Betreft : Aanpak gedigitaliseerde criminaliteit
Aan : RVO
d.d. : 20 juni 2022
Bijlagen: 1. Cyberbeeld
2. Actualisatie realisatie

Aanleiding:

Deze notitie is tot stand gekomen binnen het samenwerkingsverband van de VAR, het Openbaar Ministerie, de gemeente Rotterdam en de Politie. Ter ondersteuning en informatie zijn bij deze memo het cyberbeeld 2021 en een actualisatie van de realisatie tot nu toe bijgevoegd.

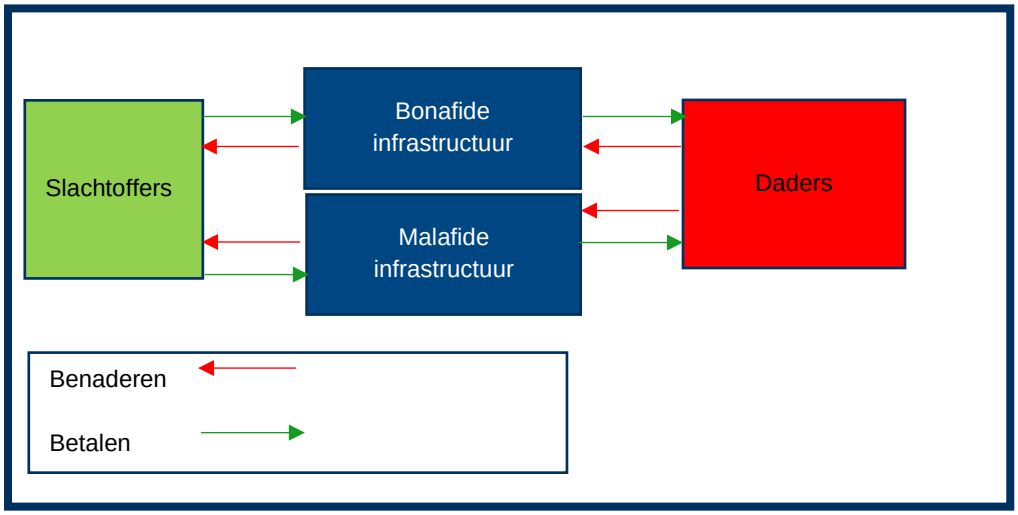
In de notitie aanpak veelvoorkomende digitale criminaliteit vastgesteld d.d.22 november 2021 in het RVO is vastgesteld dat de aanpak zich richt op zes pijlers. Te weten:

1. Commitment op gezamenlijk uitvoeren.
2. Een gedeelde visie.
3. Borging van de strategische visie.
4. Betrouwbaar cyberbeeld.
5. Aansluiten bij regionale en landelijke initiatieven.
6. Verminderen slachteroffer- en daderschap.

Deze memo beoogt een gedeelde visie (2) te realiseren en een aanzet te geven tot de borging (3) daarvan. Daarnaast is er een bijlage opgenomen waarin een overzicht geboden wordt van de ontwikkelingen/activiteiten tot nu toe.
Eerst zal een vereenvoudigde weergave worden geduid van het criminele proces zoals zich dat voordoet, aangevuld met de diverse rollen in het criminele proces. Vervolgens wordt er op basis van dit proces een onderscheid gemaakt tussen de kortetermijnvisie en de langetermijnvisie, om vervolgens af te sluiten met concreet gevraagde besluitvorming.

De scope zoals destijds verwoord in eerdergenoemde notitie is onveranderd voor wat betreft de delict soorten waar deze memo over gaat.

Het criminele proces:
Als we naar de crimescripts van de diverse vormen van “online fraude” kijken hebben ze allen een aantal overeenkomsten in het criminele proces. De actoren en factoren kunnen daarbij per delict soort echter verschillen. Waar bijvoorbeeld bank helpdesk fraude zich met name in de bancaire omgeving afspeelt, kan een andersoortig delict zich afspelen in de context van datingapps. Het verschil in context tussen zakelijke financiële dienstverlening en persoonlijke dienstverlening maakt dat er op andere belevingen van de slachtoffers wordt ingespeeld. De dader doet zich in het ene geval voor als bankmedewerker die op basis van vertrouwen het slachtoffer “behoedt” voor verlies van zijn spaargeld en in het andere geval is de dader een dame die inspeelt op de affectieve gevoelens van het slachtoffer en deze overhaalt om even tijdelijk “financieel bij te springen”.



