INFORMATIE AAN HET WERK!

Slimmer omgaan met grote hoeveelheden informatie in de veiligheidsketen

Resultaten 2012

TNO innovation for life

Arnout de Vries
Lotte de Groen

Informatie aan het werk!

Slimmer omgaan met grote hoeveelheden informatie in de veiligheidsketen

TNO innovation for life

INFORMATIE AAN HET WERK!
Slimmer omgaan met grote hoeveelheden informatie in de veiligheidsketen
Resultaten 2012 | TNO

TNO.NL

Redactie
Arnout de Vries, arnout.devries@tno.nl
Lotte de Groen, lotte.degroen@tno.nl

Drukwerk Repro TNO, Den Haag
Lay-out Coek Design, Zaandam
Afbeeldingen zoompf.com, paterva.com, go-globe.com

INHOUD

1 INLEIDING

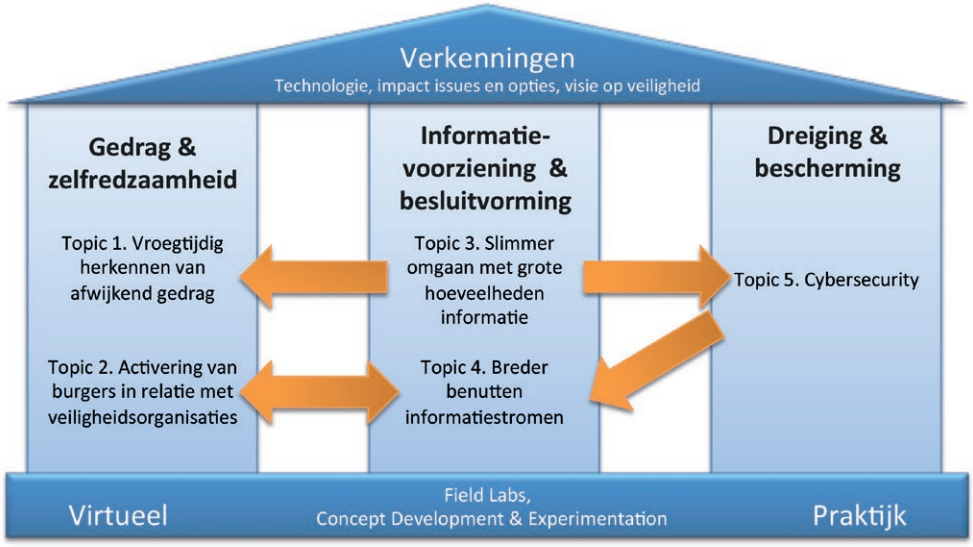
Deze publicatie neemt u in vogelvlucht mee langs de resultaten van het onderzoek dat in 2012 door TNO is verricht op het onderwerp: Slimmer omgaan met grote hoeveelheden informatie. Dit onderzoek is onderdeel van het programma Veilige Maatschappij dat TNO in opdracht van het Ministerie van Veiligheid en Justitie uitvoert.

Het is bedoeld voor alle stakeholders op het gebied van openbare orde en veiligheid. Door het lezen van dit boekje krijgt u zicht op de kennis die beschikbaar en in opbouw is en op welke wijze dit binnen het domein van openbare orde en veiligheid zijn toepassing kan vinden.

PROGRAMMA VEILIGE MAATSCHAPPIJ

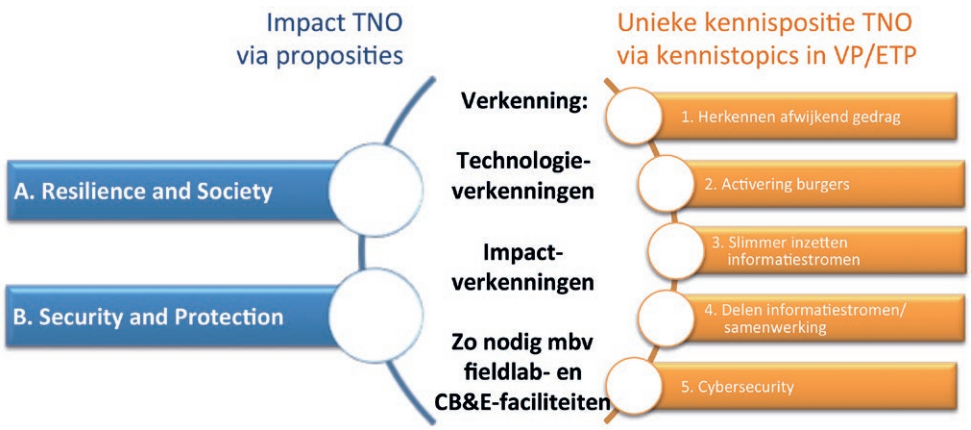
In het TNO-Innovatiegebied Veilige Maatschappij is het onderzoek dat TNO uitvoert in de strategieperiode 2011-2014 gericht op de volgende impact:

1. Effectievere/ efficiëntere veiligheidsoperaties en rampenbestrijding door innovatie van informatievoorziening, besluitvorming en organisatie van de samenwerking tussen organisaties;
2. Effectiever/ efficiënter optreden van veiligheidsorganisaties door innovatie van doctrine, materieel, uitrusting en competenties;
3. Vergroting veiligheid in openbare ruimte door effectief betrekken van burgers/bedrijven;
4. Beperking schade ten gevolge van rampen/crises (overstromingen, CBRNe-incidenten, uitval vitale infrastructuren) door snel en adequaat optreden en door kosteneffectieve pro-actieve maatregelen.



Figuur 1
In overleg met het Ministerie van V&J, stakeholders en TNO geselecteerde topics voor VP Veilige Maatschappij 2011-2014 en hun onderlinge relatie.

Om deze impact te bereiken zijn proposities opgesteld (zie figuur 2). In overleg met regievoerder Ministerie V&J en behoeftestellers zijn hier vijf topics aan gekoppeld (1-5 in figuur 2) die ieder voor zich van belang zijn voor beide proposities. Samen vormen de topics het programma Veilige Maatschappij.



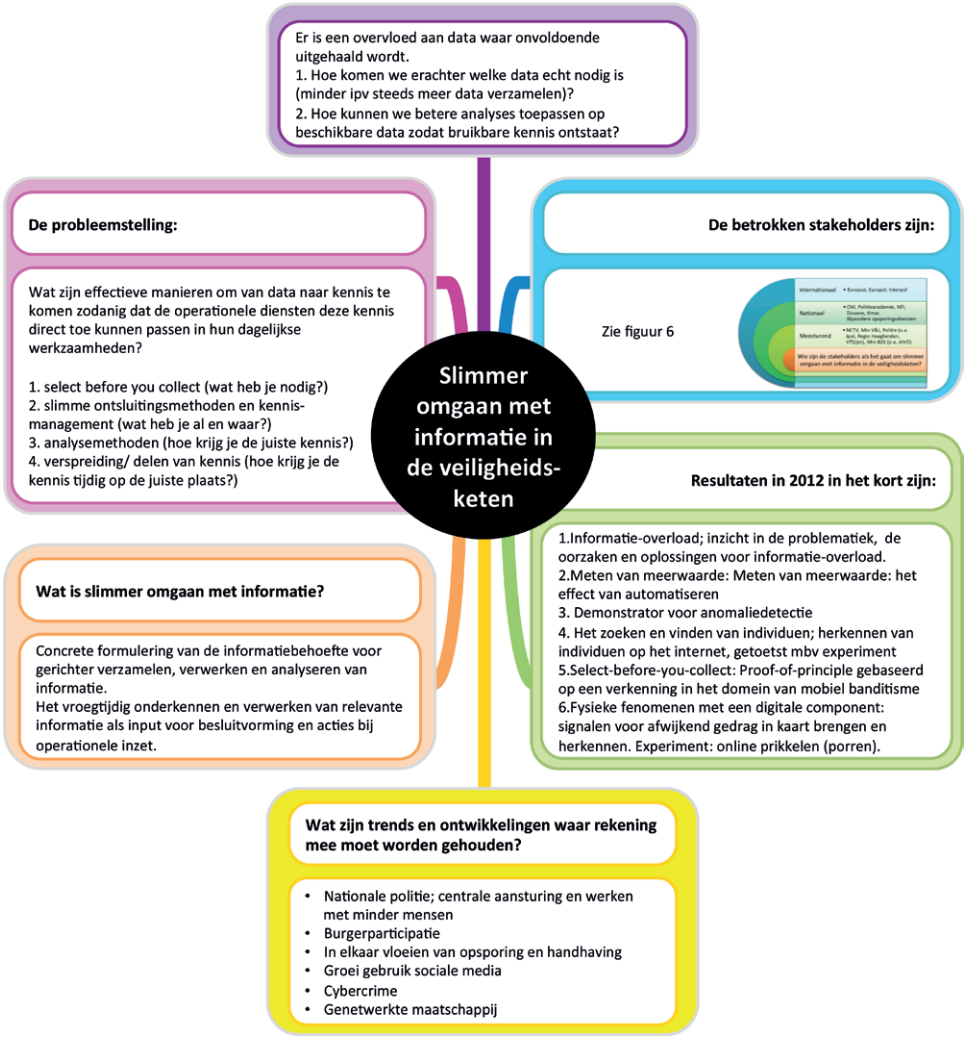
Figuur 2
Overzicht van proposities en topics van het programma Veilige Maatschappij

Deze publicatie richt zich op topic 3. Het onderwerp betreft het slimmer inzetten van beschikbare informatie en nieuwe (sociale) media voor operationele veiligheidstaken. Een belangrijke focus is de verwerking van grote hoeveelheden aanwezige informatie, waarnemingen en meldingen tot bruikbare kennis.

De probleemstelling, kernvragen en trends waarmee rekening is gehouden voor topic 3 zijn gevisualiseerd in figuur 3. In het kort is opgenomen wat de resultaten zijn van de verschillende onderdelen.

LEESWIJZER

In deze publicatie vindt u een compacte beschrijving van de resultaten van het onderzoek dat in 2012 is verricht. Eerst worden in hoofdstuk 2 de samenhang tussen de verschillende werkpakketten beschreven. In hoofdstuk 3 komt het belang van de samenwerking met stakeholders aan de orde. Per werkpakket treft u in hoofdstuk 4 de belangrijkste resultaten aan. Tot slot geeft hoofdstuk 5 een korte vooruitblik naar de plannen voor 2013.



Figuur 3
Slimmer omgaan met informatie in de veiligheidsketen

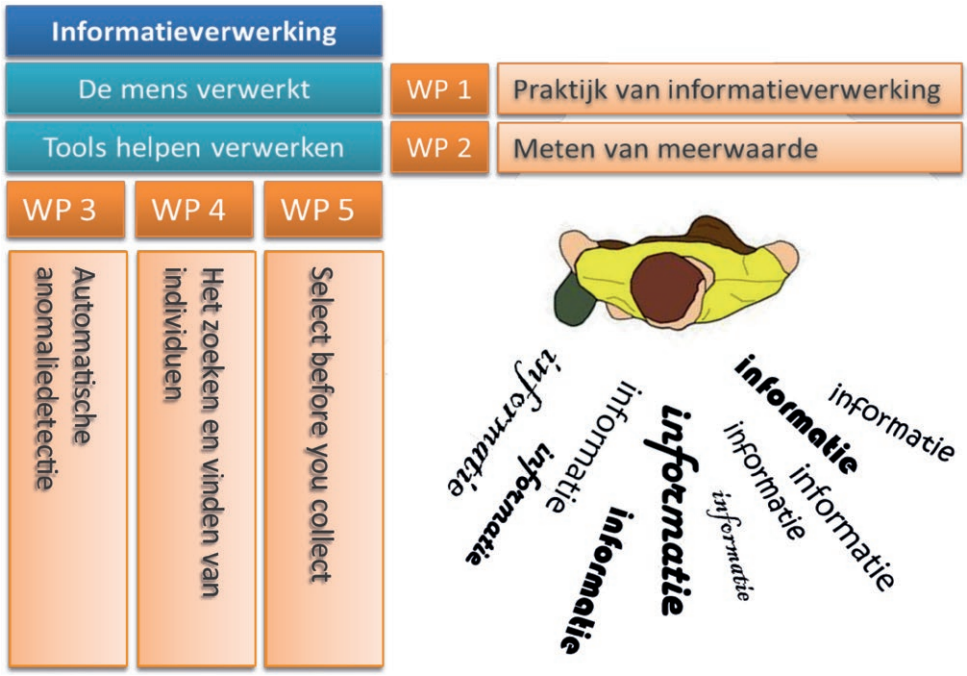
2 SLIMMER OMGAAN MET INFORMATIE

In de veiligheidsketen is het noodzakelijk dat grote hoeveelheden informatie snel verwerkt worden tot bruikbare kennis. De hoeveelheid beschikbare data en informatie neemt de afgelopen jaren explosief toe, waardoor doorgaan op de huidige (veelal niet-geautomatiseerde) wijze van informatieontsluiting een te grote inzet van de menskracht zou vergen. Het is de vraag in hoeverre meer informatie op dit moment ook meer kans op een geslaagde aanhouding of interventie opleveren. Meer is niet altijd beter en wegen de kosten voor het verzamelen en analyseren van informatie wel op tegen de resultaten?

