moet er eerst worden gekeken naar het aandeel van het gebruik van cryptovaluta's in cybercriminaliteit. In Figuur 19 is te zien dat het gebruik van cryptovaluta's in cybercriminaliteit slechts een klein percentage van de totale cybercriminaliteit omvat. Het aantal registraties van cybercriminaliteit is van 2172 in 2019 gestegen naar 7631 in 2021. Het aantal registraties van cybercriminaliteit is vervolgens weer gedaald in 2022 naar 7180 registraties.



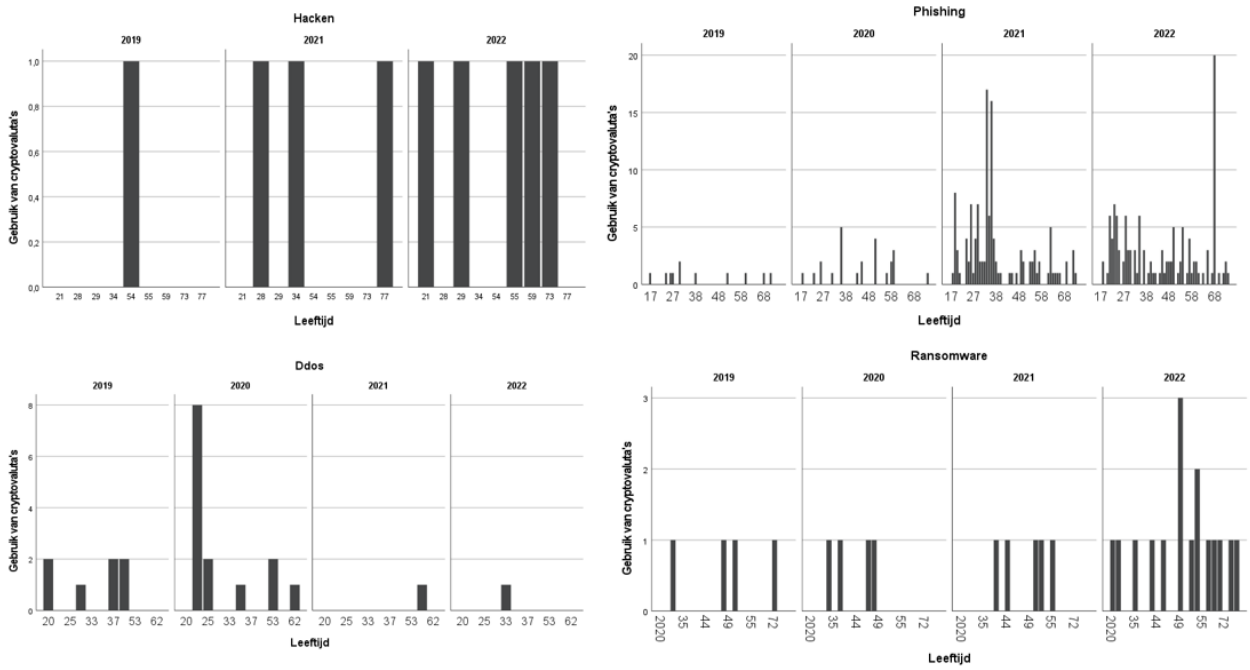
Figuur 19 **Geen- en wel gebruik van cryptovaluta's weergegeven voor 2019 tot en met 2022**



Figuur 20 Verschil in betrokkenheid bij cybercriminaliteit waarbij cryptovaluta's zijn gebruikt tussen geslacht