Overeenkomsten
Verdachten hebben altijd een infrastructuur nodig om het delict mogelijk te maken. Deze infrastructuur wordt zowel gebruikt om contact te maken met de potentiële slachtoffers, hen te beïnvloeden, maar ook om de buit te ontvangen. Dit kunnen zowel bonafide als malafide infrastructuren zijn.
Voorbeelden van bonafide structuren zijn webhosts, telecomaanbieders, social media, bankrekeningen, netwerk van geldautomaten et cetera.
Voorbeelden van malafide structuren zijn darkwebhosts, illegale wedkantoren, webstressers, illegale datahandelaren, moneymules et cetera.

Tevens zien we in het crimescript vijf (5) rollen structureel terugkeren.

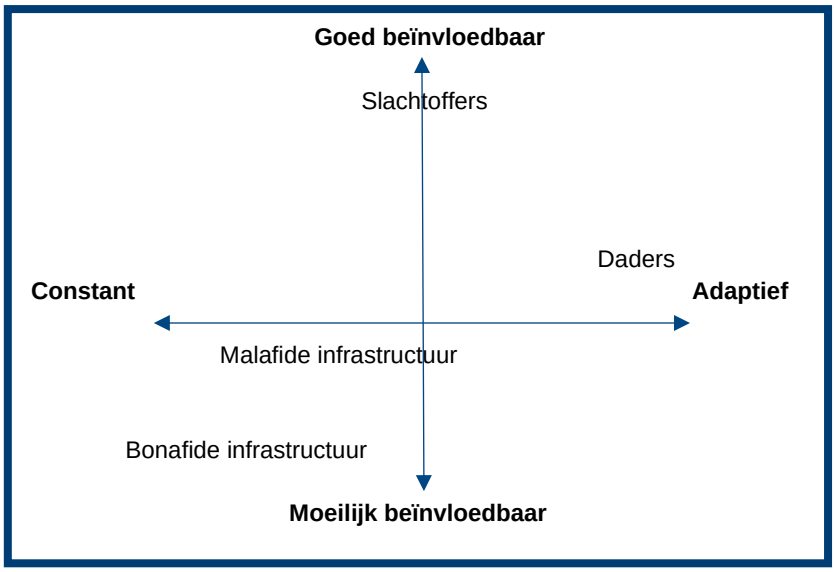
1. De geldezel die zijn rekening en bankpas ter beschikking stelt. Vaak een jongere of sociaal zwakkere, soms met mulitproblematiek, lokaal verankerd in de wijken.
2. De ronselaar van de geldezel. Meestal adolescent en een overlap met andere netwerken zoals uithalers, overlastgevende of criminele jeugdgroepen in dezelfde wijken als de geldezels.
3. De moderators die de feitelijke digitale “gesprekken” met de slachtoffers voeren. (jong)Volwassenen die groeiende zijn op de criminele ladder.
4. De pinners die de cash-out verzorgen. Overlap met de derde groep maar soms ook zelfstandig radar in het netwerk.
5. De organisatoren, als regisseur van het criminele proces en ook het sterkst in georganiseerd verband.

De vierde en de vijfde rol zijn bij uitstek ter competentie van een strafrechtelijke aanpak. Maar de eerste twee rollen en soms ook de derde vragen een veel bredere integrale aanpak waarbij ook de gemeenten, het zorg- en veiligheidshuis, hulpverlening, reclassering met elkaar een nieuw perspectief aan daders dienen te ontwikkelen.

