UIT DE PRAKTIJK

Het ontrafelen en integraal aanpakken van een cybercrimineel jeugdnetwerk

Geleerde lessen uit RIEC-casuïstiek in Noord-Nederland*

Sander Veenstra

In deze praktijkbijdrage gaan we in op de integrale aanpak van een cybercrimineel jeugdnetwerk in Noord-Nederland. Via het RIEC-samenwerkingsverband hebben gemeenten, politie, de Belastingdienst en de Arbeidsinspectie samengewerkt bij het in kaart brengen en aanpakken van het netwerk. Hoewel een integrale aanpak van cybercrime al lange tijd wordt bepleit, is deze werkwijze voor zover bij ons bekend uniek in Nederland. Het levert waardevolle inzichten op. Onze conclusie luidt dat een lokale en integrale aanpak van een 'cyber'crimineel netwerk loont, omdat het leidt tot een rijkere informatiepositie en een groter palet aan interventiemogelijkheden dan een monodisciplinaire benadering. We sluiten de praktijkbijdrage af met drie daarover geleerde lessen.

Introductie

Veiligheidspartners in Noord-Nederland verliezen naar eigen zeggen het zicht op problematische jeugdnetwerken. Professionals vermoeden dat zulke netwerken hun werkterrein (deels) hebben verlegd van traditionele criminele activiteiten naar relatief onzichtbare vormen van cybercriminaliteit.[1] Het is een praktijkhypothese die aansluit bij kennis uit de wetenschap. De literatuur suggereert bijvoorbeeld dat het actieve internetgedrag van jongeren – die volgens de *age crime curve* het grootste aandeel hebben in criminaliteitscijfers – leidt tot minder straat- en meer cybercriminaliteit (Aebi & Linde, 2010; Farell et al., 2011). Daarvoor bestaan inmiddels ook aanwijzingen: traditionele criminaliteit onder jongeren neemt af, terwijl allerlei vormen van cybercriminaliteit door jongeren toenemen (WODC, 2021; Leukfeldt & Roks, 2020).
Dat er cybercriminele (jeugd)netwerken actief zijn, staat buiten kijf. Justitie heeft inmiddels de nodige casussen behandeld en ook door de wetenschap zijn zulke netwerken al herhaaldelijk bestudeerd (zie bijv.: Leukfeldt, 2016; Kruisbergen et al.,

* Bij de totstandkoming van deze praktijkbijdrage zijn ook Jan Kornelis Dijkstra, Maaike Schaafsma en Anita Eising betrokken geweest. Jan Kornelis en Maaike zijn senior analist en Anita is projectleider/bestuurlijk expert ondermijning bij het RIEC Noord-Nederland. De contactgegevens van Sander Veenstra zijn op te vragen bij de redactie.

1 Zie de volgende paragraaf voor een toelichting over wat in dit artikel onder cybercriminaliteit wordt verstaan.

2018). Met het oog op de aanpak ervan is daarmee relevante kennis opgedaan. Bekend is dat cybercriminele netwerken zich vaak zowel bezighouden met het plegen van cybercriminaliteit als met traditionele delicten (Leukfeldt & Roks, 2020; Roks, Leukfeldt & Densley, 2020). Relevant is ook dat netwerken die cybercriminaliteit plegen veelal sterk lokaal zijn ingebed (Kruisbergen et al., 2018; Leukfeldt et al., 2019). Offline sociale banden tussen netwerkleden zijn nog altijd van belang. Leden van cybercriminele netwerken kennen elkaar uit de buurt of maken bijvoorbeeld gebruik van lokale katvangers om crimineel geld in ontvangst te nemen (Leukfeldt, Spithoven & Misana-ter Huurne, 2020). Ondanks het 'grenzeloze' karakter van cybercriminaliteit, biedt dat mogelijkheden voor de lokale aanpak van cybercriminele jeugdnetwerken.

De aanpak van criminele jeugdnetwerken vindt van oudsher plaats onder regie van gemeenten, in samenwerking met politie, OM en hulp- en zorgorganisaties (Ferwerda & Van Ham, 2010). Gezien de lokale verankering van cybercriminele jeugdnetwerken, hebben zij nog steeds een sleutelrol (Leukfeldt, Spithoven & Misana-ter Huurne, 2020). In de praktijk leunen veiligheidspartners echter sterk op de politie, terwijl de politie cybercriminele netwerken niet alleen kan bestrijden. Al geruime tijd is immers het adagium dat een integrale aanpak van cybercriminaliteit noodzakelijk is (Jewkes & Jar, 2008; Veenstra, Leukfeldt & Boes, 2013). Op lokaal niveau blijken mogelijkheden daartoe veelal echter onbekend en/of onbemind.

Het RIEC-samenwerkingsverband in Noord-Nederland heeft cybercriminaliteit benoemd als 'handhavingsknelpunt'. Dat betekent dat in RIEC-verband invulling kan worden gegeven aan de integrale aanpak van cybercriminaliteit. Een vereiste is wel dat sprake is van cybercriminaliteit die in georganiseerd verband wordt gepleegd en/of van delicten die de beoogde en legale werking van een samenlevingssysteem aantasten (het ondermijningscriterium). De onderwereld moet, met andere woorden, misbruik maken van en/of verweven zijn met de bovenwereld. Ook moeten ten minste twee RIEC-partners belang hebben bij de aanpak van een specifieke cybercrimecasus (het integraal criterium).