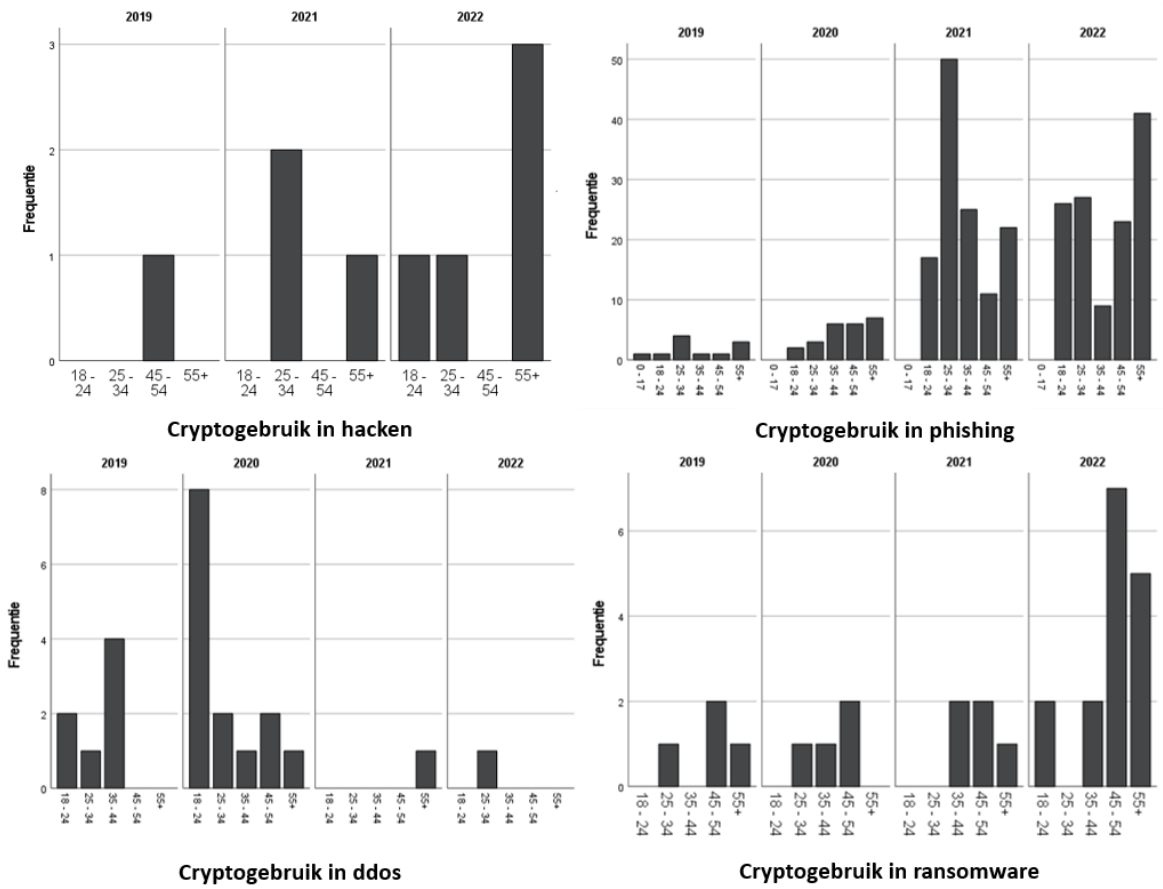
.

Mannen en vrouwen verschillen in hoeverre zij betrokken zijn bij cybercriminaliteit waarbij er gebruik is gemaakt van cryptovaluta's. De betrokkenheid uit zich in de vorm van slachtoffer- en daderschap. In Figuur 20 is te zien dat het aandeel mannen dat betrokken is bij cybercriminaliteit waarbij er gebruik is gemaakt van cryptovaluta's per jaar groter wordt vergeleken met vrouwen. Zo steeg het aantal registraties waarbij cryptovaluta's zijn gebruikt en mannen betrokken waren van 18 in 2019 naar 122 in 2022, wat een stijging is van 557,78%. De sterkste stijging voor mannen is te zien tussen 2020 en 2021. Het aantal registraties steeg van 29 in 2020 naar 110 in 2021, wat een stijging is van 279,31%. Het aantal registraties van cybercriminaliteit waarbij vrouwen betrokken waren en cryptovaluta's zijn gebruikt steeg van 5 in 2019 naar 26 in 2021, wat een stijging is van 420%.