De uitdagingen waarmee de spelers in de veiligheidsketen worden geconfronteerd hebben betrekking op een overvloed aan informatie (informatie-overload), een tekort aan menselijke verwerkingscapaciteit (personele krapte) en de noodzaak om proactief te analyseren en te beslissen (sneller voorin de keten komen). Daarnaast is er aansluiting nodig op de paradigma verschuiving die nieuwe en sociale media als vorm van communicatie met zich meebrengen; communicatie vindt in steeds mindere mate hiërarchisch of lineair plaats, maar juist diffuus door en met het publiek.

In 2012 heeft dit zich vertaald in een vijftal werkpakketten (figuur 4). Werkpakket 1 richt zich op de mens die informatie verwerkt, werkpakket 2 op de tools die de mens helpen verwerken. De werkpakketten 3, 4 en 5 richten zich specifieke tools of methoden slimmer te verwerken.

Het is wederom ons streven geweest zoveel mogelijk samen met één of meerdere stakeholders een onderwerp uit te werken. Deze manier van werken stelt ons in staat om snel zicht te krijgen op de toepasbaarheid van de ontwikkelde kennis.



Figuur 4
De samenhang tussen de deelwerkpakket.

WERKPAKKETTEN 2012

De werkpakketten voor 2012 betreffen de volgende onderwerpen:

1. Ervaren veiligheidsprofessionals informatie-overload? En zo ja, hoe komt dat en hoe kan dat verminderd worden.
2. Wat is de meerwaarde van de inzet van instrumenten / tools voor het verwerken van grote hoeveelheden informatie, en hoe kan deze worden geoptimaliseerd?
3. Hoe kan in de grote hoeveelheid data (b.v. van social media) automatisch relevante afwijkingen (anomalieën) worden gedetecteerd? Welke kenmerken zijn hiervoor het meest waardevol? Hoe kunnen opkomende incidenten vroegtijdig worden gesignaleerd?
4. Hoe kan relevante informatie over individuen online automatisch worden gecombineerd en geanalyseerd. Niet alleen netwerkanalyse op naam/nummer, maar ook op basis van kenmerken. Wat is de echte identiteit (veel mensen gebruiken meerdere identiteiten) en verandert de identiteit?
5. Hoe kan Select B4U Collect worden gebruikt om te voorkomen dat teveel data binnenkomt en hoe kan de juiste prioriteit worden aangegeven, zoals bij Triage? Door het ontwikkelen van methoden en technieken die het mogelijk maken het verwachte toekomstig nut van informatie te bepalen (conform risico gebaseerde analyse of bijvoorbeeld proportionaliteit kwantificeren) kan het “Select B4U Collect”- principe op een zo laag

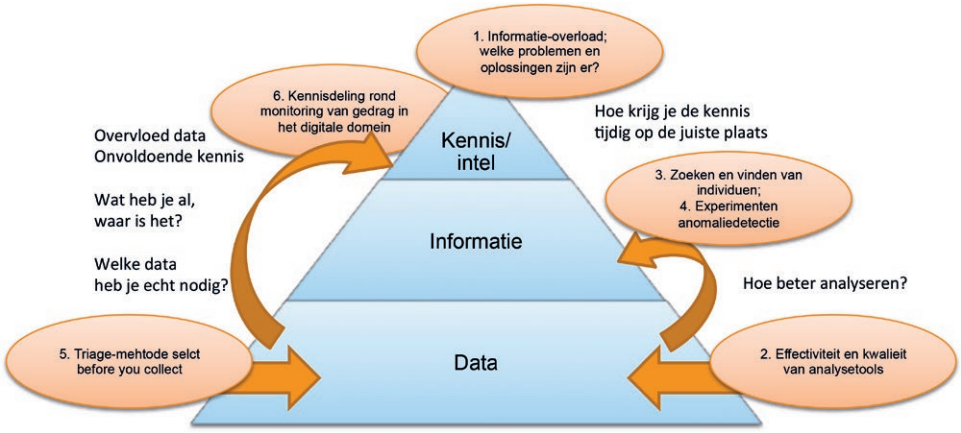
mogelijk niveau worden toegepast zodat grote hoeveelheden (onbruikbare) informatie ten behoeve van handhaving en opsporing worden voorkomen.

In de loop van het jaar ontstond de behoefte aan een zesde onderwerp.

6. Als men niet vanuit technologie kijkt naar afwijkingen op internet, maar vanuit gedragswetenschappen welke signalen zijn dan waarneembaar door de politie of door de maatschappij? Naast het in kaart brengen hiervan wordt ook een quasi-experiment gedaan om individuen of groepen te prikkelen (porren) na een dergelijk signaal ten behoeve van preventie en het verbeteren van de informatie positie of interactie.

De werkpakketten (WP's) richten zich op verschillende lagen of overgangen van data naar informatie, van informatie naar kennis zoals is gevisualiseerd in figuur 5.

De resultaten van deze werkpakketten zijn opgenomen in hoofdstuk 4.

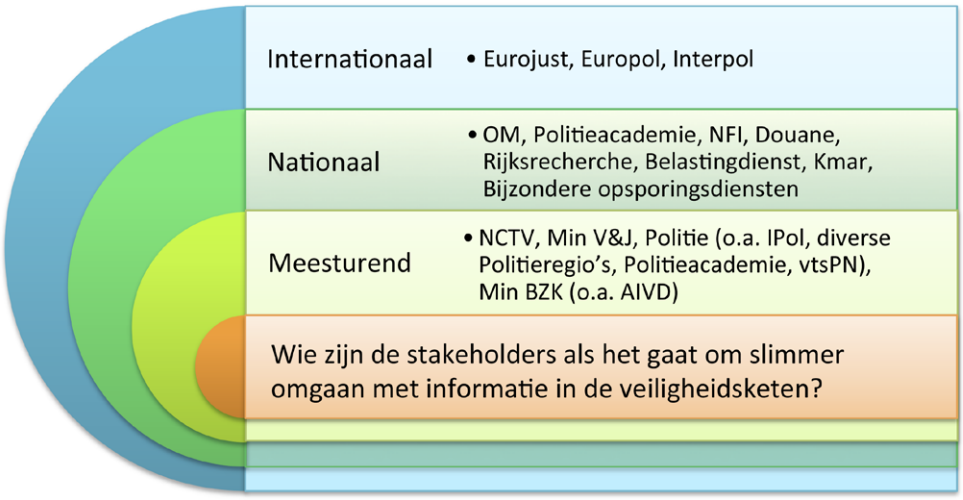


Figuur 5
De focus van de werkpakketten ten opzichte van de informatiedriehoek.

3 PARTNERS

INTENSIVERING SAMENWERKING VEILIGHEIDSORGANISATIES

Als gevolg van de activiteiten binnen het innovatieporgramma is de samenwerking tussen TNO en de diverse stakeholders versterkt. Zo wordt er samengewerkt met het iRN (internet ResearchNetwerk, voormalig internet RechercheNetwerk), met het PAC (Programma Aanpak Cybercrime) en het programma HDIef (Herkenning Digitale Informatie en Fingerprinting) van de NCTV. Daarnaast is een samenwerkingsovereenkomst gesloten tussen TNO en KLPD/IPol waarin diverse initiatieven zijn opgestart voor gezamenlijk onderzoek. Ook zijn diverse gesprekken gevoerd met de politieacademie en het KLPD om mogelijkheden voor verdergaande samenwerking te ontplooien. En de toepassing van deze innovaties is breder. Zo wordt inmiddels vanuit handhaving openbare orde, crisisbeheersing en de real-time intelligence ontwikkelingen hierin ook gekeken naar de rol van veiligheidsregio's en gemeenten. Aan het einde en aan het begin van de veiligheidsketen staat tenslotte de belangrijkste stakeholder: de burger. Cocreatie met zowel bedrijfsleven als burgers in de domeinen handhaving, opsporing en crisisbeheersing is sterk in ontwikkeling en de 'wisdom of the crowd' wordt steeds meer toegepast in het omgaan met grote hoeveelheden informatie.



Figuur 6
Overzicht van de betrokken stakeholders

INTENSIVERING SAMENWERKING INDUSTRIE

Het samenspel in een systeem van deelsystemen, een System of Systems, is één van de onderzoeksgebieden binnen de topsector High Tech Systemen en Materialen. Onder dit topsectorproject richten overheid, industrie en kennisinstellingen zich op het delen en benutten van allerhande informatiestromen, om samen veiligheidstaken te kunnen uitvoeren. TNO verzamelde kennis, ontwikkelde een visie en past die nu toe op concrete innovatietrajecten. Via politieregio NHN en KLPD is steun voor de ontwikkeling van 4 projecten met betrekking tot Real Time Intelligence Centra. Er zijn inmiddels zeven bedrijven aangehaakt (Centric, Siemens, Thales, Croon GBBS, HP, AGT, NCIM). Deze projecten worden gekoppeld aan de ontwikkelingen rond de Nationale meldkamer. Meer informatie over de topsector regeling is te vinden op http://htsm.nl (zoek term roapmap security) .

INTERNATIONALE SAMENWERKING

Op het vlak van de internationale samenwerking zijn een aantal projecten lopend en staan diverse projecten in de steigers. Een lopend project zijn bijvoorbeeld VIRTUOSO; Versatile InfoRmation Toolkit for end-Users oriented Open-Sources explOitations. VIRTUOSO is een onderdeel van het 7e kader programma van de Europese Commissie. Het project heeft tot doel voor organisaties in de veiligheidsketen een toolkit te ontwikkelen dat beslissings-ondersteuning biedt op basis van ‘open source’ informatie. De toolkit heeft een open architectuur om huidige en toekomstige tools in te passen.

KENNISDELING

Het netwerk dat is en wordt opgebouwd maakt het mogelijk dat de kennis die binnen het onderzoeksprogramma wordt opgebouwd snel aan de relevante stakeholders beschikbaar kan worden gesteld en kan worden getoetst of dit ook voldoet aan de behoeften.
Naast de terugkoppeling aan de stakeholders hebben we diverse momenten aangegrepen om kennis over de werkpakketten te delen (zie bijlage A)

4 RESULTATEN 2012

4.1 INFORMATIE-OVERLOAD IN DE POLITIE-PRAKTIJK

Betrokken | Lotte de Groen (lotte.degroen@tno.nl) en Tom Rijgersberg

Ervaren politiemedewerkers informatie-overload in hun dagelijkse praktijk?
Als dat zo is, waar komt dat dan door?
En als we dat weten, hoe kunnen we het dan oplossen?

Deze vragen lagen ten grondslag aan het onderzoek naar Informatie-overload in de Politie-praktijk dat is uitgevoerd en waarvan u de antwoorden hier kunt lezen.

AFBAKENING

Informatie-overload is een verschijnsel dat zich in elke werk- en privé-situatie kan voordoen. Zoals de titel doet vermoeden is het onderzoek echter gericht op de dagdagelijkse problematiek bij het Handhaven en Opsporen in de Politie-praktijk.

De afbakening is vooral ingegeven door de wens om de vermeende problematiek van informatie-overload te toetsen in situaties met zeer korte doorlooptijden dicht op het werkvloerniveau. Met deze afbakening wordt geprobeerd om vooral naar de eindgebruiker van de informatie te kijken.

Een onderzoeksteam van TNO heeft diverse medewerkers op diverse niveaus uit het veld geïnterviewd om het antwoord op de vragen te verkrijgen. Deze zijn met externe stakeholders getoetst en aangevuld door TNO-experts. Daarbij is zowel naar techniek, mens als proces gekeken.

De randvoorwaarden aan het werkpakket waren zodanig dat alleen een initiële verkenning heeft plaatsgevonden. Op deze wijze kan het onderzoek gefaseerd worden uitgebreid en aansluiting blijven houden bij de tussenresultaten.