Als gevolg van de ambitie om gezamenlijk op te trekken bij de aanpak van cybercriminaliteit brengt de politie september 2020 een casus in bij het RIEC-samenwerkingsverband. Kort daarvoor ontvangt de eenheid Noord-Nederland een signaal van de Electronic Crimes Task Force (ECTF), een samenwerkingsverband tussen de politie en de grootbanken in Nederland. Meerdere bij de ECTF bekende betaalverzoekfraudezaken wijzen op dat moment in de richting van een toen 21-jarig subject in Noord-Nederland. Er zijn bovendien aanwijzingen dat het subject onderdeel is van een groter crimineel netwerk. Hoewel er kansen liggen voor strafrechtelijk onderzoek, blijft dat aanvankelijk uit. Volgens de signaalindiener is ook maar de vraag of dat onderzoek er komt. Bovendien zou strafrechtelijk onderzoek zich uitsluitend richten op het subject en niet op het ontrafelen van het bredere cybercriminele netwerk waarvan hij onderdeel lijkt te zijn. Een gemiste kans, omdat inzicht in het grotere netwerk mogelijk ook zicht biedt op belangrijke(re) sleutelfiguren. Daarnaast lijkt het signaal mogelijkheden te bieden voor een integrale aanpak. Op 7 oktober 2020 neemt het RIEC-samenwerkingsverband de casus

in behandeling, waarna convenantpartners onder voorwaarden informatie met elkaar mogen delen en zich kunnen buigen over een integrale aanpak.
Het vervolg van deze praktijkbijdrage gaat over de integrale behandeling van deze cybercrimecasus in Noord-Nederland. Allereerst lichten we toe wat in deze praktijkbijdrage onder cybercriminaliteit wordt verstaan. Vervolgens leggen we de van signaal tot interventie gehanteerde werkwijze beknopt uit. Daarna zijn de analyse- en interventieresultaten beschreven. De kenmerken en criminele activiteiten van het netwerk, alsook geleerde lessen voor de lokale en integrale aanpak van cybercriminaliteit komen aan bod.

Definitie en afbakening

De term cybercriminaliteit fungeert in deze praktijkbijdrage als paraplubegrip: het omvat alle misdrijven waarbij informatie- en communicatietechnologie (ICT) van wezenlijk belang is voor de realisatie van het delict. Zowel misdrijven waarbij ICT uitsluitend het middel is, zoals oplichting via internet, als de meer high tech verschijningsvormen waarbij ICT zowel het middel als het doel is, zoals hacken en ransomware, vallen onder die definitie. De keuze om het begrip cybercriminaliteit te gebruiken is gemaakt omwille van de leesbaarheid, maar ook – en belangrijker – vanwege de verwevenheid tussen de delictscategorieën. Bij online oplichting (gedigitaliseerde criminaliteit) kan er bijvoorbeeld ook sprake zijn van hacken of het gebruik van malware (cybercriminaliteit in enge zin) om de fraude te kunnen plegen. Bij het bestudeerde cybercriminele jeugdnetwerk is daarvan sprake.

Van signaal tot interventie: gehanteerde werkwijze

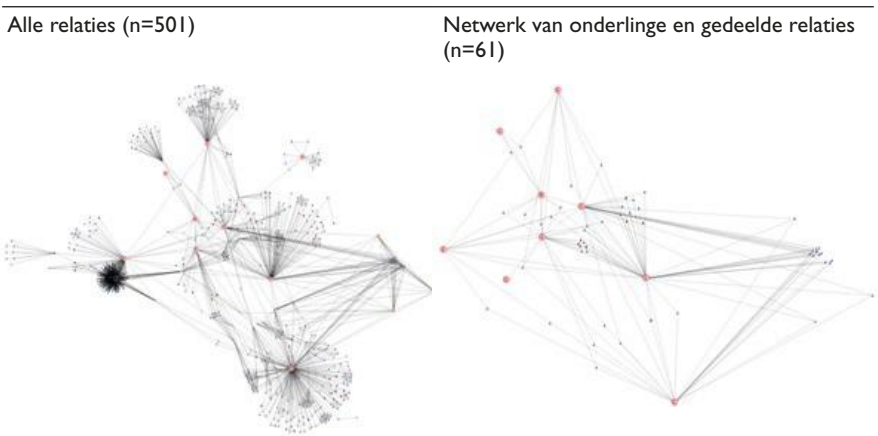
Ruim een maand nadat het signaal over betaalverzoekfraude werd ingecheckt, is het daarbij betrokken hoofdsubject op heterdaad aangehouden. Er is toen alsnog strafrechtelijk onderzoek tegen hem ingesteld. Op het grotere netwerk waarvan hij onderdeel was, werd zoals verwacht strafrechtelijk niet geïnvesteerd. In RIEC-verband is daarom een analyseplan opgesteld dat zich toespitste op het ontrafelen van het (cyber)criminele netwerk rondom het oorspronkelijke subject en het bieden van inzicht in de (cyber)criminele activiteiten ervan. Uiteindelijk met als doel om adequaat invulling te geven aan de aanpak van het (cyber)criminele netwerk.[2]
Hierna is op hoofdlijnen beschreven hoe het (cyber)criminele netwerk is ontrafeld, hoe de informatiepositie over de geïdentificeerde netwerkleden is verrijkt en hoe mogelijkheden voor de aanpak van het netwerk in kaart zijn gebracht.

