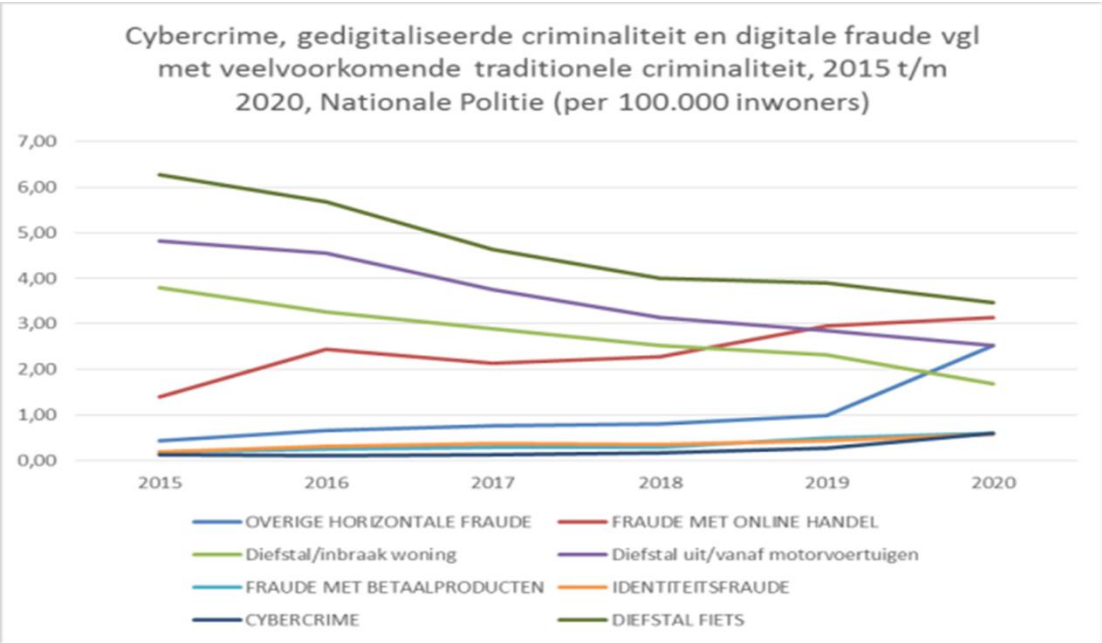
Datum:25 juni 2021
Auteurs: J.M. Bonnes, M. Chtatou, A. de Zwart A. Lensen, P. Hagenaars, L. Buis-Meulmeester A. de Jong, M. Andersen, L. Cox
Contactpersoon: J.M. Bonnes (OvJ), 06-48137027
Doel: informeren

1. Aanleiding
Het DB van het RVO besprak op 17 mei j.l. de aanpak van Online fraude. Afgesproken werd het onderwerp terug te laten komen op de vergadering van het RVO van 12 juli, vergezeld van een notitie inzake taken, rollen en verantwoordelijkheden rondom dit fenomeen.
Gelet op deze doelstelling geeft de notitie slechts enkele hoofdlijnen weer. In de concrete uitvoeringspraktijk zullen per casus exacte grenzen bepaald moeten worden.

2. Probleemstelling
De samenleving digitaliseert in hoog tempo, en dat geldt ook voor de criminaliteit. De opgaven voor handhaving en preventie veranderen drastisch doordat gedigitaliseerde criminaliteit explosief stijgt. Dat geldt voor gedigitaliseerde criminaliteit met openbare orde aspecten zoals opruiing via social media, maar ook voor cybercrime (hacking, ransomware) en voor financiële criminaliteit (online fraude). Onder online fraude verstaan we bijvoorbeeld Marktplaatsoplichting, Whatsapp-fraude en Bankhelpdeskfraude. De vorm waarin de criminele handelingen plaatsvinden verandert snel, maar de kern is dat er op grote schaal slachtoffers worden gemaakt door online handelingen met een financieel motief.

We zien een halvering van HICdelicten en een verdubbeling van onlinedelicten waarbij slachtoffers heel veel geld kwijt raken, bv hun pensioenspaarpot. De impact op slachtoffers is groot. We voelen een hoge urgentie om in deze snelle ontwikkeling in het criminaliteitsbeeld 'het been bij te trekken'.

Online fraude is inmiddels veel voorkomende criminaliteit, waarvan even vaak aangifte wordt gedaan als van auto-inbraak of fietsendiefstal. Traditionele vormen van criminaliteit, waaronder ook woninginbraken en overvallen, vertonen al jaren een dalende lijn, terwijl de online fraude jaar op jaar sterk toeneemt.