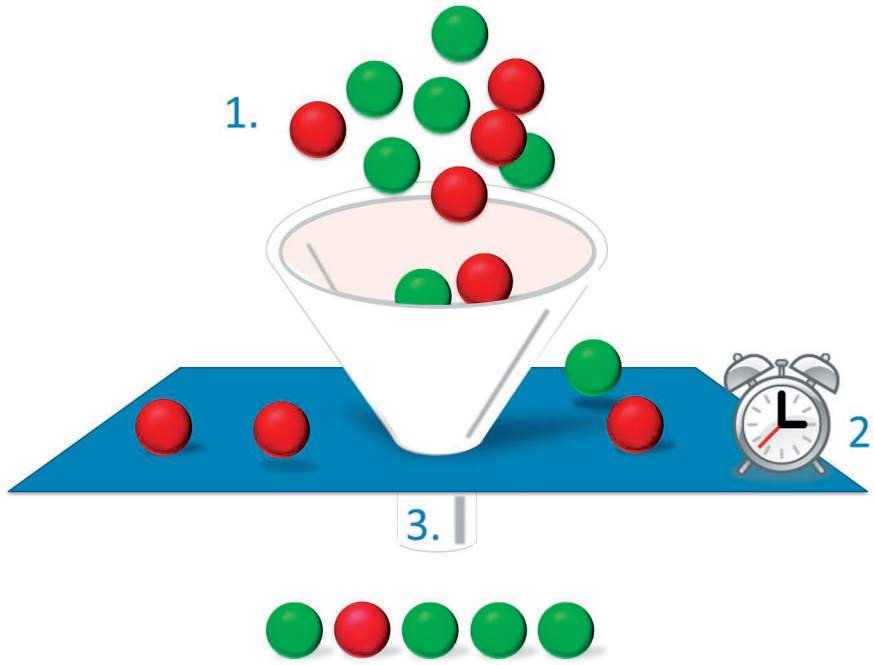
ERVAREN POLITIEMEDEWERKERS INFORMATIE-OVERLOAD IN HUN DAGELIJKSE PRAKTIJK?

Het begrip Informatie-overload kent geen algemeen geaccepteerde definitie. De definitie die in dit onderzoek is aangehouden is als volgt:
Er is sprake van informatie-overload als gewenste informatie voor het tijdig nemen van een besluit of het volbrengen van een taak, ondanks aanwezigheid, onopgemerkt blijft als gevolg van:

- te veel (minder-gewenste) informatie en/of;
- een te beperkte informatieverwerkingscapaciteit.

In deze definitie zien we drie variabelen aan het werk:

1. Hoeveelheid informatie (de load);
2. De beschikbare reactietijd;
3. De (persoonlijke) verwerkingscapaciteit.



Figuur 7
Informatie-overload geschematiseerd

Het samenspel bepaalt of er sprake is van overload. In de kern gaat het over het niet tijdig of onjuist nemen van besluiten gezien de beschikbare informatie. Dat kan grote gevolgen hebben voor politie, betrokkenen of omstanders. Men moet snel kunnen handelen en juiste informatie is daarbij cruciaal. Nog te vaak blijkt informatie wel beschikbaar maar onopgemerkt, of wordt verkeerde, onvolledige, onbetrouwbare of verlopen informatie ten onrechte gebruikt.

Informatie-overload bestaat en is een probleem ook al wordt het nog niet door iedereen zo gezien of ervaren.

Wat tijdens het onderzoek opviel is een discrepantie tussen de zienswijze van leidinggevenden en de ervaring van de werkvloer. Waar leidinggevenden aangaven dat ze dachten dat hun personeel wel informatie-overload zou ondervinden met alle informatie die nu beschikbaar is en de werkzaamheden die gevraagd worden, geven werknemers aan geen informatie-overload te ondervinden. Men mist geen informatie om goed te kunnen presteren en ondervindt daarom geen informatie-overload. Bij doorvragen blijkt dat zij filteren door bepaalde informatiebronnen te negeren (bijvoorbeeld social media of andere openbare bronnen) of niet als relevant te achten. Dat is binnen de context van dit onderzoek dus een verborgen vorm van informatie-overload.

We constateren dus, dat ondanks dat geïnterviewden aangeven dat ze geen informatie-overload ervaren maar bij doorvragen wel aangeven dat ze informatie moeten negeren door tijdgebrek , dat informatie-overload bestaat en een urgent probleem is dat prioriteit behoeft.

ALS DAT ZO IS, WAAR KOMT DAT DAN DOOR?

De beschrijving van de door de geïnterviewden genoemde problemen en onderliggende oorzaken van informatie-overload wordt in de volgende paragrafen toebedeeld aan:

- De hoeveelheid beschikbare informatie zelf;
- De beperkingen van de mens;
- De wijze van organiseren (proces);
- Het gebruik van technische middelen.

Informatie

De beschikbare hoeveelheden data stijgen enorm (zie figuur 7). Dit komt omdat het gebruik van sociale media enorm toeneemt, er steeds meer (openbare) bronnen ontstaan, de media waarop informatie kan worden geraadpleegd toeneemt en door het toenemend gebruik van realtime sensor-data zoals bijvoorbeeld camerabeelden.

Figuur 8
1 minuut digitaal[1]

Menselijke capaciteiten

Bij het verzamelen en interpreteren van informatie in een korte tijdsspanne zijn diverse problemen en oorzaken benoemd die te maken hebben met de individuele vaardigheden en eigenschappen van de persoon die de informatie verzamelt en interpreteert.

De volgende hoofdcategorieën zijn benoemd:

- De complexiteit van het verzamelen;
- Het vaststellen van de relevantie van informatie;
- Het vaststellen van de betrouwbaarheid van informatie;
- Het kunnen omgaan met incongruente informatie;
- Het toebedelen van informatie aan de juiste persoon;
- Het integreren en structureren van verschillende informatie;
- Het besluiten wanneer er genoeg verzameld is;
- Persoonlijke effectiviteit en efficiëntie.

1 (http://www.go-globe.com/, bezocht 16-08-2012)

Procesinrichting

De problematiek van informatie-overload wordt soms ook gekenmerkt door meer proces gerichte oorzaken. De volgende oorzaken zijn door de geïnterviewden benoemd:

- Mismatch met huidige prioriteringssysteem;
- Onjuiste intake van verzoeken;
- Snelle reactietijden door wetgeving, politieke druk of media-aandacht;
- Het verkrijgen van toestemmingen van informatie eigenaren;
- Veel (nieuwe) procedures.

Technische middelen

Bij het verzamelen van informatie wordt met steeds meer verschillende technische systemen gewerkt. Veel van de systemen zijn in de praktijk arbeidsintensief en daarmee tijdrovend. Omdat de reactietijd, na de hoeveelheid informatie, de tweede hoofdvariabele is bij informatie-overload, wordt de problematiek regelmatig toegeschreven aan de technische systemen. Voorbeelden zijn er van systemen die na een korte tijd van inactiviteit uitloggen, systemen die niet interoperabel zijn, systemen die export van data alleen toestaan in zeer kleine hoeveelheden per keer etc.

Naast de arbeidsintensiteit als gevolg van de technische systemen wordt ook de administratieve druk vaak genoemd. Men dient veel administratie bij te houden en dat gaat ten koste van de beschikbare tijd om informatie te vergaren en te beslissen.

Samenvattend

De stakeholders verbonden aan het programma geven aan dat de volgende punten de meeste aandacht verdienen:

1. de complexiteit van integreren en structuren;
2. de complexiteit van het vaststellen van betrouwbaarheid van informatie;
3. de complexiteit van het vaststellen van de relevantie van informatie;
4. de arbeidsintensiteit van het verzamelen van informatie;
5. de administratieve druk in het werk.

EN ALS WE DAT WETEN, HOE KUNNEN WE HET DAN OPLOSSEN?

De problemen en oorzaken zijn velerlei en oplossingen moeten gezocht worden in de techniek, menselijke capaciteit en procesinrichting. Oplossingen die zijn benoemd door de geïnterviewden en door TNO-experts zijn wederom gevat in de clusters (informatie, mens, proces en techniek.

Informatie

Veruit de meest genoemde oplossingen beginnen aan het begin van de keten: het kiezen van welke informatie wel of niet relevant is. Het vroegtijdig filteren van informatie lijkt van uitermate belang. De meeste hoop is gevestigd op software die automatisch de juiste informatie vergaard. Hetzij bij het bevragen (pull) hetzij bij het ongevraagd ontvangen (push).

Nog een stap verder is software die zelf proactief op zoek gaat op basis van profielen. Dit systeem zou dan automatische 'hits' in combinatie met de bovenstaande genoemde functionaliteiten moeten genereren.

Het moge duidelijk zijn dat dergelijke oplossingen, los van de technische mogelijkheden, zeer beperkt worden door het ontwerp van de huidige verschillende informatiebronnen die niet is bedoeld voor interoperabiliteit of het omgaan met (near)realtime bevraging , maar ook door privacy en juridisch kader.

Volgend op het verzamelen van relevante, congruente en betrouwbare informatie is het in samenhang beschouwen ervan. Het integreren en structureren van informatie uit verschillende bronnen blijkt lastig in de praktijk.

TNO-experts suggereren een te ontwikkelen tool: 'Interactive Visual Situation Report'. Een tool dat het voor eindgebruikers mogelijk maakt om (gekoppelde) informatie door eigen 'bril' te zien middels interactief instelbare 'views' ten behoeve van het ondersteunen van integratie en structurering. Voordeel hiervan is dat ook nieuwe inzichten kunnen ontstaan omdat alles met elkaar in relatie is gebracht.

Menselijke capaciteiten

Zoals benoemd bij de oorzaken ondervindt de 'mens' problemen met het vaststellen van betrouwbaarheid, relevantie, bevragingen etc.
Veel systemen hebben complexe interfaces voor de bevraging. Klaargezette sjablonen (eventueel met een aantal keuzevelden) zal de gebruiker enorm helpen. Het integraal bevragen van meerdere systemen tegelijk zou ook enorm helpen.

Ten tweede zullen Question-Answer (QA) machines hoogstwaarschijnlijk de opvolger worden van het huidige zoeken op Internet middels het matchen op bepaalde woorden. Je stelt gewoon je vraag en je krijgt een antwoord in plaats van een lijst van pagina's met bepaalde woorden erop.

Goed integreren en structuren kan grote waarde hebben. Het lid zijn van een schietvereniging én het onder behandeling zijn bij een psychiatrische instelling is tezamen bijvoorbeeld veel meer zeggend dat de twee losstaande gegevens. Dit correleren en vervolgens weergeven van een geïntegreerd en gestructureerd beeld, binnen de korte tijdsspanne, is niet eenvoudig. Informatie is vaak ook niet gelijksoortig (gestructureerd versus ongestructureerd, statisch versus dynamisch, tekst versus spraak versus beeld etc). Dat bemoeilijkt dit nog meer.

Voor het integreren en structureren kijkt men dan ook naar software die bedoeld is om alle informatiegegevens uit diverse informatiebronnen tezamen op een logische manier te presenteren voor de eindgebruiker. Soms kan ook informatie uit een enkele bron worden gestructureerd. Een voorbeeld hiervan is het mappen van tweets op een tijdas en een geografische kaart.

Een niet softwarematige oplossing ter ondersteuning van de 'mens' is de invoering van Real-Time Intelligence Centres (RTIC). Dit concept is al op enkele plaatsen beproefd en zeer succesvol.
Een andere oplossing die is genoemd is het maken van een cultuuromslag van 'goed en grondig' naar 'goed genoeg en snel'. Door training en het hebben van boegbeelden die het goede voorbeeld geven wordt deze cultuurslag vergemakkelijkt.

TNO experts suggereren om de capaciteiten van de mens bij het zoeken en verwerken van relevante en betrouwbare informatie binnen de beschikbare tijd te vergroten door het selecteren van mensen op basis van specifieke competenties en door het meetbaar maken van de capaciteiten. Een andere oplossingsrichting is gericht op het trainen van de competenties met extra aandacht voor wil (naast kunde).

Hierbij kan worden gedacht aan de ontwikkeling van een motivatie- en bewustzijnsgame voor wijkagenten (= willen); een competentie game voor RTIC-medewerkers of als assessment-tool (= kunnen), of een trainingstoolbox met zelfstandige leermiddelen.

TNO heeft uitgebreide kennis van en ervaring in het ontwikkelen van dergelijke games.

Op Internet zijn diverse mechanismen ontstaan waardoor bepaalde informatie(bronnen) hoog staan aangeschreven. Door systemen als 'I like' en bijvoorbeeld het aantal views van een youtube-filmpje komt zonder regie zaken bovendrijven. Hierbij speelt vooral kwantiteit een rol.

Dergelijke mechanismen zijn natuurlijk ook zeer bruikbaar om de informatie(bronnen) binnen de context van de Politie in haar dagdagelijkse werkzaamheden te voorzien van een betrouwbaarheidsoordeel. Hierbij moet niet alleen kwantiteit een rol spelen maar bovenal de kwaliteit.