Het ontrafelen van het (cyber)criminele netwerk op basis van politie-informatie
Het onderzoek richtte zich aanvankelijk op het in kaart brengen van het (cyber)criminele netwerk rondom het oorspronkelijke hoofdsubject. In het door de politie

2 Cyber is hier bewust tussen haakjes geplaatst. Cybercriminaliteit vormt namelijk wel het vertrekpunt voor de analyse, maar de analyse is daar niet toe begrensd. Aanwijzingen voor andere ondermijnende criminaliteitsvormen zijn daarin meegenomen.

aangedragen signaal waren al negen subjecten in beeld. Om te beginnen zijn alle personen in kaart gebracht waarmee die oorspronkelijke negen subjecten gezamenlijk voorkomen in politieregistraties. Zo ontstond een overzicht van 501 personen. Het gros daarvan was irrelevant voor de casus: we zijn namelijk op zoek gegaan naar de kernleden van het cybercriminele netwerk. Daarvoor zijn twee criteria gehanteerd. Om te behoren tot een samenwerkend netwerk van kernleden, moeten alle leden een directe relatie hebben met minimaal twee andere leden uit het netwerk. Daarnaast moeten er aanwijzingen bestaan dat de netwerkleden gezamenlijk (cyber)criminele activiteiten ontplooien. Met behulp van Analyst's Notebook is daarom allereerst gefilterd op alle onderlinge en gedeelde relaties van de oorspronkelijke negen subjecten. Van de 501 personen, blijven er dan 61 subjecten over.

Figuur 1 Het afpellen van het netwerk



Vervolgens is getoetst in hoeverre de 61 overgebleven subjecten gezamenlijk (cyber)criminele activiteiten ontplooien. Daarvoor zijn de 96 unieke BVH-registraties waarop de relaties tussen de 61 overgebleven subjecten zijn gebaseerd, gestructureerd geanalyseerd. 59 registraties hebben geen betrekking op de (gezamenlijke) betrokkenheid van subjecten bij cybercriminaliteit of andere (ondermijnende) criminele activiteiten. In de resterende 37 relevante registraties komen 34 van de 61 eerder geïdentificeerde subjecten terug. Opnieuw zijn niet alle 34 subjecten relevant voor verdere analyse, omdat niet alle subjecten een criminele rol vervullen in de registraties. Zij zijn bijvoorbeeld slachtoffer of getuige of hun rol wordt in de politieregistratie(s) niet geduid. Alle irrelevante personen zijn vervolgens verwijderd uit de selectie. Uiteindelijk zijn op deze wijze vijftien kernleden geïdentificeerd die (in wisselende samenstelling) gezamenlijk (cyber)criminele activiteiten ontplooien.

- Parallelle witwascasus met een overlappend netwerk

Ruim een maand voor aanvang van de cybercrimecasus nam het RIEC Noord-Nederland ook een andere casus in behandeling. Het hoofdsubject in die casus zou criminelen faciliteren door voertuigen op zijn naam te zetten en via zijn bedrijf crimineel geld wit te wassen. Parallel aan de inspanningen om het cybercriminele netwerk in kaart te brengen, is ook in die casus onderzoek verricht. Onderdeel van de analyse was het criminele netwerk rondom de vermeende facilitator in kaart te brengen. Daarvoor is een vergelijkbare methode gehanteerd als in de cybercrimecasus: de relaties van het hoofdsubject zijn in kaart gebracht en op basis van een inhoudelijke analyse van politieregistraties zijn relevante netwerkleden geïdentificeerd. Uiteindelijk is in de witwascasus een netwerk van veertien kernleden ontrafeld. Opvallend genoeg bleek er een sterke overlap te bestaan met de leden van het cybercriminele netwerk. Acht subjecten zijn zowel kernlid in de cybercrimecasus als in de witwascasus. Daarnaast kwamen in de witwascasus drie subjecten voor die wel naar voren zijn gekomen in de cybercrimecasus, maar daarin geen criminele rol vervulden. Zij behoorden daarom aanvankelijk niet tot de vijftien kernleden in de cybercrimecasus. Tot slot zijn in de witwascasus drie kernleden geïdentificeerd die in de cybercrimecasus buiten beschouwing bleven. Gezien de grote overlap tussen de subjecten in de cybercrime- en de witwascasus, is besloten om beide casussen samen te voegen. Alle geïdentificeerde kernleden zijn daarin meegenomen. In totaal bestaat het initieel geïdentificeerde netwerk dan uit 21 personen en drie bedrijven.