Figuur 21 De leeftijd van de betrokkenen van cybercriminaliteit waarbij cryptovaluta's zijn gebruikt

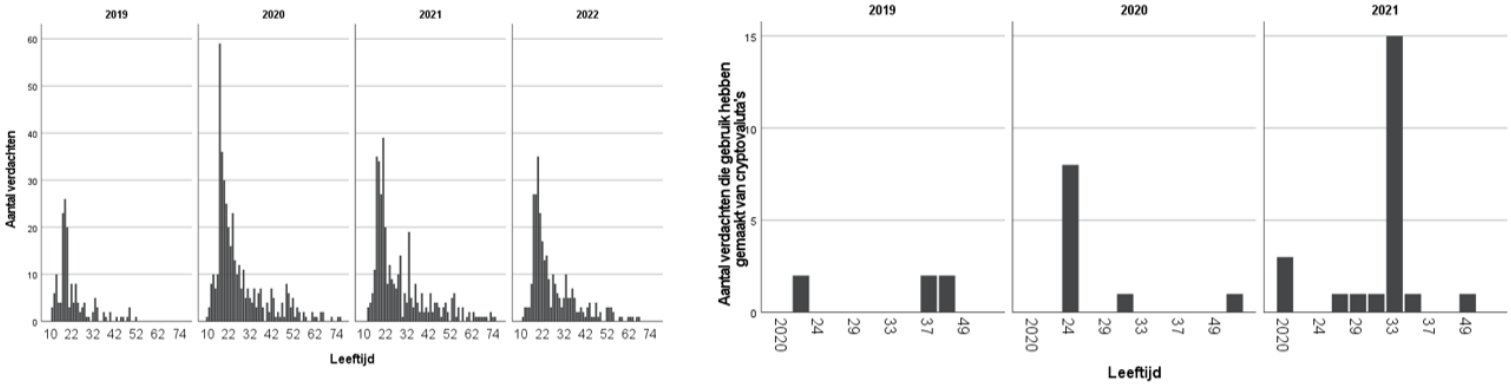
In Figuur 21 wordt de leeftijd van betrokkenen van cybercriminaliteit, waarbij cryptovaluta's zijn gebruik weergegeven voor de verschillende vormen van cybercriminaliteit. De betrokkenheid komt tot uiting in de registraties van verdachten en slachtoffers. Uit Figuur 21 blijkt dat oudere mensen vaker betrokken zijn bij ransomware en phishing.



Figuur 22 Het gebruik van cryptovaluta's per vorm van cybercriminaliteit voor de leeftijdscategorieën

In Figuur 22 wordt het gebruik van cryptovaluta's in cybercriminaliteit weergegeven voor leeftijd. Om de interpretatie van de resultaten van Figuur 19 te verbeteren is er voor gekozen om leeftijd weer te geven in intervallen. De resultaten laten verschillen in de betrokkenheid zien tussen de leeftijden. Zo geldt voor hacken, phishing en ransomware dat over het algemeen ouderen vaker betrokken zijn bij cybercriminaliteit waarbij cryptovaluta's worden gebruikt. Dit is echter niet het geval bij ddos. In Figuur 22 is te zien dat vooral jongeren betrokken zijn bij ddos aanvallen. Hieruit kan worden opgemaakt dat de betrokkenheid bij cybercriminaliteit waarbij cryptovaluta's worden gebruikt verschilt tussen de vormen van cybercriminaliteit voor leeftijd.