En wie kent niet de ervaring dat je met veel pijn en moeite een gewenst stuk informatie hebt bemachtigd die iemand anders zo voor je had kunnen aanwijzen. Een voorgedragen oplossing door TNO experts is gericht op het vinden van die tussenpersoon oftewel het expliciet vergroten van inzicht in impliciete expertkennis.
Om de zichtbaarheid van impliciete expertkennis te vergroten kan gedacht worden aan het opstellen van expliciete 'wat heb ik te bieden' profielen. De betrouwbaarheid van een profiel zou bestendigd kunnen worden met een 'I like' mechanisme.

Procesinrichting

Zoals benoemd worden er vaak nieuwe procedures opgesteld om bepaalde incidenten zoveel mogelijk te voorkomen wanneer er in de media of politiek veel aandacht uitgaat naar een incident. De oplossing is om nieuwe procedures beter te laten aansluiten bij de bestaande en bekende procedures.

Het intakeproces dient te worden geformaliseerd. Zoals eerder benoemd, worden informatieverzoeken buiten het takenpakket nogal eens gehonoreerd. Het strikter uitvoeren van de intake voorkomt inmenging met informatieverzoeken die wel binnen het takenpakket vallen.

Ook eerder genoemd is de mismatch tussen de prioritering van de meldkamer en de prioritering met betrekking tot het snel vergaren van informatie. Andere afspraken hierover zouden dit probleem kunnen verhelpen. Bij een melding van een ongeval met onopzettelijk lichamelijk letsel (een prioriteit 1 melding voor de centralist en agent op straat) is het snel vergaren van contextuele informatie minder van toepassing. De functionaris die daarmee behept is wil veel liever met urgentie die meldingen doorkrijgen die wel om intensieve informatievergaring vragen, zoals een melding van huiselijk geweld. De urgente informatiebehoefte die daarbij speelt is: hoe vaak is er al eerder een melding geweest, wat was toen de situatie, wie zijn er bij betrokken, is de betrokkene vuurwapengevaarlijk? Als de agent weet dat er kinderen aanwezig kunnen zijn, een agressieve hond of een vuurwapengevaarlijke man, kan hij zijn manier van optreden daar op aanpassen. Dit helpt de effectiviteit en de veiligheid van de diender.

Om het delen van informatie tussen verschillende informatie eigenaren dient zowel het proces als de vertrouwensrelatie op een hoger niveau te komen. Het verbeteren van publiek-private samenwerking valt hier ook onder.
Tenslotte wordt het gedisciplineerd briefen én debriefen als een zeer succesvolle oplossing benoemd om prioriteringen op een dag helder te krijgen.

Technische middelen

In de eerdere paragraaf over informatie is al uitvoerig stilgestaan bij technische (softwarematige) oplossingen. Hieraan kunnen de volgende genoemde oplossingen worden toegevoegd.

- Maak bronnen zodanig bevraagbaar dat het kopiëren van data niet meer nodig is.
- Voorkom dat (politie) systemen te snel automatisch uitloggen bij inactiviteit.

De geïnterviewden noemde ook het voortbouwen op het concept van Front Office Back Office (FOBO) voor het vastleggen van de benodigde administratie waarmee de uitvoerder wordt ontlast.

CONCLUDEREND

De problemen en oorzaken zijn velerlei. De oplossing zal dan ook niet eenvoudig zijn en zowel op het gebied van techniek, menselijke capaciteiten en procesinrichting goed doordacht moeten worden. Het onderzoek in ogenschouw nemende, willen wij daarom volgende punten benadrukken:

- TECHNIEK Er is speciale aandacht nodig voor interoperabiliteit van de diverse informatiebronnen evenals de daarbij behorende juridische en privacy gerelateerde vraagstukken. Dit is een voorwaarde om technisch gekleurde oplossingen eenvoudiger mogelijk te maken;
- MENS Er is bij medewerkers veel kennis aanwezig. Deze is echter gefragmenteerd en onbekend. Het opheffen van deze fragmentatie en onbekendheid middels modern kennis- en informatiemanagement is een noodzaak;
- PROCES De kern van de zaak draait om het tijdig nemen van 'voldoende geïnformeerde' besluiten. Het expliciet inrichten van de processen rondom besluitvorming aangevuld met onderzoek naar beslissingsondersteunende middelen die antwoord geven op 'wat is voldoende', verdient alle aandacht.

De toename van de hoeveelheid en diversiteit van informatie zal nieuwe mogelijkheden doen ontstaan mits de informatie-overload problematiek gelijktijdig wordt aangepakt. Daarom wordt aanbevolen om de genoemde oplossingsrichtingen prioriteit te geven. Het kundig en snel kunnen verwerken en gebruiken van relevante informatie zal de volgende positieve uitwerkingen kennen:

- Grotere heterdaadkracht;
- Verhoogde veiligheid voor de agent op straat;
- Effectievere inzet;
- Informatievoorsprong op de burger;
- Een beter en modern imago;
- De basis leggen voor proactief (voorkomen) optreden in plaats van reactief (genezen).

4.2 METEN VAN MEERWAARDE

Betrokken | Egon L. van den Broek (egon.vandenbroek@tno.nl) en Mirjam Huis in 't Veld

INTRODUCTIE

Wij hebben ons gericht op het beantwoorden van de vraag: Door welke factoren wordt de (meer)waarde van open bronnen beïnvloed bij rechercheonderzoek in de handhaving en opsporing? En: hoe kan die (meer)waarde verhoogd worden?

De (meer)waarde van open bronnen intelligence (OSINT) wordt onder andere beïnvloed door de kenmerken van zoekmachines en door de trainingen om open bronnen te ontsluiten met dergelijke tools. In een recentelijk vooronderzoek van de vts Politie Nederland (de Lignie en van der Waal, 2011) wordt een overzicht gegeven van analysevoorzieningen die gebruikt worden in 23 korpsen in Nederland, waarbij iBase, BRAINS, DataDetective en Palantir diepgaand zijn geanalyseerd. Daarnaast worden door zowel commerciële partijen als de overheid verschillende trainingen op het gebied van OSINT aangeboden, zoals http://onstrat.com/, http://www.uk-osint.net/ en http://www.opensourceintelligence.eu/.

In dit project hebben wij ons wat breder georiënteerd om andere factoren te identificeren die invloed hebben op de (meer)waarde van open bronnen. Er is een beperkt aantal interviews gehouden met verschillende stakeholders uit het domein van de handhaving en opsporing. Daarnaast is een set cursusmateriaal en literatuur bekeken.

Op basis hiervan is een zestal factoren geïdentificeerd en zijn inzichten verkregen die kunnen helpen bij het verhogen van de (meer)waarde van open bronnen. Deze factoren zijn geclusterd in drie categorieën: Automatisering, Zoeken in open bronnen en Standaardisering. De indeling is als volgt:

1. Automatisering
   - Workflow
   - Big data analyse
2. Zoeken in open bronnen
   - Beperkingen van zoekmachines
   - Context, profiel en sociaal netwerk
3. Standaardisering
   - Werkwijzen en training
   - Dossiervorming

In de volgende secties zullen wij de drie categorieën behandelen. Deze opsomming is niet onuitputtelijk en dient als basis voor verdere uitwerking.

AUTOMATISERING

Enerzijds wordt de verwerking van informatie uit open bronnen gekenmerkt door een complexe workflow, waarin de mens een cruciale schakel is. Anderzijds kan het veel tijdswinst opleveren en structuur afdwingen in een zoekproces, waardoor het meer informatie kan opleveren.

Workflow

De workflow van het verwerken van informatie uit open bronnen laat zich uitstekend vatten in een stroomschema (Pouchard e.a., 2009; Rasool e.a., 2010). Hier wordt een voorbeeld geschetst van zo'n workflow.

Een onderzoek start met de beschikbare persoonsgegevens (bijv. Naam, Adres, Woonplaats). Vervolgens wordt een scala aan websites gebruikt (bijv. Pipl, Facebook, Marktplaats en Wayback machine). Ook kan het Kadaster geraadpleegd worden. Daarnaast wordt een scala aan plugins voor browsers gebruikt. Zo'n workflow wordt verder beïnvloed door onder andere de typering van de zaak/het delict, de beschikbare gegevens, de individuele rechercheur, de beschikbare websites en tools en de beschikbare tijd. Dit resulteert in de praktijk tot maatwerk, waardoor het vooralsnog een utopie is om een workflow in zijn geheel te automatiseren. Daarentegen kunnen bepaalde onderdelen van de workflow die nu handmatig worden uitgevoerd, uitstekend geautomatiseerd worden. Zo kan automatisch en parallel op meerdere websites worden gezocht en kunnen automatische varianten van persoons- en plaatsnamen worden gegenereerd en worden opgenomen in de zoekvraag (Feitelson, 2004; Ravin en Wacholder, 1997). Ook kunnen zogenaamde meta crawlers tegelijkertijd meerdere zoekmachines (bijv. Google, Bing en Yahoo) benaderen met dezelfde zoekvraag (bijv. http://www.dogpile.com/, http://www.metacrawler.com/ en http://www.mamma.com/).

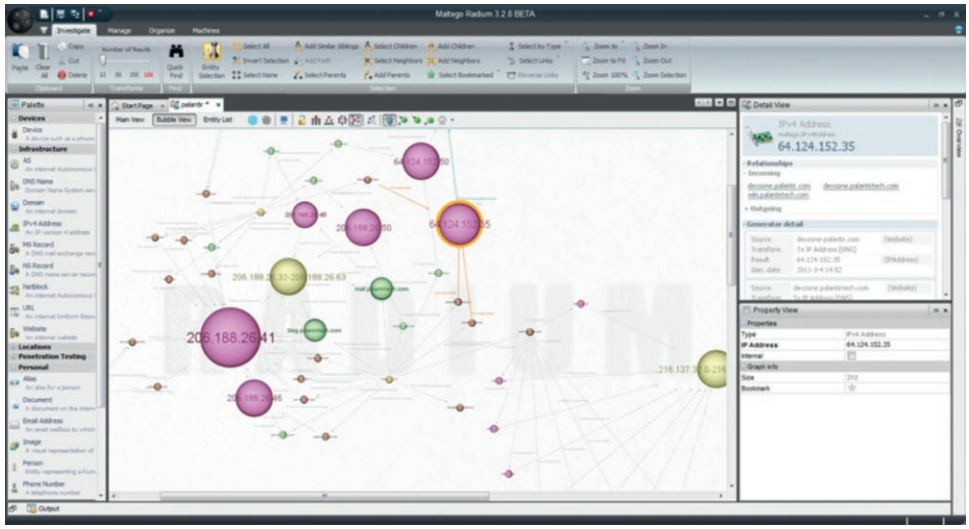
Big data analyse

Zoals bekend is de stroom aan data groot en complex en heeft onder andere invloed op het vinden, opslaan, doorzoeken en analyseren van de data. De verwachting is dat de hoeveelheid data alleen maar toeneemt door de alsmaar toenemende hoeveelheid communicatie en de verscheidenheid ervan. Hierbij valt te denken aan remote sensing, mobile sensing, draadloze sensornetwerken, camera's, microfoons, RFID's en weblogs.

De huidige hoeveelheid datastromen worden soms onvoldoende benut. Er zal dus zeker in (semi)geautomatiseerde verwerking geïnvesteerd moeten blijven worden om de groeiende datastromen te kunnen verwerken (Fisher e.a., 2012).

Een complicerende factor treedt op als data in een snel tempo verandert, waardoor de 'window of opportunity' om data te gebruiken kort kan zijn. Verwerking moet in dat geval snel plaatsvinden.

Een allereerste stap in het samenbrengen van informatie uit verschillende typen data zou kunnen door metadata uit beeld en video materiaal automatisch uit te lezen. Een drietal zeer bruikbare tools zijn Metagoofil, Exiftool en Strings. Een tool die informatie uit verschillende bronnen kan verzamelen is Maltego (zie http://paterva.com/web6/products/maltego.php en figuur 9).



Figuur 9
Een screenshot van Paterva's tool Maltego[2].