- Katvangers

Opgeteld zijn in beide casussen ook tientallen katvangers geïdentificeerd, maar omdat onze aanpak zich richtte op kernleden in het criminele netwerk, blijven zij verder buiten beschouwing.

Het verrijken van de informatiepositie

Om meer zicht te krijgen op aanwijzingen voor ondermijnende criminele activiteiten is de informatiepositie over leden van het netwerk verrijkt met informatie van de betrokken gemeenten, het OM, de Belastingdienst, de FIOD, de Nederlandse Arbeidsinspectie, de IND en de Financial Intelligence Unit (FIU). Daarnaast zijn (semi)open bronnen geraadpleegd (openbare websites, openbare profielen op social media, Kadaster, Kamer van Koophandel).

Multidisciplinair overleg

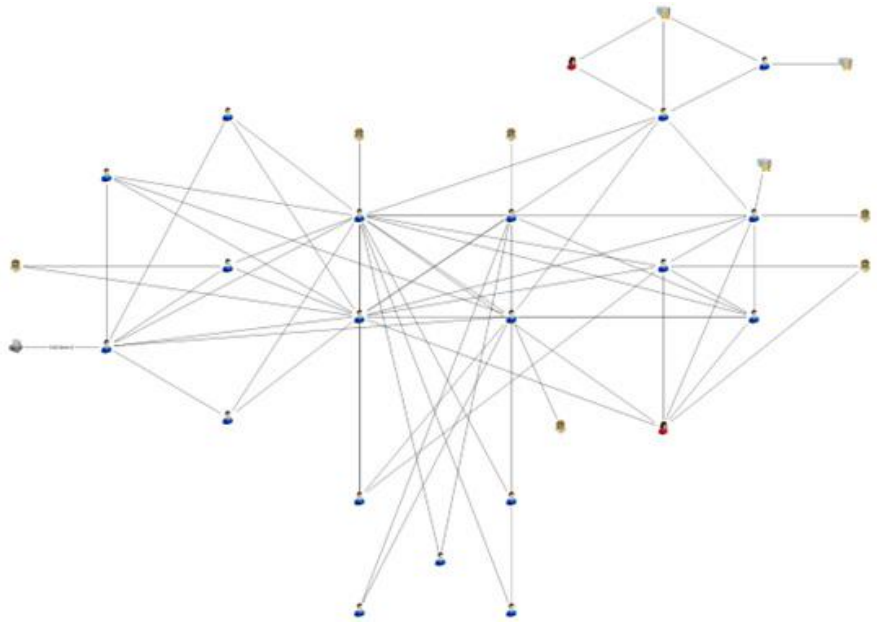
In RIEC-verband vindt tweewekelijks overleg plaats, waarin bevindingen over een casus worden geduid en waarin wordt gespard over interventiemogelijkheden. Zo ook in deze casus. Los daarvan zijn een aantal (groeps)gesprekken gevoerd met ambtenaren die op lokaal niveau betrokken zijn bij de aanpak van jeugdgroepen, omdat zij dossierkennis hebben over diverse leden in het netwerk.

Bevindingen

Het netwerk

In figuur 2 is het netwerk met personen, bedrijven en hun onderlinge relaties weergegeven.[3] Na de figuur zijn de kenmerken van het netwerk en de netwerkleden beschreven. Daarbij is uitgegaan van het hier gepresenteerde initiële netwerk. Een kanttekening is dat gedurende de casus het netwerk continu in beweging is. Netwerkleden die aanvankelijk een belangrijke rol lijken te spelen, verdwijnen naar de achtergrond, terwijl er nieuwe leden in beeld verschijnen. Nieuwe leden blijven echter in de netwerkbeschrijving hierna buiten beschouwing.

Figuur 2 Netwerk van cybercrime- en witwascasus (n=21)



Demografische kenmerken

Op twee subjecten na, zijn alle netwerkleden man. De twee vrouwen zijn de moeders van twee van de subjecten. Beide vrouwen spelen een relatief kleine, maar faciliterende en/of profiterende rol in de casus en zijn daarom aanvankelijk meegenomen in de analyse. Ze treden bijvoorbeeld op als gevolmachtigde in aan het netwerk gerelateerde bedrijven of kopen luxe voertuigen die ze gezien hun officiële inkomenspositie niet kunnen betalen en zijn bekostigd met cybercrimineel geld.

3 Netwerkleden die een relatie onderhouden met de eigenaar van een bedrijf, worden veelal ook aan diens bedrijf gerelateerd. Bijvoorbeeld omdat zij bij het bedrijf worden gesignaleerd of in auto's van het bedrijf rondrijden. Omdat het hier (voor het overzicht) een versimpelde weergave betreft, zijn die relaties niet ingetekend. Wel zijn relaties met de eigenaar weergegeven.

De leeftijd van subjecten varieert. De twee moeders zijn, samen met een tweede gevolmachtigde van het vermeende witwasbedrijf, respectievelijk 52, 48 en 46 jaar oud. De leeftijd van de andere subjecten ligt tussen de 18 en 28 jaar met een gemiddelde leeftijd van 22 jaar.