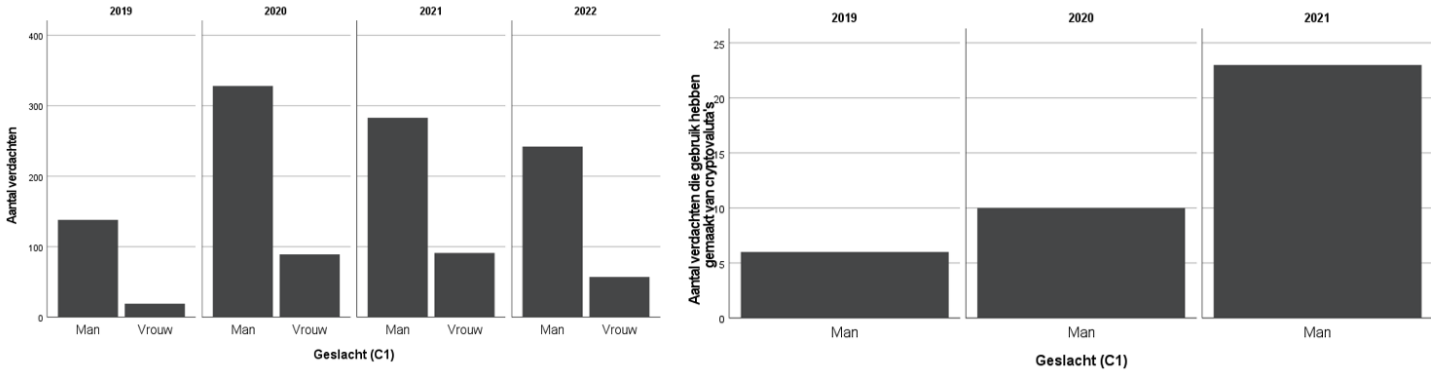
Bijlage VI– Verdachten en leeftijd



Figuur 23 Het aantal verdachten voor de verschillende jaren en welke gebruik hebben gemaakt van cryptovaluta's

De resultaten van Figuur 23 tonen aan dat er geconcludeerd kan worden dat jongeren vaker verdacht worden van cybercriminaliteit. In het rechterfiguur wordt de leeftijd van verdachten in cybercriminaliteit weergegeven die gebruik hebben gemaakt van cryptovaluta's. Bovendien tonen de resultaten uit Figuur 23 aan dat er weinig conclusies kunnen worden getrokken over de leeftijd van verdachten die cryptovaluta's hebben gebruikt. Er zijn te weinig bekende registraties en de leeftijd varieert sterk per jaar.

Bijlage VII– Verdachten en geslacht



Figuur 24 Geslacht van verdachten in cybercriminaliteit en die gebruik hebben gemaakt van cryptovaluta's

De resultaten in Figuur 24 tonen aan dat het overgrote deel van de verdachten in cybercriminaliteit mannen zijn. Bovendien toont Figuur 24 aan er geen vrouwelijke verdachten bekend zijn die gebruik hebben gemaakt van cryptovaluta's.

Bijlage VIII

In deze bijlage worden de verschillende kansen op het gebruik van cryptovaluta's voor de periode 2021 en 2022, evenals de verschillende vormen van cybercriminaliteit en het effect van de interactie op de kansen, beschreven. Model 3 laat zien dat de odds op het gebruik van cryptovaluta's in 2021 en 2022 19,242 keer hoger is dan in de periode 2019 en 2020. De odds van het gebruik van cryptovaluta's in Ddos is 533,679 keer hoger dan die van phishing. Voor ransomware is de odds 138,282 keer hoger dan die van phishing. Om de effecten van de onafhankelijke variabelen op het gebruik van cryptovaluta's te bepalen, zijn de kansen op het gebruik van cryptovaluta's voor de desbetreffende groep berekend. Zie onderstaande berekening ter verduidelijking.

Gebruik cryptovaluta's voor phishing in 2021/2022 $p = \frac{e^{-7.578+2.957}}{1+ e^{-7.578+2.957}} = \frac{0,0098}{1.0098} = 0,0097$

Gebruik cryptovaluta's voor hacken in 2021/2022 $p = \frac{e^{-7.578+2.957-0,172}}{1+ e^{-7.578+2.957-0,172}} = \frac{0,0083}{1.0083} = 0,0082$

Gebruik cryptovaluta's voor Ddos in 2021/2022 $p = \frac{e^{-7.578+2.957+6.280-4.643}}{1+ e^{-7.578+2.957+6.280-4.643}} = \frac{0,0506}{1.0506} = 0,0482$

Gebruik cryptovaluta's voor ransomware in 2021/2022 $p = \frac{e^{-7.578+2.957+4.929-2.924}}{1+ e^{-7.578+2.957+4.929-2.924}} = \frac{0,0731}{1.0731} = 0,0681$

Gebruik cryptovaluta's voor phishing in 2019/2020 $p = \frac{e^{-7.578}}{1+ e^{-7.578}} = \frac{0,0005}{1.0005} = 0,0005$

Gebruik cryptovaluta's voor hacken in 2019/2020 $p = \frac{e^{-7.578-0,172}}{1+ e^{-7.578-0,172}} = \frac{0,0004}{1.0004} = 0,0004$