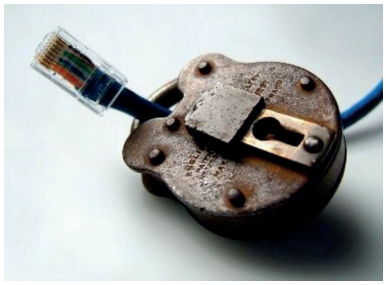
ZOEKEN IN OPEN BRONNEN

Beperkingen van zoekmachines

Er zijn verschillende zoekmachines, waarvan Google een van de meest gebruikte zoekmachines is. Elk van deze zoekmachines heeft zijn voor- en nadelen. Daarom dienen meerdere zoekmachines parallel gebruikt te worden, om zo de (directe) afhankelijkheid van Google (of een andere zoekmachine) te verkleinen. De beperkingen van elke zoekmachine dienen bekend te zijn bij de gebruiker, zodat hij weet welke bronnen en gegevens benaderd en zichtbaar gemaakt worden, en welke niet.

De belangrijkste beperking van de traditionele zoekmachine is dat zij het zogenaamde deep web slechts zeer beperkt penetreren (Xu en Chen, 2008; ter illustratie, zie ook Figuur 10). Dit deep web is dat deel van het WWW dat niet behoort tot het surface web. Het surface web is dat deel van het web dat geïndexeerd wordt door normale zoekmachines. Enkele zoekmachines die gebruikt kunnen worden om het deep web te penetreren zijn CompletePlanet

2 http://paterva.com/web6/images/maltegosidebar/2.jpg.



Figuur 10
Unlocking the hidden Internet[3].

(zie: http://aip.completeplanet.com/), BrightPlanet (zie: http://www.brightplanet.com/) en specifiek voor het zoeken naar individuen Pipl (zie: http://pipl.com). Met behulp van dergelijke zoekmachines kan informatie gevonden worden die anders verborgen blijft. Zo was ook Robert M. actief op dit deel van het internet (Volkskrant, 2012).
Het deep web bestaat uit de volgende bronnen: i) dynamische pagina's (waaronder contextuele webpagina's en door scripts genereerde pagina's); ii) webpagina's waar geen verwijzingen naar zijn; iii) Privé pagina's zoals Facebook die ook kent; iv) webpagina's die een blokkade gebruiken om web crawlers tegen te houden (bijv. door CAPTCHA); v) webpagina's met bestandsformaten die een zoekmachine niet kan interpreteren; en vi) webpagina's buiten het HTTP en HTTPS protocol. Het deep web bestaat ook nog uit zogenaamde darknets (Mansfield-Devine, 2009), dark internet en dark nets (Everett, 2009). Volgens Everett worden veel criminele activiteiten via deze onderdelen van het deep web gecoördineerd, zoals drugshandel en kindermisbruik.

Context, profiel en sociaal netwerk

Open bronnen kunnen informatie bevatten die meerwaarde kan hebben bij de reconstructie van een gepleegd delict. Te denken valt aan het profiel en het sociale netwerk van zowel daders als slachtoffers (McGloin en Kirk, 2010). Het extraheren van deze informatie uit open bronnen gebeurt veelal handmatig. Gezocht zou moeten worden naar een standaard vorm om deze profielen en sociale netwerken (automatisch) te genereren (Colombini en Colella, 2012; Sangadharan, 2012). In 2013 start het project "data mining in context" dat zal ingaan op deze materie. Het zal gebruik maken van de inzichten van ons project en de resultaten zoals beschreven in paragraaf 4.4: Het koppelen van online identiteiten van dezelfde persoon.

STANDAARDISERING

Werkwijzen en training

Goede werkwijzen kunnen in het algemeen worden bevorderd door het definiëren van standaarden en protocollen. Het gebruik van open bronnen vraagt echter om een aanpassing van de tot nu toe gebruikelijke werkwijzen. Dat heeft onder andere te maken met de snelle, dynamische ontwikkelingen op het gebied van OSINT (verschijningsvormen, tools, inhoud) (Breakspear, in press). Daardoor dient regelmatig getoetst te worden of deze werkwijzen (en trainingen) nog voldoen.

3 http://zoompf.com/2012/09 explaining-the-crime-weakness-in-spdy-and-ssl.

Ook dienen juridisch en ethische aspecten voldoende aandacht te krijgen. Zo moet worden vastgesteld hoe digitaal bewijs dat verzameld is uit open bronnen (bijv. in het kader van profiling) in lijn kan worden gebracht met bepaalde wetgeving. Een helder inzicht en duidelijke werkwijze op dat gebied kunnen betekenen dat het OM op een juiste wijze gebruik kan maken van dergelijke informatie bij de vervolging van verdachten.

Dossiervorming

Bovengenoemde inspanningen staan onder andere ten diensten van het vormen van dossiers op een zaak of een onderwerp. De rechercheur die gebruik maakt van open bronnen moet zijn resultaten op basis van bijvoorbeeld zoekopdrachten geautomatiseerd en met de juiste rubricering kunnen toevoegen aan een (klad)dossier (Prasad en Saritha, 2011). Aan het op deze wijze sneller opnemen van resultaten uit open bonnen in dossiers zal dus de nodige aandacht besteed moeten worden. Tot dusverre is hier nog nauwelijks onderzoek naar gedaan en zijn voor een dergelijke automatisering ook nog nauwelijks of zelfs geen standaarden voor ontwikkeld.

CONCLUSIE

Wij stellen dat er naast tools en training ook andere factoren zijn waarmee de (meer)waarde van open bronnen beïnvloed en verhoogd kan worden, in ieder geval op het gebied van Automatisering, Zoeken in open bronnen en Standaardisering. Het is van groot belang dat eenduidig beleid wordt ontwikkeld en voortvarend wordt overgegaan op de uitvoering ervan.

REFERENTIES (EEN SELECTIE)

Andrews, M. (2012). Searching the Internet. IEEE Software, 29(2), 13-16.
Colombini, C., Colella, A. (2012). Digital scene of crime: technique of profiling users. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 3(3), 50-73.
Everett, C. (2009). Moving across the dark side. Network Security, 9(1), 10-12.
Feitelson, D.G. (2004) On identifying name equivalences in digital libraries. Information Research, 9(4), paper 192.
Fisher, D., DeLine, R., Czerwinski, M., Drucker, S. (2012). Interactions with big data analytics. Interactions, 19(3), 50-59.
de Lignie, M., van der Waal, V. (2011). Vooronderzoek naar analysevoorzieningen; consequenties (versie 1.0). vts Politie Nederland.Mansfield-Devine, S. (2009). Darknets. Computer Fraud & Security, 12, 4-6.
McGloin, J., Kirk, D. (2010). An overview of social network analysis. Journal of Criminal Justice Education, 21(2), 169-181.
Pouchard, L.C., Dobson, J.M., Trien, J.P. (2009). A framework for the systematic collection of Open Source Intelligence. Proceedings of the AAAI Spring Symposium on Technosocial Predictive Analytics, 102-107. Stanford, CA, USA: AAAI.
Prasad, C., Saritha, S.K. (2011). Digital dossier aggregation and defence by online social networking sites. MES Journal of Technology and Management, II(1), 6-11.
Rasool, P.A., Memon, N., Wiil, U.K., Karampelas, P. (2010). Filtering the open-source information. In Proceedings of the IEEE International Conference on Software Engineering and Service Sciences (ICSESS), 217-220.
Ravin, Y., Wacholder, N. (1997) Extracting names from natural-language text. IBM Research Report, RC 20338 (04/10/97). Yorktown Heights, NY, USA: T. J. Watson Research Center, IBM Research Division.

Sangadharan, S.P. (2012). Digital inclusion and data profiling. First Monday, 17(5), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/3821.
Volkskrant (13 maart 2012). Dit is de duistere kant van het internet. Ook Robert M. was er te vinden. Online: http://www.volkskrant.nl/vk/nl/2694/Internet-Media/article/detail/3224853/2012/03/13/Dit-is-de-duistere-kant-van-het-internet-Ook-Robert-M-was-er-te-vinden.dhtml
Xu, J., Chen, H. (2008). The topology of dark networks. Communications of the ACM, 51(10), 58-65.

4.3 AUTOMATISCHE ANOMALIEDETECTIE

Betrokken | Henri Bouma (henri.bouma@tno.nl), Olga Rajadell, Daniel Worm, Corne Versloot, Harry Wedemeijer en Johan-Martijn ten Hove

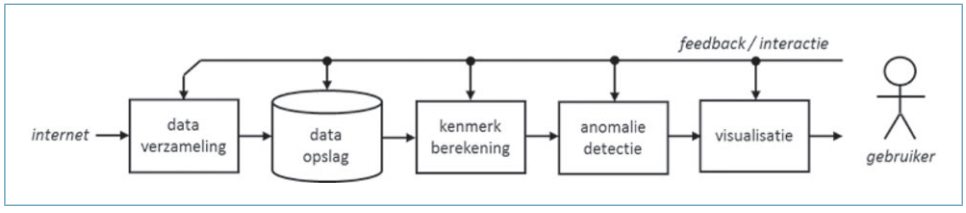
Anomaliedetectie is belangrijk voor het zo vroeg mogelijk detecteren van dreigingen. Anomaliedetectie is een techniek die kan helpen om in grote hoeveelheden data de abnormale veranderingen (anomalieën) snel terug te vinden.

Steeds vaker kunnen dreigingen voor personen en infrastructuur in de echte wereld worden gerelateerd aan activiteiten van personen op sociale media, blogs en fora op het internet. Internet surveillance beoogt het vroeg detecteren van deze dreigingen en helpt bij het vinden van verdachten gebaseerd op informatie op het web. De hoeveelheid data op het internet stijgt echter snel en het is tijdrovend om de continue stroom van tweets, posts en updates van webpagina's te volgen.

In dit werkpakket is een nieuwe methode ontwikkeld om trends automatisch te monitoren en abnormaal gedrag op Twitter of andere social media te detecteren. We presenteren een systeem voor het vroeg detecteren van dreigingen gebaseerd op een aantal kenmerken, zoals activiteit, sentiment, dreiging en tijdindicatie, toegepast in de context van demonstraties. De lijst van kenmerken die de inhoud van berichten analyseert kan gemakkelijk worden aangepast en uitgebreid om tegemoet te komen aan de behoefte van gebruikers. Het systeem is getest op Twitter data. De resultaten tonen aan dat het systeem succesvol abnormale dreigingen kan waarnemen gebaseerd op de inhoud van berichten.

METHODE

De methode bestaat uit de volgende stappen: dataverzameling en -opslag, kenmerkberekening, anomaliedetectie en visualisatie.



Figuur 12:
Architectuur van de methode.

Om de ontwikkeling en validatie op relevante data uit te voeren is een tool gemaakt die zowel de historische als de nieuwe berichten van Twitter verzamelt en opslaat.

In 2011 is een begin gemaakt met het ontwikkelen van een anomaliedetector. In 2012 is metname gefocust op het ontwikkelen van kenmerken die de inhoud van berichten typeren, dus naast het activiteits-kenmerk ook: sentiment (positief, neutraal en negatief), dreiging (dreiging / niet dreiging) voor doodsbedreigingen, demonstratie (demonstratie / niet demonstratie) voor demonstraties en protestbijeenkomsten en een tijdsaanduiding (verleden, heden, toekomst). De tijdsaanduiding is belangrijk voor het vroeg signaleren van dreigingen om een voorspelling van agressie in de (nabije) toekomst te kunnen doen en dit te onderscheiden van een reflectie op een activiteit in het verleden. Deze kenmerken kunnen door de gebruiker worden aangepast en uitgebreid.

De anomaliedetectie wordt opgedeeld in drie stappen. Eerst wordt een voorbewerking gedaan op periodes zonder activiteit te verwijderen en om ruis te onderdrukken. In de tweede stap wordt de classificatie van anomalieën uitgevoerd, waarbij is gekozen voor een 'one-class classifier', omdat deze het normaal beeld goed kan beschrijven en zeer geschikt zijn voor het detecteren wat daarvan afwijkt. Omdat niet elke afwijking (anomalie) relevant is wordt een nabewerkingsstap uitgevoerd, waarin extra eisen worden opgelegd om onbelangrijke afwijkingen te scheiden van dreigingen. Zo moet in deze stap de tijdsaanduiding wijzen op iets wat nu of in de toekomst plaatsvindt, de negatieve sentiment, dreiging en demonstratie moeten toenemen, en er moet een hoog dreigingsniveau in de berichten aanwezig zijn.

Tenslotte worden de kenmerken en dreigingen getoond aan de gebruiker. De gebruiker kan selecteren welke data wordt verzameld, welke kenmerken worden berekend, welke drempels worden gebruikt voor anomaliedetectie en welke kenmerken worden gevisualiseerd. Daarnaast kunnen eventueel nieuwe kenmerken worden geleerd.

Meer details over de methode zijn te vinden in twee publicaties die in 2012 zijn uitgebracht (zie referenties).