Voor een deel zal de daling van offline delicten een gevolg zijn van de COVID-crisis, maar niet helemaal. Al is het maar omdat de daling al inzette ver vóór COVID.
COVID heeft wel gezorgd voor een forse versnelling in de stijging van digitale delicten.
Daarnaast is aannemelijk dat de stijging van de online fraude zal doorzetten, omdat de schaal en de geringe pakkans dit een aantrekkelijk verdienmodel voor criminelen maken.

Tegenover die zich ontwikkelende criminaliteit heeft de overheid nog onvoldoende weerwoord gegeven. Er is een achterstand in aanpak.
De aanpak wordt nog bepaald door gewoonte, en is nog niet afgestemd op de nieuwe online wereld: "*Zo doen we dit nu eenmaal. We pakken criminaliteit aan met opsporing en met een bepaalde manier van opsporen*."
In de huidige aanpak komt online fraude vaak bij de afdelingen van de politie terecht inzake Veel Voorkomende Criminaliteit. Daarna wordt gerechercheerd vanuit de aangifte. Deze leidt naar de bankrekening waar het gefraudeerde geld op is gestort. Verder dan degene die zijn bankrekening ter beschikking heeft gesteld, de geldezel, komt men aldus vaak niet. En hoe waardevol het ook is om een geldezel aan te spreken en indien nodig hulp te bieden (vaak zijn geldezels naast dader zelf ook slachtoffer, naar onze ervaring zijn het vaak kwetsbare mensen), het is een druppel op een gloeiende plaat. Via social media worden geldezels in grote aantallen geronseld. En er gebeurt te weinig om online fraude ècht aan te pakken.

Men kan zich de vraag stellen of het erg is dat de huidige aanpak ontoereikend is. Wij vinden van wel.
Allereerst uit rechtsstatelijke redenen: het is online oplichting en diefstal op grote schaal.
Maar ook omdat we een grote verwevenheid zien tussen criminelen uit de online en de offline wereld. Eventuele gewelddadige conflicten tussen hen vinden plaats in het publieke domein, met alle denkbare gevolgen van dien. Zo zijn er escalaties die voorkomen uit conflicten (drillrap) op het internet, maar ook de berovingen bij cash out momenten. In een zeer recent onderzoek van de Rotterdamse politie worden twee Haagse mannen van 17 en 18 jaar ervan verdacht meer dan € 100.000 met Whatsapp-fraude te hebben "verdiend". In hun woning is naast cash geld een vuurwapen aangetroffen.
Daarnaast zien we dat vele verdachten van online fraude zich óók bezig houden met offline vormen. Dit is voor hen een verdienste erbij.
Ten slotte tast deze vorm van criminaliteit het vertrouwen aan in de aanpak aan van politie en OM, maar ook het vertrouwen in de financiële diensten. Zo zijn er geldezels die aan politie en OM vertellen dat zij eerst slachtoffer waren van online fraude, maar "*De politie deed helemaal niets met mijn aangiftes, dus blijkbaar vinden jullie het wel ok.*" Kwalijk, maar helaas soms praktijk.

Wat ons betreft moet online fraude worden aangepakt. Maar de vraag is wat er anders moet worden gedaan en wie dit zal doen. Ook is de vraag hoe de beweging op gang wordt gebracht om dit daadwerkelijk anders te gaan doen.

1. *Onze stelling is dat een stevige impuls op lokaal niveau nodig is.* Met zo'n stevige impuls kan de opgelopen achterstand worden geanalyseerd, opgepakt en weggewerkt op een creatieve en integrale manier. Dit is nodig omdat vanwege de achterstand in aanpak op veel vragen nog geen antwoord valt te geven. Zo is nog niet duidelijk wat de beste aanpak is en wie die moet toepassen. Wel is duidelijk op basis van de beginnende experimentele aanpak rond geldezels in onze regio, dat een stevige impuls werkt. Deze impuls zou tijdelijk moeten zijn, incrementeel werken (al doende leren), en na enige tijd geëvalueerd moeten worden.'
2. *Onze tweede stelling is dat de stevige impuls zowel op landelijk niveau (bijvoorbeeld door landelijke analyses) moet plaatsvinden, maar daarnaast ook op lokaal niveau*. Dáár, op het lokale grondgebied, wonen zowel de daders als de slachtoffers van online fraude Zo blijken uit cijfers van het Landelijke Meldpunt Internet Oplichting (LMIO) alsook uit die van het landelijke project tot aanpak van Vriend-in-nood fraude (VINF), dat onze regio in 2020 een landelijke hotspot van geldezels was.
   Het is dus nadrukkelijk niet zo dat de lokale aanpak kan of moet wachten op de landelijke. Beide ontwikkelingen moeten elkaar versterken. Landelijk is er van alles in ontwikkeling of reeds ontwikkeld (zoals het LMIO en VINF), maar die landelijke impuls is onvoldoende effectief als er niet ook een lokale impuls plaatsvindt.