Oorsprong: lokale wortels
Het netwerk is geworteld in één stad in Noord-Nederland. Veertien van de 21 subjecten zijn daar woonachtig en een groot deel van hen is daar ook geboren of getogen. Twee anderen wonen in een nabijgelegen dorp, maar zijn volgens praktijkprofessionals bekenden in de stad. Dat geldt ook voor een derde subject, wiens adres onbekend is. Hij zou een jeugdvriend zijn van een aantal andere subjecten en zijn opgegroeid en naar school zijn gegaan in dezelfde stad. Vier subjecten wonen verder weg: twee daarvan – die gerelateerd zijn aan het vermeende witwasbedrijf – wonen in een andere stad in Noord-Nederland, waar ook het bedrijf is gevestigd. De overige twee subjecten zijn woonachtig in de Randstad.
Lokale professionals stellen dat de subjecten die geworteld zijn in dezelfde stad in Noord-Nederland elkaar vermoedelijk kennen van de buurt en/of van school. De beschikbare data ondersteunen dat: op één na, wonen alle subjecten in een aantal dezelfde buurten, die zich allemaal aan één bepaalde kant van de stad bevinden. Ten minste acht van de 21 subjecten hebben bovendien vanaf (in ieder geval) 2015 een deels gemeenschappelijke onderwijscarrière. Zij stonden op diverse momenten (in wisselende samenstelling) ingeschreven bij drie dezelfde instellingen voor middelbaar beroepsonderwijs.
Over de hele linie blijkt het netwerk sterk lokaal verankerd. Offline sociale banden, waarvoor de buurt en school als broedplaats kunnen fungeren, hebben bij de totstandkoming ervan vermoedelijk een belangrijke rol gespeeld.

Ontwikkeling
Acht van de 21 subjecten zijn op lokaal niveau al geruime tijd in beeld bij gemeente en politie, bijvoorbeeld als lid van hetzelfde traditionele criminele jeugdnetwerk of omdat zij onderdeel zijn van een andere specifieke probleem- of persoonsgerichte aanpak. De problematiek waarbij deze subjecten betrokken zijn, is uiteenlopend van aard, zoals scooterdiefstal, heling, geweldsdelicten en drugshandel.
Opvallend is dat een vijftal subjecten al in 2019 gezamenlijk in verband is gebracht met een cyberdelict. Vermoedelijk zijn de cybercriminele carrières van twee van de destijds betrokken netwerkleden daar begonnen. Daarna nemen ze een steeds prominentere rol in het netwerk in en fungeren ze uiteindelijk als opleiders voor nieuwe cybercriminele aanwas. Eén daarvan ontpopt zich zelfs tot het voornaamste subject in de casus (zie hierna onder Sleutelfiguren).

Sleutelfiguren
Het berekenen van centraliteitsmaten[4] in combinatie met een inhoudelijke analyse van politieregistraties biedt in eerste instantie zicht op een viertal sleutelfiguren binnen het netwerk. Eén daarvan heeft de meest prominente rol. Gedurende de

4 Degree en eigenvector.

casus zijn politieregistraties en registraties van gemeentelijke Buitengewoon Opsporingsambtenaren (BOA) actief gemonitord. Twee van de oorspronkelijk geïdentificeerde sleutelfiguren, waaronder het kernlid met de meest prominente rol, blijven actief als sleutelfiguur. De hoeveelheid en aard van aan hen gerelateerde registraties doet vermoeden dat de rol van de twee andere sleutelfiguren afzwakt. Hun positie wordt ingenomen door een nieuw sleutelfiguur die al wel tot het initiele netwerk behoorde. De drie vormen gedurende de casus (2020-2022) een drie-eenheid en trekken gezamenlijk op bij het plegen van (cyber)criminele activiteiten.

Ondermijnende criminele activiteiten

Het geïdentificeerde netwerk pleegt uiteenlopende delicten. Er zijn aanwijzingen voor cybercriminele activiteiten, maar ook voor betrokkenheid bij de handel in verdovende middelen, zware geweldsdelicten, wapenbezit, witwassen en economische delicten. Deze bevindingen corresponderen met eerder onderzoek, waaruit blijkt dat traditionele en cybercriminele activiteiten sterk met elkaar zijn verweven.