RESULTATEN

Voor het trainen en testen van onze methode is de volgende data gebruikt:

- Sentiment: 1500 negatief, 2100 neutraal, 1500 positief;
- Dreiging: 3300 dreiging, 2900 niet dreiging;
- Demonstratie: 3300 demonstratie, 2900 niet demonstratie;
- Tijdsindicatie: 3000 verleden, 3000 heden, 3000 toekomst.

De Tromp-dataset (Tromp, 2011) is gebruikt voor de sentiment analyse. In deze dataset zijn negatief, neutraal en positieve berichten apart geannoteerd. Dreigingen zijn verzameld van doodsbedreiging.nl, en demonstratie-berichten zijn verzameld op Twitter door te zoeken op een aantal gerelateerde keywords, zoals 'protesteren', 'rellen', 'vechten', etc. De niet-dreigingen en de niet-demonstratie zijn samengesteld uit een gebalanceerde set berichten

uit de Tromp-dataset met evenveel negatieve, neutrale en positieve berichten. De tijdsindicatie berichten zijn ook verzameld op Twitter door diverse keywords te gebruiken voor de drie verschillende tijdsmomenten, zoals onder andere: ‘gaan’, ‘morgen’, ‘zul’ (voor toekomst), ‘vandaag’, ‘nu’, ‘staan’ (voor heden), en ‘gister’, ‘had’, ‘waren’ (voor verleden).

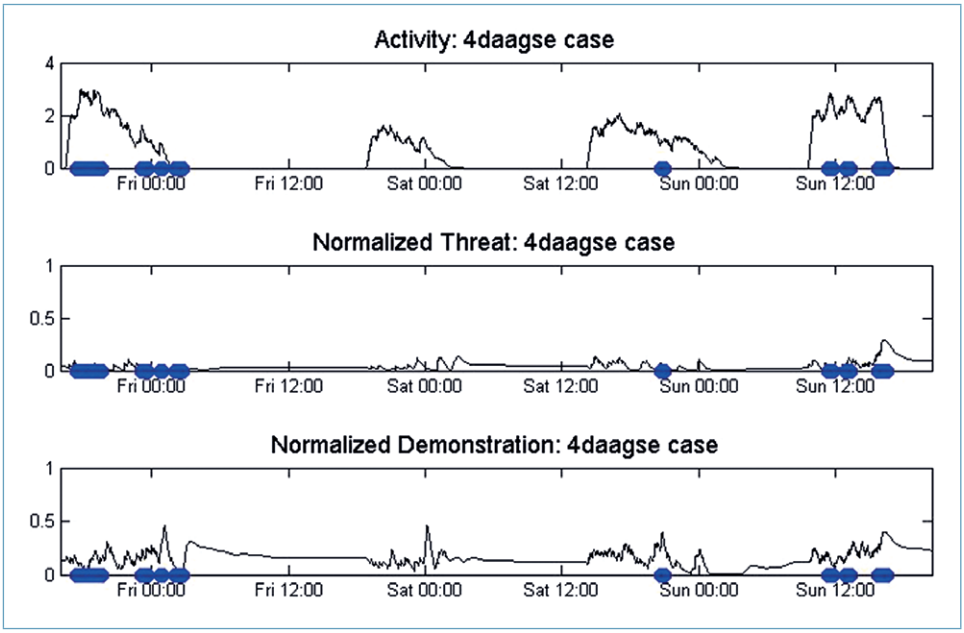
Voor het evalueren is gebruik gemaakt van de volgende data, die is verzameld van Twitter:

- Turks-Koerdische data (gewelddadige botsing; Amsterdam, oktober 2011; 9600 tweets).
- 4daagse data (vreedzaam wandel evenement van vier dagen; Nijmegen, juli 2012; 4100 tweets).

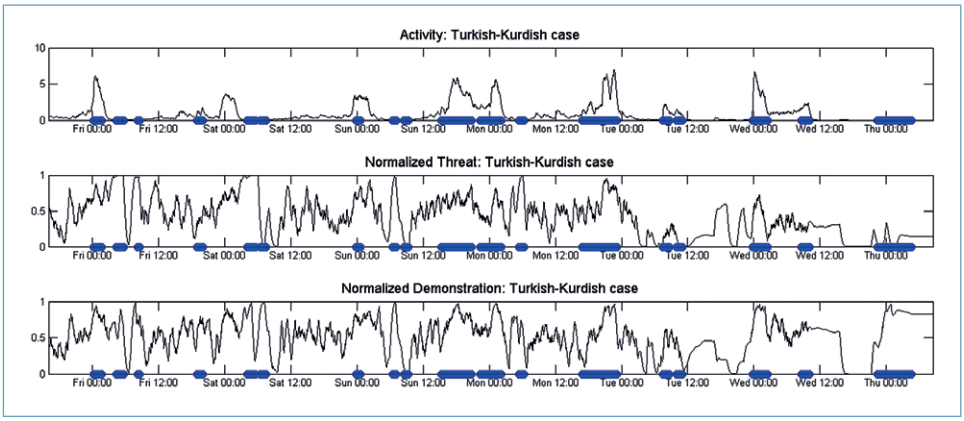
De eerste dataset bevat 9600 tweets over een gewelddadige botsing tussen Turken en Koerden in Amsterdam in oktober 2011. In de nacht van donderdag op vrijdag waren de eerste oproepen tot een demonstratie die vrijdagmiddag (21 okt) plaatsvond. Vervolgens was er op zaterdagmiddag nog een oproep tot een protest. De onrust begon zich zondag (23 okt) rond het middaguur te ontwikkelen en vanaf 16.00 werd het zeer dreigend en de incidenten vonden plaats tussen 16.30 en 17.30 uur. Na zondag waren er nog enkele oproepen tot rellen, maar die hebben niet plaatsgevonden. De tweede dataset bevat 4100 tweets over een vreedzaam wandel evenement in Nijmegen in juli 2012. Deze dataset bevat geen dreigingen of rellen.

De dreigende anomalieën die automatisch gedetecteerd worden in de Turkse-Koerdische data komen overeen met de ons bekende beschrijving van de incidenten. We detecteren toekomstige dreigingen op vrijdag vroeg in de morgen die overeen komen met een oproep tot demonstraties. Vervolgens vindt op diezelfde dag een demonstratie plaats die wordt gedetecteerd als een huidige dreiging. Later was er weer een oproep voor een demonstratie op zaterdag (toekomstige dreiging) en de grote uitbraak van gewelddadigheid vind plaats op zondagmiddag (huidige dreiging). Op maandag en dinsdag werd nogmaals opgeroepen tot meer rellen (die worden gedetecteerd als toekomstige dreigingen).

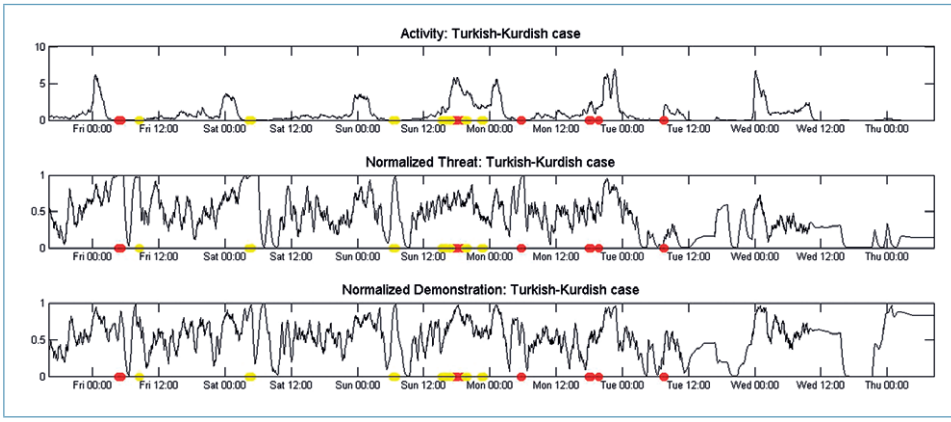
Voor de vierdaagse data werden geen dreigingen gedetecteerd. De resultaten tonen wel abnormale wijzigingen, maar het gemeten dreigingsniveau is zo laag dat deze worden verwijderd in de nabewerking.



Figuur 13
Anomalie kandidaten in 4daagse data voor post-processing (blauw).



Figuur 14
Anomalie kandidaten in Turkse-Koerdische data voor post-processing (blauw).



Figuur 15
Automatisch gedetecteerde anomalieën met een grote dreiging in de toekomst (rood) en het heden (geel). Een beschrijving van wat er echt gebeurde is opgenomen in de tekst.

CONCLUSIES EN VOORUITBLIK

In het werkpakket is een methode ontwikkeld dat dreigende afwijkingen in de fysieke wereld kan detecteren op basis van informatie op het internet. We hebben een manier laten zien waarbij meerdere kenmerken kunnen worden gedefinieerd die de inhoud van berichten analyseren, zoals sentiment, dreiging, demonstratie en tijdsaanduiding. De kenmerken kunnen worden aangepast en uitgebreid voor een andere context. De anomaliedetectie scheidt normaal gedrag van afwijkend gedrag, zodat de aandacht kan worden gefocust op de abnormale veranderingen. Met onze nabewerking zijn we in staat om dreigende activiteiten en demonstraties te rapporteren die gepland zijn in de toekomst, wat het mogelijk maakt om vroeg dreigingen te detecteren voordat ze plaatsvinden.

Het werkpakket in 2012 heeft geleid tot een framework dat een bijdrage kan leveren voor het tijdig herkennen van dreigingen. Het framework is getest en dient in een vervolg met grotere hoeveelheden en een grotere verscheidenheid aan data gevalideerd te worden. Toepassing op een groter aantal cases en interactie met gebruikers maakt het mogelijk om vervolgens gericht verbeteringen aan te brengen.

REFERENTIES

H. Bouma, O. Rajadell, D. Worm, C. Versloot, H. Wedemeijer, “On the early detection of threats in the real world based on open-source information on the internet”, Int. Conf. Information Technologies and Security ITSEC, (2012).
H. Bouma, S. Raaijmakers, A. Halma, H. Wedemeijer, “Anomaly detection for internet surveillance”, Proc. SPIE, vol. 8408, (2012).
Tromp, E., “Multilingual sentiment analysis on social media”, M.Sc. Thesis TU Eindhoven The Netherlands, (2011).

4.4 HET KOPPELEN VAN ONLINE IDENTITEITEN VAN DEZELFDE PERSOON

Betrokken | Peter Jan Doets (peterjan.doets@tno.nl), Hiddo Hut, Egon L. van den Broek en Arnout de Vries

Figuur 16
Individuen hebben vaak diverse identiteiten op internet (bron: http://sociacard.com)

ACHTERGROND

Internetonderzoek maakt een steeds groter deel uit van operationele onderzoeken door opsporings- en veiligheidsdiensten. Dit kan gaan om onderzoek naar activiteiten waar het internet als medium gebruikt wordt voor illegale activiteiten, maar vaak ook betreft dit het raadplegen van het Internet als informatiebron bij onderzoeken in de breedte. In beide gevallen is sociale media een belangrijke bron van informatie. Onder sociale media verstaan we[4]:

> Sociale media zijn een verzamelbegrip voor online platformen waar gebruikers, met geen of weinig tussenkomst van een professionele redactie, de inhoud verzorgen. Tevens is er sprake van interactie en dialoog tussen de gebruikers onderling.

4 Resultatenboekje topic 3, 2011.

Wanneer onderzoek naar individuen gedaan wordt, dan is het van belang om uitingen op sociale media te kunnen relateren aan waar het individu onderzoek naar gedaan wordt. Op het internet in het algemeen en sociale media in het bijzonder maken mensen gebruik van meerdere online identiteiten: een alias of nickname, een e-mailadres etc. Vaak is een online identiteit gekoppeld aan een specifiek sociaal medium. In veel gevallen vermelden ze niet hun fysieke identiteit: hun eigen naam. Omdat mensen middels hun verschillende online identiteiten verschillende gedaanten aannemen op het internet is het lastig om een compleet beeld op te bouwen over een individu. Wanneer dit beeld niet gevormd kan worden neemt dit het risico met zich mee dat verkeerde conclusies worden getrokken uit de incomplete data, de stukjes informatie die wel beschikbaar zijn niet geduid kunnen worden omdat de context ontbreekt.

Daarom is het relevant om de identiteiten die behoren bij hetzelfde individu bijeen te brengen: dit biedt de aanknopingspunten om het beeld compleet te krijgen en de beschikbare informatie over een individu in context te kunnen plaatsen.