Perspectieven:
Adaptief en beïnvloedbaar.
Het fenomeen veelvoorkomende digitale criminaliteit groeide de afgelopen jaren in omvang met 10-tallen procenten. Er is vooralsnog geen aanleiding om te veronderstellen dat deze trend zal worden verbroken. Het gaat in deze cijfers alleen over de delicten die daadwerkelijk zijn aangegeven. Vermoed wordt dat het darknumber significant is en de ware omvang nog vele malen groter. De wijze waarop de delicten worden uitgevoerd verschilt van elkaar, maar we zien wel dat er steeds nieuwe gaten in de markt worden gevonden en dat de daders in hoge mate adaptief zijn. Daar waar helpdeksfraude voorheen uit naam van de aanbieder (Microsoft – banken) werd gepleegd, zien we dit nu verschuiven naar uit naam van betrouwbare overheidsinstituties. (belastingdienst – politie). De noodzaak tot dit adaptieve gedrag komt voort uit het feit dat ook slachtoffers adaptief zijn en steeds weer leren, al dan niet met behulp van de overheid, wat onveilig gedrag is.
Tevens laten onze ervaringen van de afgelopen jaren zien dat de overheid in staat is zowel potentiële slachtoffer te beïnvloeden, als daders aan te pakken. Indien voorwaarden als urgentie, operationele capaciteit, kennis van het delict en financiering zijn geregeld, kan met relatief geringe inspanning worden ingespeeld op situatie. Enerzijds door slimme campagnes en anderzijds door intensieve samenwerking in de veiligheidsketen. Middelen

en bevoegdheden zijn voorhanden om interventies te plegen. Er is daadwerkelijk een handelingsperspectief op zowel slachtoffers als verdachten.

Constant en moeilijk beïnvloedbaar.
De constante in het geheel is dat men de beschikbare infrastructuur zoals social media, telefoon, digitaal betalingsverkeer, blijft gebruiken als middel om het feit mogelijk te maken. Deze infrastructuur is over het algemeen op nationaal of internationaal niveau georganiseerd. Veiligheid is zelden het primaire doel van het onderliggende businessmodel en er zijn zeer beperkte bevoegdheden ten aanzien van de bonafide infrastructuur vanuit de veiligheidsketen. Het beïnvloeden van de malafide infrastructuur is wel mogelijk, maar ook complex in verband met de hoge mate waarin deze verhuld wordt. Daarbij komt dat een klein deel van de slachtoffers bereikt wordt via de malafide infrastructuur. De meesten worden bereikt via de, in de ogen van de slachtoffers, betrouwbare kanalen zoals facebook, whatsapp, sms, eigen telefoon, marktplaats, websites et cetera.



Vanuit dit diagram en voorstaande kunnen we meerdere conclusies trekken:

1. Daders zijn aan te pakken, maar veranderen van tactiek naar mate daar behoefte aan is. Dit vraagt om een adequaat cyberbeeld zodat er geanticipeerd kan worden.
2. Slachtoffers zijn goed beïnvloedbaar, maar pas nadat we kennis hebben genomen van hoe daders acteren.
3. Malafide infrastructuur is aan te pakken, maar kost in verhouding veel capaciteit, is gericht op een kleine doelgroep. Tevens is malafide infrastructuur adaptiever dan de bonafide infrastructuur.
4. Bonafide infrastructuur bereikt de grootste doelgroep, maar is tevens het moeilijkst te beïnvloeden.

Overheidsactoren:
Verschillende overheidsinstanties hebben van nature in hun taakstelling een verbinding met dit fenomeen. Politie en Openbaar Ministerie, Rechterlijke Macht, hebben verdachten op te sporen, aan te houden en te berechten. Reclassering heeft tot taak een duurzame stopreactie te bewerkstelligen bij veroordeelde verdachten. Slachtofferhulp Nederland ondersteunt slachtoffers bij het dempen van de negatieve effecten van het slachtofferschap. Gemeenten lichten hun inwoners en ondernemers voor, voorkomen slachtofferschap en regisseren zorg voor sociaal psychologische problematiek bij slachtoffers en daders. Samengevat, voor zowel de slachtoffers als de daders zijn er logische actoren in het veiligheidsdomein met een verantwoordelijkheid. Het eigenaarschap van de aanpak van daders en zorg voor (toekomstige) slachtoffers is belegd in de taakstelling van de diverse overheidsorganisaties.