3. *Onze derde stelling is dat op lokaal niveau samenwerking tussen OM, politie en gemeenten noodzakelijk is.* In de kern komt het erop neer dat we langs de lijn van de ontwikkeling in het criminaliteitsbeeld, waarbij zowel aan de slachtoffer- als daderkant vele inwoners betrokken zijn, gezamenlijk op willen trekken en we daar elkaar en elkaars netwerken ook voor nodig hebben. Nodig uit het oogpunt van weerbaarder maken van burgers en bedrijven, het voorkomen van daderschap maar ook uit het oogpunt van slachtofferbescherming. In een creatieve expert-sessie is begin juni 2021 verkend wat die effectieve aanpak op lokaal niveau *inhoudelijk* zou kunnen inhouden. Die sessie verliep langs vier lijnen: daders – slachtoffers – aanpak – communicatie. Hieronder voorbeelden van daar benoemde acties die in samenwerking tussen politie, OM en gemeenten zouden moeten worden opgepakt.

Een greep uit de opbrengst van de Rotterdamse creatieve sessie begin juni 2021:

- Uit politie-onderzoek blijkt: 50% money mules wordt offline geronseld => schakel analisten in om uit alle processen-verbaal *fysieke lokaties / hotspots* te destilleren.
- Richt nuttig *slachtofferloket* in, waar aangifte gedaan kan worden maar ook handelingsperspectief wordt gegeven (de weg naar concrete hulp) => schakel anderen in om uit aangiftes maar ook uit informatie van de Fraudehelpdesk en van SlachtofferHulp Nederland te destilleren waar slachtoffers concreet behoefte aan hebben.
- Investeer in *digitale opvoeding*. Kies voor peers bij de boodschap. Zowel qua 'hoe bescherm je jezelf' als 'de strafbaarheid doorhebben', want jongeren weten dat vaak niet => schakel politie en justitie in om de strafbaarheidsboodschap goed over te brengen, maar faciliteer dat als gemeente.
- Onderneem de actie '*Lever je cyberwapen in*', om zodoende een betere informatiepositie op te bouwen => samenwerking politie, OM en gemeente.
- Uit politie-onderzoek blijkt: Tussen fraude en cashing zit max 30 min. Ga in overleg met *banken* hoe hierop te handelen. Ook hier zijn lokale initiatieven mogelijk.

De drie stellingen bijeen leiden tot een pleidooi voor een tijdelijke lokale stevige impuls door politie, Openbaar Ministerie en gemeenten gezamenlijk.

NB1. Dit náást een landelijke extra impuls, die evenzeer nodig is en waarop door politie en OM eveneens wordt ingezet.
NB2. En ook onverlet de bredere digitale transformatie die nodig is om adequaat op te treden op het bredere terrein van digitaliserende criminaliteit.

Aan de leden van het RVO wordt gevraagd:

- Kennis te nemen van de hierna genoemde taken, rollen en verantwoordelijkheden rond online fraude.
- Onderschrijven urgentie die voortvloeit uit het criminaliteitsbeeld om extra prio te geven aan online fraude.
- In te stemmen met het oprichten van een werkgroep 'aanpak online fraude' met vertegenwoordigers vanuit politie, OM, VAR en gemeentes. De werkgroep zal de mogelijkheden voor een gezamenlijke aanpak van online fraude verder onderzoeken en tijdens het volgende RVO een concreet voorstel voor een gezamenlijke aanpak voorleggen.

Maar alvorens eventueel tot een tijdelijke samenwerking te komen, is het wenselijk om de rollen, taken en verantwoordelijkheden van deze drie partijen expliciet te maken. Hieronder wordt dit per partij op hoofdlijnen geschetst. In de slotparagraaf wordt aan de hand van een schema toegelicht dat de meest effectieve aanpak plaatsvindt vanuit ieders rol en verantwoordelijkheid.