Dit bijeenbrengen van informatie over bijvoorbeeld een persoon, groep, zaak of fenomeen wordt ook wel profiling genoemd. Profiling is het zoeken naar, combineren van, en redeneren met informatie in open en gesloten bronnen, maar ook het toeschrijven van eigenschappen aan een persoon of groep (bijvoorbeeld op basis van statistieken). Het aan elkaar verbinden van de identiteiten die iemand gebruikt in de fysieke en/of online wereld is hier onderdeel van. Andere varianten van profiling komen voor in literatuur, zoals het opstellen van een voorstellend profiel; daar is hier geen sprake van. Hier staat het bijeenbrengen van feitelijke informatie uit open bronnen centraal.

PROBLEEMSTELLING

Op basis van interviews die we met vertegenwoordigers uit het veld hebben afgenomen ontstaat het beeld dat profiling momenteel slecht ondersteund wordt met tooling. Het nadeel van deze situatie is dat het bijeenbrengen en vergelijken van identiteitsinformatie momenteel een tijdrovend proces is, en dat de mate waarin dit succesvol gebeurt sterk afhankelijk is van de persoon en de ervaring van de digitaal analist.

Er zijn veel situaties denkbaar waarbij er niet veel tijd is om een beeld op te bouwen, bijvoorbeeld in geval van een acute dreiging, in geval van grote hoeveelheden onderzoeken die in kort tijdsbestek moeten worden uitgevoerd, of wanneer de (online) gebeurtenissen rond een evenement zich in razendsnel tempo ontwikkelen zoals bij het recente Project-X slagveld in het Groningse Haren. In dergelijke situaties is er behoefte aan een snelle duiding van de online informatie.

Als startpunt van dit werkpakket stellen we dan ook:

– De digitaal analist is gebaat bij een tool of dashboard dat hem/haar ondersteunt bij het snel bijeenbrengen van de identiteiten behorende bij hetzelfde individu op basis van open bronnen.

In dit werkpakket dragen we hieraan bij door:

– Het verkennen van mogelijkheden om middels tooling sneller een beeld rond een individu op te kunnen bouwen, door informatie afkomstig van ditzelfde individu uit verschillende sociale media bronnen onder verschillende online identiteiten bijeen te brengen.

De bijbehorende onderzoeksvragen zijn:

1. Hoe kun je het proces van online profiling ondersteunen?
2. Welke informatie in sociale media profielen is bruikbaar om deze profielen aan elkaar te kunnen relateren?

SCOPE EN AFBAKENING

In sommige onderzoeken zal een fysieke identiteit van een individu bekend zijn, in andere gevallen slechts een of meerdere online identiteiten, in enkele gevallen beide. Afhankelijk van het type onderzoek, en welke informatie reeds beschikbaar is, ontstaat de behoefte om online identiteiten dan wel de fysieke identiteit van het individu te verzamelen. Op deze wijze onderscheiden we de volgende drie varianten:

Tabel 1
Verschillende vormen van het aan elkaar relateren van iemands fysieke en online identiteiten.

STARTPUNT:		ZOEKEN NAAR:	MET ALS DOEL:
1. Fysieke identiteit	→	Online identiteit	Informatie rond een bekend individu verzamelen
2. Online identiteit	→	Fysieke identiteit	Vaststellen wie iemand op het internet is
3. Online identiteit	→	Online identiteit	Beeld opbouwen rond een online identiteit.

Om te zorgen dat de resultaten voor een brede groep stakeholders toepasbaar zijn hebben we binnen het werkpakket de volgende afbakening gemaakt:

1. We raadplegen alleen open bronnen, met name zoekmachines (zoals Google, Bing etc.) en sociale media (waarbij de focus ligt op de “big 5”: Facebook, Twitter, LinkedIn, YouTube, Flickr aangevuld met Hyves);
2. We kijken in eerste instantie primair naar (Nederlandstalige) tekst. Technieken die werken op beeldinformatie, of die specifiek voor andere talen aangepast zouden moeten worden laten we dus buiten beschouwing;
3. We richten ons op het bijeenbrengen van de online identiteiten van een individu (variant 1 en 3 in tabel 1).

De volgende use beschrijft de rol van tooling in het proces van online identiteiten koppelen.

De politie komt een dreigtweet op het spoor van een twitteraar met als gebruikersnaam '@dreigerhenk'. De politie is in staat om met tooling snel mogelijke andere online identiteiten (en bijbehorende content die door deze persoon is gepost) te achterhalen waarmee deze persoon op Twitter en andere sociale media fora actief is. De mogelijke identiteiten worden op een overzichtelijke wijze aan de analist getoond in aflopende volgorde van waarschijnlijkheid. De analist valideert de voorgestelde identiteiten en/of onderdelen van de voorgelegde profielen. Het bijeenbrengen van informatie afkomstig van dezelfde persoon ondersteunt de analist bij het inschatten van de ernst van de dreiging en de dreiger.

Figuur 17 illustreert deze use case. Hier is het startpunt een online identiteit. In andere gevallen kan het startpunt een fysieke identiteit zijn, bijvoorbeeld de eigennaam van een persoon.

Figuur 17
In de use case wordt uitgaande van een dreigtweet en bijbehorende online identiteit (@dreigerhenk) gepoogd om een overzicht te creëren van de online identiteiten behorende bij hetzelfde individu. De tweet is daadwerkelijk aangetroffen, de online identiteiten zijn gefingeerd.

OVERZICHT VAN RESULTATEN

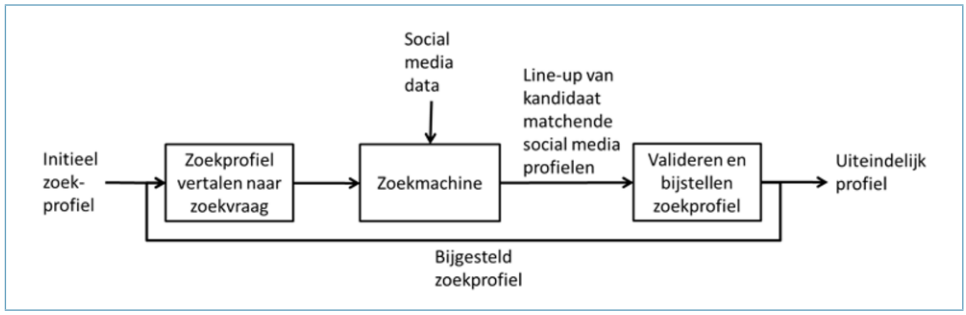
Dit werkpakket levert de volgende resultaten op:

1. Een analyse van functionaliteit die nodig is voor het aan elkaar kunnen relateren van online identiteiten;
2. Een analyse van informatie in sociale media die bruikbaar kan zijn voor het aan elkaar kunnen relateren van online identiteiten;
3. Een experimentele beproeving van de bruikbaarheid van enkele stukken informatie voor het aan elkaar kunnen relateren van online identiteiten.

Deze resultaten worden bijeengebracht in een TNO rapport; dit bevat de detailinformatie waar in dit boekje geen plek voor is.

Analyse van benodigde functionaliteit

Aan de hand van het volgende blokschema hebben we de use case over de dreigtweet van @dreigerhenk vertaald naar functionaliteiten.

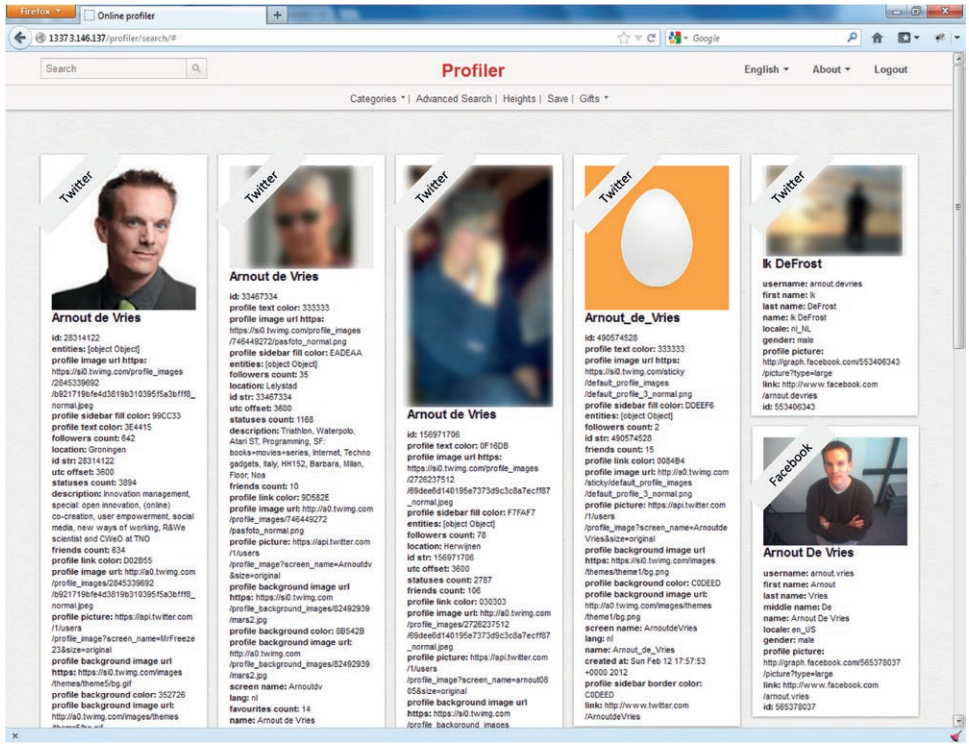


Figuur 18
Blokschema met stappen om iteratief een profiel op te bouwen rond een individu, een middels steeds nieuwe zoekslagen te pogen om de online identiteiten behorende bij dit individu in een profiel bijeen te brengen.

Startpunt in figuur 18 zijn een berg data in sociale media (boven), en een informatiebehoefte bij een analist die alle beschikbare informatie bijeen gebracht heeft in een initieel zoek-profiel (geheel links). Als het goed is komt er zo gedurende het onderzoek steeds meer informatie boven water. Het meenemen van deze informatie kan weer betere resultaten opleveren. Daarom zien we een iteratief proces voor ons, waarbij de analist zijn zoekvraag steeds verder aanscherpt op basis van de dan beschikbare informatie.

Technisch gezien zijn we op zoek naar een zoekmachine die op basis van een zoekvraag een line-up geeft van de meest waarschijnlijke matchende sociale media profielen (midden). De line-up presenteert een lijst van sociale media profielen die in steeds minder sterke mate lijken op de ons ter beschikking staande informatie. Denk aan het resultaat van een Google query, maar dan met een line-up van sociale media profielen. Figuur 19 laat een screenshot

zien van een line-up uit de onderzoeksoftware die ontwikkeld wordt voor een experiment in het kader van dit onderzoek.



Figuur 19
Screenshot van de onderzoekstool waarin online profielen behorende bij 'Arnout de Vries' aan een analist getoond worden.

Op twee plekken in figuur 18 speelt de analist een cruciale rol waarin hij zo mogelijk gefaciliteerd moet worden:

1. Het zoekprofiel bestaat uit het totaal aan beschikbare informatie in een onderzoek en is nog geen kant-en-klare zoekvraag die een zoekmachine snapt; eerst moet een zoekvraag geformuleerd worden uit de beschikbare informatie. Denk hierbij aan het formuleren van een Google query. Achter de vertaling naar de zoekvraag gaat een hoop vakmanschap en kennis over zoekstrategieën schuil;
2. Ook kan de mens als geen ander de kwaliteit van de zoekresultaten beoordelen en relevante inzichten uit de zoekresultaten toevoegen aan de beschikbare informatie in het zoekprofiel.

Vergelijking van online profielen

We onderscheiden twee stappen:

1. In eerste instantie wordt middels bestaande internet zoekfunctionaliteit zoals Google en de zoekopties in de sociale media zelf een serie mogelijk gelijkende profielen verzameld. Uitdaging is om de selectie zo scherp mogelijk te maken op basis van de beschikbare informatie, zodat zo min mogelijk informatie wordt verzameld, maar tevens geen relevante profielen worden gemist;
2. Vervolgens kunnen de profielen op verschillende criteria met elkaar vergeleken worden. Dit hangt o.a. af welke informatie in het sociale medium opvraagbaar is. Grofweg kunnen de volgende types informatie gebruikt worden om sociale media profielen met elkaar te vergelijken:
   - De gebruikte alias zelf: lijken ze op elkaar of zijn ze zelfs identiek?
   - Overige profiel informatie, incl. persoonsgegevens en sociale netwerkinformatie;
   - De berichten en content zelf die geplaatst worden.

Bij een quickscan op bestaande tools zijn we tools tegengekomen die de gehele functionaliteit biedt.