Dit eigenaarschap ontbreekt echter bij de beïnvloeding en aanpak van bonafide infrastructuren. Alle actoren hebben wel argumenten ter overtuiging aan te leveren, maar geen van hen heeft op zichzelf daadwerkelijk invloed of de mogelijkheid tot een interventie. Deze bevoegdheid is deels aanwezig bij een aantal geïnstitutionaliseerde toezichthouders zoals bijvoorbeeld ACM. Er is geen sprake van een gecoördineerde invloed vanuit de overheid op aanbieders van de infrastructuur die wordt gebruikt bij het plegen van bedoelde misdrijven. Toekomstige Europese wetgeving zal meer handvaten, maar ook verplichtingen geven aan toe is

echter nu nog geen werkelijkheid. Hoe dit feitelijk vorm zal krijgen en wat de effecten daarvan zullen zijn, is nu nog onvoldoende te duiden.

Visie:
De visie voor de aanpak van veelvoorkomende gedigitaliseerde criminaliteit heeft een korte- en een langetermijn perspectief. Beide perspectieven hebben een eigen dynamiek, maar ook eigen opbrengsten.

Wij werken slagvaardig samen aan de bestrijding van gedigitaliseerde criminaliteit door de weerbaarheid van slachtoffers te vergroten, daders aan te pakken en duurzame barrières op te werpen.

Korte termijn:

Verminderen van dader en slachtofferschap door de toename (golf) van veelvoorkomende gedigitaliseerde criminaliteit te dempen.

Voor de korte termijn is het belangrijk dat we de toename (golf) van veelvoorkomende gedigitaliseerde criminaliteit dempen. Dit dempende effect kan worden bereikt door in te zetten op het beïnvloeden van daders en slachtoffers. Dit kan met de logische samenwerkingspartners worden bereikt. Dit zal echter tot een schommelbeweging leiden in het criminaliteitsbeeld doordat hier in hoge mate sprake is van adaptief vermogen bij de daders. De partners in de veiligheidsketen dienen nauw met elkaar samen te werken om te komen tot preventie, slachtoffernotificatie, opsporen van daders en (technisch) verstoren. Afhankelijk van waar op gericht wordt, verschillen de coalities die moeten worden gesloten. Het ligt voor de hand dat politie en Justitie aanhoudend zich richten op het opsporen van verdachten en dat de reclassering recidive tracht tegen te gaan. Het ligt tevens voor de hand dat politie, justitie en gemeenten (jeugd en jongerenwerk) zich bijvoorbeeld met elkaar richten op jongeren die zich lenen als moneymule. Hiervoor is nodig dat alle organisaties binnen de veiligheidsketen de aanpak van veelvoorkomende online criminaliteit de komende jaren opnemen in hun planvorming en voldoende prioriteit geven aan de uitvoering daarvan. Het gaat hier meer over het adequaat reageren vanuit de eigen taakstelling op de crimeshift van offline naar online en niet zozeer om iets nieuws buiten de eigen taakstelling.

Lange termijn:

Verminderen van dader- en slachtofferschap door structurele interventies binnen de faciliterende bonafide infrastructuur.

Voor de lange termijn dienen we ons te richten op het beïnvloeden van de infrastructuur. De aanbieders hiervan dienen vanuit maatschappelijk verantwoord ondernemen, beschermingsmaatregelen voor hun klanten te nemen en drempels op te werpen voor daders. Het is niet vanzelfsprekend dat deze marktpartijen zelf hier hun verantwoordelijkheid in nemen. Juist hier is het van belang dat we als partners in het veiligheidsdomein samen optrekken en met elkaar die vuist maken en via verleiden, overtuigen en drangvarianten hen te bewegen mede-eigenaar te worden van dit veiligheidsvraagstuk. Hun rol moet wijzigen van facilitator naar poortwachter. Het zit in geen van de organisaties in de veiligheidsketen in hun primaire taakstelling en dus vraagt dit om een vernieuwende gezamenlijke strategie om dit ook daadwerkelijk te realiseren. Als je alleen bankrekeningen kan openen met een geverifieerde identiteit, je als minderjarige niet in staat bent om duizenden euro's per week te pinnen, als verdachte social media accounts snel worden verwijderd en vanaf die IP-adressen geen nieuwe accounts meer kunnen worden aangemaakt voor een bepaalde periode, prepaid telefoonnummers zonder identificerende gegevens niet meer bestaan et cetera, dan worden er structurele barrières in de infrastructuur aangebracht die een duurzame bijdrage leveren aan het verminderen van gedigitaliseerde criminaliteit.