Gebruik cryptovaluta's voor Ddos in 2019/2020 $p = \frac{e^{-7.578+6.280}}{1+ e^{-7.578+6.280}} = \frac{0,2731}{1.2731} = 0,2145$

Gebruik ransomware voor hacken in 2019/2020 $p = \frac{e^{-7.578+4.929}}{1+ e^{-7.578+4.929}} = \frac{0,0707}{1.0707} = 0,0660$

In de (lineaire) regressieanalyse is de gemiddelde financiële schade de afhankelijke variabele. Om de effecten van de onafhankelijke variabelen op de gemiddelde financiële schade te bepalen, zijn de gemiddelde voorspelde scores op de financiële schade berekend. Zie onderstaande berekening ter verduidelijking.

Gemiddelde financiële schade in 2019 zonder gebruik cryptovaluta's

- Phishing 12,959
- Hacken 12,959 – 12,168 = 0,791
- Ddos 12,959 + 5,589 = 18,548
- Ransomware 12,959 + 5,522= 18,481

Gemiddelde financiële schade in 2020 zonder gebruik cryptovaluta's

- Phishing 12,959 + 1.853 = 14.812
- Hacken 12,959 – 12,168 + 1.853 = 2.644
- Ddos 12,959 + 5,589 + 1.853 = 20.401
- Ransomware 12,959 + 5,522 + 1.853 = 20.334

Gemiddelde financiële schade in 2021 zonder gebruik cryptovaluta's

- Phishing 12,959 + (1.853 * 2) = 16.665
- Hacken 12,959 – 12,168 + (1.853 * 2) = 4.497
- Ddos 12,959 + 5,589 + (1.853 * 2) = 22.254
- Ransomware 12,959 + 5,522 + (1.853 * 2) = 22.187

Gemiddelde financiële schade in 2022 zonder gebruik cryptovaluta's

- Phishing 12,959 + (1.853 * 3) = 18.518
- Hacken 12,959 – 12,168 + (1.853 * 3) = 6.35
- Ddos 12,959 + 5,589 + (1.853 * 3) = 24.107
- Ransomware 12,959 + 5,522 + (1.853 * 3) = 24.04

Gemiddelde financiële schade in 2019 als gevolg van het gebruik van cryptovaluta's

- Phishing 12,959 + 12.943 = 25.902
- Hacken 12,959 – 12,168 + 12.943 -14.480= -0,746 (dus 0)
- Ddos 12,959 + 5,589 + 12.943 + 11.497= 42.988
- Ransomware 12,959 + 5,522 + 12.943 - 26.448= 4.976

Gemiddelde financiële schade in 2020 als gevolg van het gebruik van cryptovaluta's

- Phishing 12,959 + 12.943 + 1.853 + 3.203 = 30.958
- Hacken 12,959 – 12,168 + 12.943 + 1.853 + 3.203 -14.480 = 4.31
- Ddos 12,959 + 5,589 + 12.943 + 1.853 + 3.203 + 11.497 = 48.044
- Ransomware 12,959 + 5,522 + 12.943 + 1.853 + 3.203 - 26.448 = 10.032

Gemiddelde financiële schade in 2021 als gevolg van het gebruik van cryptovaluta's

- Phishing 12,959 + 12.943 + (1.853*2)+ (3.203 * 2) = 36.014
- Hacken 12,959 – 12,168 + 12.943 + (1.853*2)+ (3.203 * 2) -14.480 = 9.366
- Ddos 12,959 + 5,589 + 12.943 + (1.853*2)+ (3.203 * 2) + 11.497 = 41.603
- Ransomware 12,959 + 5,522 + 12.943 + (1.853*2)+ (3.203 * 2) -26.448 = 15.088

Gemiddelde financiële schade in 2022 als gevolg van het gebruik van cryptovaluta's

- Phishing 12,959 + 12.943 + (1.853*3)+ (3.203 * 3) = 41.07
- Hacken 12,959 – 12,168 + 12.943 + (1.853*3) + (3.203 * 3) -14.480 = 14.422
- Ddos 12,959 + 5,589 + 12.943 + (1.853*3) + (3.203 * 3) + 11.497 = 58.156
- Ransomware 12,959 + 5,522 + 12.943 + (1.853 *3)+ (3.203 * 3) -26.448 = 20.144