Cybercriminaliteit
Een groot deel van de netwerkleden wordt in politieregistraties gerelateerd aan cybercriminele activiteiten (n≥15). Daarin zijn drie varianten geconstateerd. Aanvankelijk is vooral sprake van verkoopfraude via Marktplaats. Leden uit het netwerk misbruiken Marktplaats om producten te verkopen die zij vervolgens niet leveren. De tweede door netwerkleden gehanteerde methode staat bekend als betaalverzoekfraude. Leden van het netwerk sturen dan vanaf een 'vals' of gespoofd (Marktplaats)account of telefoonnummer een betaallink van € 0,01 die leidt naar een vervalste bankomgeving. Verdachten krijgen daardoor inlognamen en wachtwoorden van de slachtoffers, waarna ze hun bankrekeningen plunderen. In een aantal gevallen wordt met de verkregen gegevens ook de bankier-app overgenomen, zodat netwerkleden zelf via hun telefoons overboekingen kunnen verrichten vanaf andermans bankrekening. Later richten de netwerkleden zich in toenemende mate op bankhelpdeskfraude. Vanaf een gespoofd telefoonnummer, waardoor het lijkt alsof netwerkleden bellen met het nummer van een bank, worden slachtoffers ervan overtuigd dat hun geld (door een hack) in gevaar is en dat zij hun geld direct over moeten maken naar 'een veilige rekening'. Die rekening is dan in het bezit van het criminele netwerk. Bij alle verschijningsvormen van cybercriminaliteit maakt het netwerk onder valse voorwendselen, tegen betaling en/of onder dwang gebruik van katvangers om het geld te innen.

Handel in verdovende middelen
Eén van de leden van het criminele netwerk bezit een groothandel. In de praktijk manifesteert hij zich als lachgaskoerier. Hoewel zij niet bij hem op de loonlijst staan, worden de sleutelfiguren en nog een aantal andere leden uit het netwerk regelmatig door de politie gesignaleerd als zij handelshoeveelheden lachgas in- en uitladen, vervoeren of aanwezig zijn bij feestjes waar aanzienlijke hoeveelheden

Tijdschrift voor Veiligheid 2023 (22) 2
doi: 10.5553/TvV/.000055

lachgas beschikbaar zijn. Opvallend is dat zij dan steeds auto's tot hun beschikking hebben die niet op hun eigen naam of op naam van het lachgasbedrijf staan, maar eigendom zijn van het bedrijf uit de parallelle witwascasus.
In de witwascasus bestaat van meet af aan het vermoeden dat de auto's die op naam staan van het bedrijf worden gebruikt voor drugshandel. Hoewel het ook om inkomsten uit cybercriminaliteit of lachgashandel kan gaan, dragen leden uit het criminele netwerk die in de auto's worden staandegehouden steevast schoudertasjes met grote stapels cash geld in coupures van € 50 bij zich. Opvallend is dat zij vooral 's avonds en 's nachts rijden in de omgeving van een specifieke stad in Noord-Nederland, maar ook regelmatig nachtelijke ritten maken richting de Randstad. Een van de auto's die op naam staat van het bedrijf wordt, schijnbaar in haast achtergelaten, aangetroffen door de politie in Amsterdam. Het valt dan op dat het verlichtingsvak van één van de achterlichten in de kofferbak is opengemaakt. Politiecollega's vermoeden dat het gaat om een geheime bergplaats voor drugs of grote sommen geld.
Bij de meeste staandehoudingen van netwerkleden worden overigens niet meer dan gebruikershoeveelheden drugs aangetroffen. Een uitzondering is dat de politie de eigenaar van het lachgasbedrijf staande houdt terwijl hij acht ponypacks cocaïne en ruim € 12.000 aan contanten bij zich heeft.
Naast het (mogelijk) drugsgerelateerde autogebruik zijn er nog een aantal andere indicaties voor drugscriminaliteit. Eén van de sleutelfiguren maakt op enig moment geld met de omschrijving 'drugs' over aan een ander sleutelfiguur, vanaf de balustrade van het appartement van een van de sleutelfiguren worden 's nachts (drugs)pakketjes naar beneden gegooid en daar ingeladen in een bestelbus en de sleutelfiguren onderhouden contacten met personen uit het drugscircuit. Het betreft bijvoorbeeld een lokale coffeeshophouder en een crimineel uit het zuiden van het land, bij wie recent voor miljoenen beslag is gelegd in verband met drugscriminaliteit en witwassen.

Geweld en wapenbezit
Ten minste zeven van de netwerkleden worden in verband gebracht met zware geweldsdelicten. Het betreft steevast incidenten waar (vuur)wapens mee gemoeid zijn. Politieregistraties doen vermoeden dat sprake is van conflicten in het criminele circuit, zoals een ripdeal, een gijzeling/bedreiging met vuurwapens, een kogelbrief en een schietpartij. Steeds zijn er geïdentificeerde sleutelfiguren betrokken. Ook tijdens een 'klapdag', waarbij de drie sleutelfiguren uit het criminele netwerk op heterdaad worden betrapt tijdens het plegen van bankhelpdeskfraude vanuit een speciaal daarvoor gehuurde verblijfplaats, worden vuurwapens aangetroffen.