3. Rollen, taken en verantwoordelijkheden Openbaar Ministerie

a. Wettelijke taak en verantwoordelijkheid

Het OM is belast met de strafrechtelijke handhaving van de rechtsorde (art. 124 Wet RO). Deze algemene verantwoordelijkheid leidt tot de taak van het doen opsporen en vervolgen van alle strafbare feiten en het doen uitvoeren van alle strafvonnissen.

- Online fraude is een strafbaar feit, namelijk oplichting. Dus valt dit binnen de verantwoordelijkheid van het OM.

b. Rollen

Het OM is bevoegd gezag over de opsporing, en heeft daarmee ook een veto bij het delen van opsporingsinformatie voor zover dit het onderzoek kan raken. Het OM is tevens eigenaar van justitiële informatie. De taak van de OvJ is wettelijk gezien het nemen van strafvorderlijke beslissingen in een onderzoek.
De rol van het OM is dus gekoppeld aan het begrip "opsporing". Het is de bedoeling van de wetgever dat hieronder ook valt de fase van misdaadanalyse (intel). Ook is de moderne interpretatie van "opsporing" dat hieronder ook verstoring kan vallen, dat wil zeggen: inzet van informatie of middelen om het plegen van strafbare feiten tegen te houden. En ook wil het OM bijdragen aan preventie. Zodat het zich vervolgens kan richten op de grotere criminelen, en daarmee een hefboom effect neerzetten (vanuit schaalbaarheidsperspectief) en zo bijdragen aan legitieme rol in een veilige samenleving.

- Toegepast op online fraude kan dit bijvoorbeeld inhouden:
  - opdracht geven aan de politie om op basis van informatie uit politiesystemen relevante analyses te maken t.b.v. de opsporing, bijvoorbeeld wat verklaren aangehouden geldezels over ronselaars;
  - informatie over de locatie waar de geldezels geronseld worden verstrekken aan bijv. de gemeente (denk aan locaties waar beschermd wonen plaatsvindt of aan "een pleintje op Zuid"), zodat deze adequate interventies kan uitvoeren;
  - toestemming geven om informatie uit aangiftes te delen met de gemeente, zodat er passende slachtofferhulp kan worden geboden;
  - bij de afdoening van daders volop hulpverlening betrekken à la de aanpak in de Zorg- en Veiligheidshuizen.
- Hoewel dus de rol van het OM van belang kan zijn voor zowel daders, slachtoffers, aanpak van de criminaliteit, als communicatie, ligt het zwaartepunt bij de aanpak van gepleegde daden.

4. Rollen, taken en verantwoordelijkheden politie

a. Wettelijke taak en verantwoordelijkheid

De politie heeft tot taak in ondergeschiktheid aan het bevoegd gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven. (art. 3 Politiewet).
De politie heeft een taak rond de handhaving van de openbare orde en rond de hulpverlening, dit gebeurt onder gezag van de burgemeester.
Daarnaast heeft de politie een taak rond de opsporing van strafbare feiten ("suspect attribution"), de verstoring, slachtoffernotificatie en preventie (het zgn. ballonnen-model). Bij online delicten is inmiddels gebleken dat louter focus op opsporing onvoldoende effectief is.

b. Rollen

De politie heeft een rol bij de opsporing, bij de hulpverlening, bij slachtoffer- en bij daderpreventie. Overkoepelend hieraan is een analyserol (informatie omzetten in mogelijke acties) en een communicatierol. Met name communicatie zal immers behulpzaam zijn bij preventie.

- Toegepast op online fraude kan dit bijvoorbeeld inhouden:

- analyseer opsporingsinformatie op diverse manieren om zodoende een opsporings- preventie- en/of verstoringsaanpak te kunnen voeden;
- richt een loket in waar anoniem "cyberwapens" kunnen worden ingeleverd: deel de daaruit komende informatie met relevante partijen;
- zorg dat de wijkagenten van wijken waar veel daders komen, hun ogen en oren wijd open houden voor de manieren waarop zij handelen.

- De rol van de politie ziet zowel op dader-aanpak, als op verstoring, als op hulpverlening en preventie en communicatie.

5. Rollen, taken en verantwoordelijkheden gemeenten

a. Wettelijke taak en verantwoordelijkheid

De burgemeester is verantwoordelijk voor de openbare orde en veiligheid van de gemeente en vervult de rol van 'burgervader'. Voor de bestrijding van criminaliteit, en daarmee online fraude, is de gemeente daarom gebonden aan de bevoegdheden van de burgemeester op het gebied van openbare orde en veiligheid.