Hoe:
Op dit moment is er sprake van een stuurgroep geleid door de regionaal portefeuillehouder cybercrime, namens het RVO. Onder verantwoordelijkheid van deze stuurgroep is een integrale werkgroep actief die zich tot op heden vooral heeft gericht op laaghangend fruit dat zich met name in het slachtoffer- en daderdomein bevindt. Een bijlage van de realisatie tot nu toe treft u bij deze memo aan.

Korte termijn:
Voor de korte termijn is het dempen van de golf het belangrijkste doel. Dit kan goed worden overgelaten aan de voornoemde stuur- en werkgroep waarin projecten zijn opgestart en nieuwe zullen worden opgestart. Deze geven invulling aan pijler 6, verlagen van dader- en slachtofferschap. Het doel van de stuurgroep zou moeten zijn deze werkwijze te laten borgen in de staande organisaties door middel van opnemen in (meer)jaren beleidsplannen en het formaliseren van samenwerkingsactiviteiten voor de duur dat dit op basis van het cyberbeeld nodig is.

Lange termijn:
O.l.v. de stuurgroep dient een stakeholdersanalyse van de meest relevante aanbieders van de infrastructuur te worden gerealiseerd. Per stakeholder zullen activiteiten moeten worden ontwikkeld om deze aan boord te krijgen in een Publiek-Private samenwerking om te komen tot het structureel opwerpen van barrières. Daarbij is dit niet per se alleen de verantwoordelijkheid van de partners binnen het verzorgingsgebied van uw RVO. Het vraagt om het aangaan van coalities met landelijke organisaties. Te groot voor het servet en te klein voor het tafellaken dient hierbij te worden doorbroken. Daarbij zou het noodzakelijk kunnen zijn om bestuurlijke druk uit te oefenen om beweging te realiseren die in gezamenlijkheid leiden tot voldoende hefboomwerking om aanbieders van de infrastructuur mede-eigenaar te maken. Hierbij is het van belang dat we uit pijler 5 aansluiten bij- of initiëren van landelijke initiatieven. Verwacht wordt dat dit een arbeidsintensief proces is, maar dat de uiteindelijke opbrengsten een structurele bijdrage leveren aan het verminderen van zowel slachtoffer- als daderschap.

Concreet:
Er dient een stakeholders analyse te worden gemaakt van aanbieders van de bonafide infrastructuur. Op basis van deze analyse dient per stakeholder een beïnvloeding strategie (in combinatie met reeds lopende initiatieven) te worden ontwikkeld en ingezet waardoor zij in een publiek-private samenwerking van facilitator naar poortwachter zullen ontwikkelen. Daarbij dient nog te worden gezocht naar capaciteit en inbedding van deze capaciteit om dit mogelijk te maken.

Zowel de korte termijn als de lange termijn dragen bij aan het uiteindelijke doel benoemd in pijler 6, terugdringen van aantallen slachtoffers en daders.

Gevraagde besluiten:
Aan de leden van het RVO wordt gevraagd:

- De visie ‘Aanpak veel voorkomende digitale criminaliteit regio Rotterdam’ vast te stellen.
- Commitment op de uitvoering te borgen door dit een terugkerend onderwerp te laten zijn op de lokale DVO’s.
- Commitment op de uitvoering te borgen door dit een terugkerend onderwerp te laten zijn op het strategisch politieoverleg tussen burgemeester en teamchef politie. (Wat is het lokale cyberbeeld en hoe is de lokale aanpak georganiseerd?)
- Opdracht te verlenen aan de werkgroep o.l.v. de portefeuille houdend burgemeester om de lange termijn aanpak vorm te geven, waarbij de intentie door de VNG is uitgesproken om hierin een constructieve samenwerking op te zetten.
- Kennis te nemen van de stand van zaken ‘Aanpak veel voorkomende digitale criminaliteit regio Rotterdam’.
- Kennis te nemen van het `Jaarbeeld Cyber’.