Witwassen en financieel-economische criminaliteit
Tot slot zijn er aanwijzingen voor witwassen. Naast de grote sommen contant geld die de netwerkleden tijdens staandehoudingen bij zich dragen, beschikken ze ook over dure spullen. Het gaat dan meestal om schoenen, merkkleding en tassen van dure merken als Louboutin, Balenciaga en Louis Vuitton. Ter illustratie: in een van de politiemutaties wordt de waarde van de bij een staandehouding aangetroffen merkkleding geschat tussen de € 5.000 en € 10.000. Op basis van hun bekende

(legale) inkomen kunnen betrokkenen zich zulke dure spullen niet veroorloven. Volgens de FIU is ten aanzien van meerdere netwerkleden bovendien sprake van aan hen gerelateerde verdachte transacties.
Ook is geconstateerd dat het bedrijf uit de parallelle witwascasus luxe en voor de bedrijfsvoering onnodige auto's aanschaft ter waarde van ongeveer € 60.000. De omzet van het bedrijf is ontoereikend om die auto's te bekostigen. Hoewel dat niet betekent dat het bedrijf als dekmantelonderneming voor witwassen fungeert – dan zouden hoge omzet en winst de aanschaf van de auto's immers 'wit' mogelijk moeten maken – wijst het er wel op dat de auto's betaald zijn uit onbekend vermogen. Datzelfde geldt voor een aantal individuele netwerkleden. Op naam van gezinsleden die bijvoorbeeld slechts een bijstandsuitkering ontvangen, schaffen zij met onverklaarbare contante middelen auto's aan van tussen de € 10.000 en € 20.000.
Daarnaast is het bedrijf uit de witwascasus ogenschijnlijk betrokken bij economische delicten. De Belastingdienst heeft bijvoorbeeld aanwijzingen voor valsheid in geschrifte. Door middel van opzettelijk onjuiste (suppletie)aangiften omzetbelasting over het jaar 2019 lijkt sprake van een hogere omzetderving tijdens de coronacrisis. Hierdoor is ogenschijnlijk te veel TVL-subsidie[5] verkregen. Verder heeft de arbeidsinspectie zwartwerken en kinderarbeid geconstateerd in het bedrijf.

Slot: lokale en integrale kansen voor de aanpak van een 'cyber'crimineel netwerk

De casusbevindingen sluiten aan bij wat in de literatuur al is geschreven. Het 'cyber'criminele netwerk is lokaal verankerd en traditionele (criminele) activiteiten en cybercriminaliteit zijn sterk met elkaar verweven. Dit biedt niet alleen kansen voor een lokale aanpak, maar ook voor een integrale benadering. In de praktijk zijn er echter niet of nauwelijks voorbeelden bekend van een lokale, integrale casusaanpak in relatie tot cybercriminaliteit. In Noord-Nederland is daar in RIEC-verband nu ervaring mee opgedaan. Bij de aanpak van het 'cyber'criminele netwerk hebben namelijk een tweetal gemeenten, de Politie, de Belastingdienst en de Arbeidsinspectie samengewerkt. Hierna volgt per partner een korte opsomming van de ingezette interventiemogelijkheden.

Gemeenten:
- Ter verrijking van de integrale informatiepositie zijn BOA's ingezet om opmerkelijkheden rond netwerkleden en specifieke locaties te signaleren.
- Gemeentelijke toezichthouders hebben getoetst in hoeverre het bedrijf uit de witwascasus zich houdt aan lokale regelgeving. Er bleek sprake van illegale bewoning boven het bedrijfspand. Daarvoor is een last onder dwangsom opgelegd.
- In ten minste twee gevallen hebben familieleden een faciliterende rol gespeeld voor en/of geprofiteerd van de criminele verdiensten van netwerkleden. On-

5 TVL: Tegemoetkoming Vaste Lasten: dit was een regeling voor ondernemers met omzetverlies door coronamaatregelen.

Tijdschrift voor Veiligheid 2023 (22) 2
doi: 10.5553/TvV/.000055

danks hun bijstandsuitkering, hadden zij bijvoorbeeld dure voertuigen op hun naam staan. Bevindingen uit de casus zijn gebruikt om de bijstandsuitkeringen stop te zetten.

Politie:
- De politie heeft ingezet op een bestuursrechtelijke aanpak van het lachgasbedrijf in verband met het herhaaldelijk overtreden van regelgeving voor het wegtransport van gevaarlijke stoffen (ADR[6]). In dat verband zijn boetes opgelegd.
- Er is strafrechtelijk onderzoek verricht. De drie sleutelfiguren zijn uiteindelijk op heterdaad aangehouden en er is conservatoir beslag gelegd op geld en goederen.

Belastingdienst:
- De Belastingdienst heeft verschillende derdenonderzoeken verricht om inzicht te krijgen in de kopers en de financiering van de door netwerkleden gebruikte auto's. Op basis daarvan is geconstateerd dat auto's op naam van het bedrijf uit de parallelle witwascasus en auto's op naam van familieleden zijn bekostigd met onverklaarbaar en vermoedelijk crimineel verkregen vermogen. Netwerkleden waren bovendien betrokken bij de aanschaf ervan.
- Voor zover wederrechtelijk verkregen voordeel niet op een andere wijze is teruggevorderd (bijv. door beslag van de politie), zet de Belastingdienst in op het naheffen van de misgelopen belasting op het crimineel verkregen inkomen.
- De Belastingdienst heeft boekenonderzoek verricht bij het bedrijf uit de witwascasus en op basis daarvan aanwijzingen voor het opzettelijk doen van onjuiste aangiften omzetbelasting en het plegen van valsheid in geschrifte voor het verkrijgen van coronasteun.