In de aanpak op ondermijnende criminaliteit wordt er een beroep gedaan op deze bevoegdheden om barrières op te werpen en daarmee daderschap en faciliteerders aan te pakken en hun processen te verstoren. De mogelijkheid om dit ook toe te passen in een aanpak op gedigitaliseerde criminaliteit en specifiek online fraude wordt onderzocht.
Voor een aanpak op het stimuleren van digitale weerbaarheid van burgers en ondernemers kan vooral worden gekeken naar de rol van burgervader. Veel gemeenten zetten hier al op in met online campagnes en projecten.

b. Rollen

De verantwoordelijkheid voor het veiligheidsbeleid op lokaal niveau ligt bij de gemeente.
De gemeente heeft de regierol bij het ontwikkelen van het integraal veiligheidsbeleid. Ze zorgt voor afstemming met (veiligheids)partners als politie en openbaar ministerie. Afhankelijk van het onderwerp worden ook vele andere partijen betrokken, zoals scholen, sociale wijkteams, ondernemers en de brandweer. Daarnaast voert de gemeente de regie over de verschillende maatregelen die met de partners zijn afgesproken. Dit wordt veelal vastgelegd in een uitvoeringsplan.

Inmiddels hebben de meeste gemeenten binnen de eenheid Rotterdam, cybercriminaliteit in veiligheidsbeleid en uitvoeringsplannen opgenomen. Bij de Gemeente Rotterdam is dit bijvoorbeeld onderdeel van het collegeprogramma en meerjaren veiligheidsprogramma Veilig@Rotterdam. Hierbij gaat het veelal specifiek om cybercriminaliteit. Andere vormen van gedigitaliseerde criminaliteit zijn hierin vooralsnog veelal niet expliciet opgenomen.

- Toegepast op online fraude (naast en soms als onderdeel van cybercriminaliteit) zien gemeenten echter wel een rol voor zichzelf bij:
  - Het beter zicht krijgen op daders, slachtoffers en fenomenen en daar samen met veiligheidspartners een aanpak op ontwikkelen. Bijvoorbeeld door een aanpak gericht op daders en faciliteerders door het opwerken van barrières.
  - Het versterken van de digitale awareness en weerbaarheid van burgers en bedrijven in de regio. Hierbij aandacht voor het voorkomen van daderschap en slachtofferschap.

Ondersteuning door VAR; campagnes

De VeiligheidsAlliantie regio Rotterdam (VAR) ondersteunt gemeenten door het aanbieden en ontwikkelen van aanbod voor gemeenten, waarmee zij hun digitale weerbaarheid (en die van hun burgers en ondernemers) kunnen vergroten.

- Toegepast op online fraude (naast en soms als onderdeel van cybercriminaliteit) houdt dit bijvoorbeeld in:
  - de mediacampagne Echt Nep
  - het project HackShield (doelgroep 8-12 jaar) en
  - het project Cyberbuddies (doelgroep ondernemers).
- Ook de Gemeente Rotterdam is betrokken bij verschillende van deze activiteiten en deelt graag ervaringen met kleinere gemeenten in de regio.

6. Conclusie

Hoewel er duidelijke verschillen zijn in de rollen, taken en verantwoordelijkheden tussen OM, politie en gemeenten, kan een fenomeen als online fraude pas effectief worden aangepakt in samenwerking. Dit is een strafbaar feit en daarom zijn politie en justitie als eerste aan zet. Maar daar achteraan komt de lokale overheid, omdat deze belangrijke en effectieve acties kan ondernemen. *In de tijd gezien vanuit het crimescript,* komt de lokale overheid zelfs als eerste maatschappelijke verdedigingslijn, gezien vanuit haar preventieve rol.

Met enkel repressie van daders redden we het niet, samenwerking met andere partijen is nodig om het benodigde maatschappelijk effect te bereiken. De samenleving verdient een effectieve overheid, ook rond dit fenomeen.

	OM	**Politie**	**Gemeenten/ VAR**
Daders	X	X	X (bijv. schuld hulpverlening ter voorkoming recidive)
Daderpreventie	X (bijv. voorlichting over strafbaarheid geven)	X	X
Slachtoffers	X	X	X
Slachtofferpreventie	X (bijv. opdracht geven tot verstoring, bijv. neerhalen frauduleuze websites)	X	X
Communicatie	x	X	X
Strategische communicatie	X	X	X
Ongoing campagne	X	X	X
Aanpak	X	X	X