Arbeidsinspectie:
- Uit toezicht van de Arbeidsinspectie is gebleken dat sprake was van zwartwerken en kinderarbeid. Daarvoor zijn boetes opgelegd.

Samenwerken loont

Onze conclusie luidt dat een lokale en integrale aanpak van een 'cyber'crimineel netwerk loont, omdat het leidt tot een rijkere informatiepositie en een groter palet aan interventiemogelijkheden dan een monodisciplinaire benadering. In dat kader sluiten we af met een drietal geleerde lessen:

1 Het is duidelijk dat de aanpak van een ogenschijnlijk 'cyber'crimineel netwerk zich niet hoeft te beperken tot het bestrijden van cybercriminele activiteiten. Zowel de casus als de literatuur laten zien dat cybercriminele netwerken zich veelal schuldig maken aan uiteenlopende delicten. De integrale benadering biedt kansen om niet de aanpak van een specifiek delict, maar de aanpak van het criminele netwerk centraal te stellen. Dat vergroot het interventiepotentieel: partners hoeven daardoor niet uitsluitend te putten uit interventies op het gebied van cybercriminaliteit, maar kunnen – voor zover de casus daar aanlei-

6 ADR: een Europese overeenkomst voor het internationale wegtransport van gevaarlijke stoffen.

ding toe geeft – hun volledige interventierepertoire aanwenden. Zo worden het netwerk en de netwerkleden zo veel mogelijk gedwarsboomd.

2 Het traditionele instrumentarium voor de aanpak van ondermijnende criminaliteit biedt handvatten voor de bestrijding van cybercriminaliteit. Denk bijvoorbeeld aan mogelijkheden om ervoor te zorgen dat misdaad niet loont door beslag te leggen, een uitkering stop te zetten of een naheffing op te leggen voor misgelopen belasting uit (crimineel) inkomen. Zowel bij traditionele delicten als bij cybercriminaliteit zijn zulke interventies toepasbaar. Koudwatervrees vanwege de 'aard en complexiteit' van cybercriminaliteit is dus onnodig.

3 Via het RIEC-samenwerkingsverband kan invulling worden gegeven aan de lokale en integrale aanpak van een 'cyber'crimineel netwerk. Dat biedt ook elders in het land kansen om de informatiepositie over en de aanpak van 'cyber'criminele netwerken te versterken.

Kortom: wees bij de aanpak van criminele jeugd(netwerken) alert op aanwijzingen voor cybercriminaliteit en werk vooral samen. Cybercriminaliteit mag niet lonen, samenwerken doet dat wel.

Literatuur

Aebi, M.F. & A. Linde (2010) Is there a crime drop in Western Europe? *European Journal on Criminal Policy and Research*, *16*(4), 251-277.

Farell, G., A. Tseloni, J. Mailley & N. Tilley (2011) The Crime Drop and the Security Hypothesis. *Journal of Research in Crime and Delinquency, 48*(2), 147-175.

Ferwerda, H. & T. van Ham (2010) *Problematische Jeugdgroepen in Nederland: Omvang, aard en politieproces beschreven*. Arnhem: Bureau Beke.

Jewkes, Y. & M. Yar (2008) Policing cybercrime in the twenty-first century. In: T. Newburn (Ed.), *Handbook of policing* (pp. 280-607). Collumpton, UK: Willan.

Kruisbergen, W.W., E.R. Leukfeldt, E.R. Kleemans & R.A. Roks (2018*) Georganiseerde criminaliteit en ICT. Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit*. Den Haag: WODC.

Leukfeldt, E.R. (2016) *Cybercriminal networks. Origin Growth and criminal capabilities*. Den Haag: Eleven International Publishing.

Leukfeldt, E.R. & R.A. Roks (2021). Cybercrime on the streets of the Netherlands? An exploration of the intersection of cybercrime and street crimes. *Deviant Behavior, 42*(11), 1458-1469.

Leukfeldt, E.R., E.R. Kleemans, E.W. Kruisbergen & R. Roks (2019) Criminal Networks in a Digitized World: On the Nexus of Borderless Opportunities and Local Embeddedness. Trends in Organized Crime. Doi: 10.1007/s12117-019-09366-7.

Leukfeldt, E.R., R. Spithoven & E. Misana-ter Huurne (2020) De lokale aanpak van cybercrime. Risicocommunicatie als antwoord op een grenzeloos vraagstuk. In: C. de Poot, E. Lievens, W. Stol & L. de Kimpe (red.), *Politie en cybercrime* (pp. 203-223). Den Bosch: Gompel & Svacina.

Roks, R.A., E.R. Leukfeldt & J.A. Densley (2021) The hybridization of street offending in the Netherlands. *The British Journal of Criminology, 61*(4), 926-945.

Veenstra, S., E.R. Leukfeldt & S. Boes (2013) Fighting Crime in a Digitized Society: The Criminal Justice System and Public-Private Partnerships in the Netherlands. In: W.Ph. Stol & J. Jansen (red.), *Cybercrime and the police*. Den Haag: Eleven International Publishing.
WODC (2021) *Monitor Jeugdcriminaliteit 2020*. Cahier.