Experiment

In een experiment realiseren en beproeven we een stuk van de functionaliteit benodigd voor het aan elkaar relateren van online profielen:

1. Het vertalen van beschikbare informatie naar een zoekvraag als input voor een online zoekmachine;
2. Het aggregeren van de zoekresultaten en deze overzichtelijk presenteren;
3. Het semi-automatisch aan elkaar relateren van de gevonden online identiteiten.

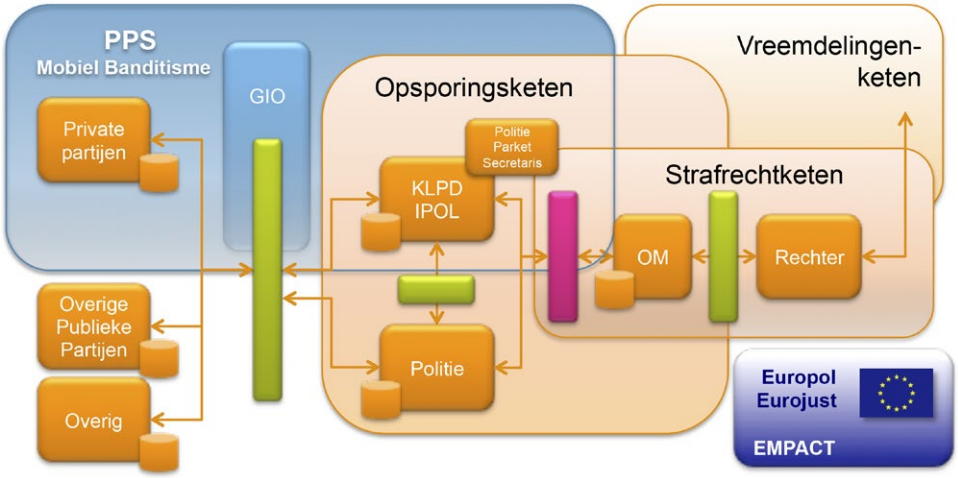
VOORLOPIGE CONCLUSIES

Online profiling gebeurt nu nog grotendeels handmatig. Semi-automatische tooling kan dit proces ondersteunen, specifiek bij het aan elkaar relateren van online identiteiten op sociale media. Het is van belang om de analist zo goed mogelijk te ondersteunen en in dit zoekproces te betrekken.

Let wel, dit werkpakket betreft een verkenning. Hierin zijn privacy by design aspecten meegenomen maar deze konden nog niet evenwichtig worden uitgewerkt, omdat dit afhangt van operationele implementatie. Bij verdere toepassing van deze kennis in producten moet het juridische kader een prominente rol spelen.

4.5 SELECT B4U COLLECT

Betrokken | Kees den Hollander (kees.denhollander@tno.nl), Marcel van Hekken, Fouad Gaddur, Julian de Wit en Tom Logtens



Figuur 20
De keten die zich bezighoudt met het bestrijden van mobiel banditisme

ACHTERGROND

Burgers en bedrijven worden in toenemende mate geconfronteerd met en zijn het slachtoffer van mobiel banditisme. Mobiel banditisme wordt op Europees niveau als volgt gedefinieerd: “Een mobiele (rondtrekkende) dadergroep is een vereniging van daders die zich stelselmatig verrijken middels vermogenscriminaliteit of fraude, een breed scala aan operaties uitvoeren en internationaal actief zijn.”

Zoals uit de definitie blijkt, plegen rondtrekkende bendes een breed scala aan vermogensdelicten: winkeldiefstallen, inbraken in woningen en bedrijven, oplichting, skimming, zakkenrollerij, diefstal van metalen, ladingdiefstal, voertuigcriminaliteit en diefstal op bouwplaatsen. Gegeven de huidige ontwikkelingen zijn door VenJ en het KLPD winkeldiefstallen, inbraken in bedrijven en voertuigcriminaliteit als het meest relevant geïdentificeerd.
Om deze grensoverschrijdende georganiseerde bendes effectief en efficiënt te bestrijden is een aanpak zowel op nationaal als op Europees niveau nodig. Deze aanpak gaat uit van een integrale set aan maatregelen voor zowel preventie, tegenhouden, opsporen en vervolgen van mobiel banditisme. Daarbij wordt zoveel mogelijke aangesloten op initiatieven en mogelijkheden op Europees niveau om mobiele bendes te bestrijden.

In figuur 20 zijn schematisch de verschillende partijen en ketens weergegeven die samenwerken bij de aanpak van mobiel banditisme. Naast de opsporings-, strafrecht- en vreemdelingenketen zijn dat private partijen die met de publieke partijen samenkomen in de nog op te richten GIO PPS: Gemeenschappelijke Informatie Organisatie Publiek Private Samenwerking. De GIO heeft als doelstelling om de verschillende partijen effectiever te laten opereren door de afzonderlijk geregistreerde en bewerkte gegevens te normaliseren, te sorteren, te filteren, te analyseren en te combineren.

Een specifiek aandachtspunt bij de integrale aanpak van mobiel banditisme is dat de vervolging van daders in de strafrechtketen onvoldoende geborgd is, omdat de beschikbare gegevens kennelijk tot onvoldoende prioriteitstelling leiden in relatie tot de beschikbare capaciteit. Hierdoor is de kans groot dat dadergroepen in een later stadium elders actief kunnen zijn.

Het werkpakket 'Select B4U Collect' heeft zich in 2012 gericht op de procesgang, informatiebehoefte, gegevensverzameling en bewerking, en keuzecriteria(indicatoren) omtrent de aanpak van mobiel banditisme in de in figuur 20 geschetste keten, met de nadruk op de opsporings- en strafrechtketen. 'Select before you collect' richt zich in deze context op zo goed mogelijke beslissingen over het inzetten van opsporings- en strafrechtcapaciteit op zaken die (mogelijk) zijn gerelateerd aan mobiel banditisme.

Betrokken zijn vertegenwoordigers van KLPD/IPol, Ministerie van V&J, het Openbaar Ministerie, Politie Rotterdam Rijnmond en Europol. De bevindingen en resultaten zijn getoetst in een plenaire bijeenkomst.

RESULTATEN

Op basis van interviews met de betrokken vertegenwoordigers is goed inzicht verkregen in de opsporings- en strafrechtketen. Uiteraard is ook gekeken naar de diverse lopende ontwikkelingen en initiatieven in nationaal en Europees verband.

Ten behoeve van het inzichtelijk maken van de complexe structuren in het systeem van mobiel banditisme en de opsporings- en strafrechtketen, is een globaal kwalitatief Systeem Dynamisch model ontwikkeld. Hiermee zijn de werking van verschillende causale relaties en een aantal mogelijke effecten van maatregelen en interventies gedemonstreerd. Deze methodiek heeft de potentie om de verdere ontwikkeling van een geïntegreerde aanpak mobiel banditisme te ondersteunen.

Als afgeleide van de bevindingen is in nauwe samenwerking met het KLPD/Dienst IPol een demonstrator ontwikkeld: de MoB Monitor (Mobiel Banditisme Monitor). De Dienst IPol heeft als experiment de demonstrator getoetst in lopende landelijke tactische operaties rondom mobiel banditisme. De functionaliteit blijkt een belangrijke aanvulling te zijn op de bestaande

analysetools van het KLPD bij de opsporing en monitoring van de verschillende vormen van vermogensdelicten van mobiel banditisme.

BEVINDINGEN

Het werkpakket heeft de volgende bevindingen over de keten opgeleverd:

1. Ondanks een aantal lopende initiatieven is er nog onvoldoende en bredere awareness over het fenomeen mobiel banditisme, zowel kwantitatief (omvang van de problematiek en van de gevolgen/schade) als kwalitatief (modus operandi van rondtrekkende dadergroepen / flexibele netwerken).
   Gevolg: Op het strategische/tactische niveau leidt dit tot het onvoldoende toekennen van de juiste urgentie en prioriteit aan het fenomeen. Op het operationele niveau wordt de context waarin een delict is gepleegd onvoldoende ingeschat. Bij de opsporing leidt dit er toe dat de keuze om een verdachte al dan niet langer dan zes uur vast te houden en/of verder te vervolgen zonder het besef van deze context en dus louter of capaciteitsgronden plaatsvindt.

2. Het kost erg veel inspanning om in het geval van een aanhouding van een verdachte voldoende informatie te krijgen over de totale context van de verdachte en het delict. Zowel de opslag als het delen van informatie is incompleet en versnipperd, regionaal, nationaal en Europees. Dit geldt zowel binnen de opsporings- en strafrechtketen als tussen deze ketens.
   Gevolg: bij de opsporing en vervolging is de verwachting vaak vooraf al dat drie dagen (laat staan zes uur) niet voldoende zullen zijn om een voldoende sluitend en compleet dossier over een verdachte op te bouwen. De prijs voor doorrechercheren is dan ook een groot beroep op schaarse recherchecapaciteit die vaak als onevenredig groot wordt ingeschat in relatie tot het delict, zeker wanneer dat niet in de juist context kan worden geplaatst (zie ook awareness bij punt 1).

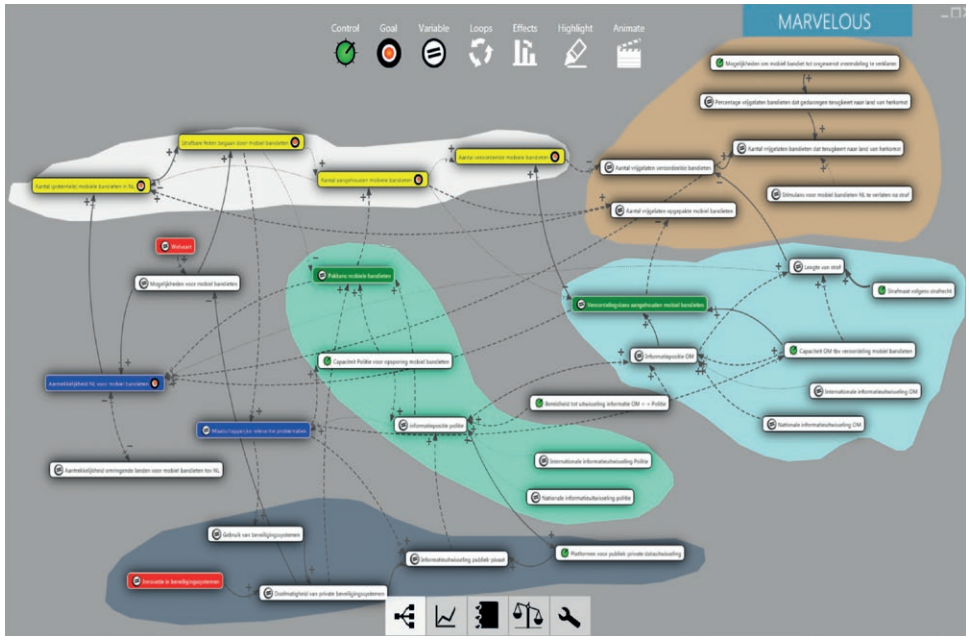
3. Er wordt te weinig gebruik gemaakt van internationale samenwerking en mogelijkheden tot informatie-integratie en coördinatie op Europees niveau. Europol heeft de faciliteiten om een Europees totaalbeeld op te bouwen op het gebied van mobiel banditisme. In de praktijk wordt echter maar een beperkt deel van incidentinformatie of andere gerelateerde informatie door de landen gedeeld met Europol.
   Gevolg: de informatiepositie van een coördinerend orgaan als Europol is onvoldoende. Dit leidt er toe dat landen vaak te weinig resultaat zien wanneer zij een bevraging bij Europol doen, waardoor ze toch weer zelf of bilateraal (‘old boys’) informatie verzamelen en uitwisselen. Hierdoor wordt nog minder informatie aangeleverd aan Europol en ontstaat een vicieuze cirkel.
   Eén niveau lager (nationaal) geldt ongeveer dezelfde redenering voor de positie van het KLPD/Dienst IPol (zie ook punt 2). De bevindingen over die positie uit 2011 (ref. [1]) geven hier waarschijnlijk ook een onderbouwing van.

4. De samenwerking in de keten, met name tussen opsporingsketen en strafrechtketen is onvoldoende (hangt ook samen met punt 2 over de informatiepositie). Er is geen afstemming over de processen. De actoren in de keten weten ook onvoldoende van elkaar welke criteria worden gehanteerd bij prioriteitstelling en welke informatie ze dus aan elkaar moeten aanleveren. Afstemming over begripsvormen (voorbeeld: “criminele samenwerkingsverbanden” versus “flexibele netwerken”) was beperkt, maar daar is inmiddels verbetering in aangebracht.
   Gevolg: er is geen integrale sturing en prioriteitstelling op en binnen de totale keten en de expertises worden niet gebundeld.

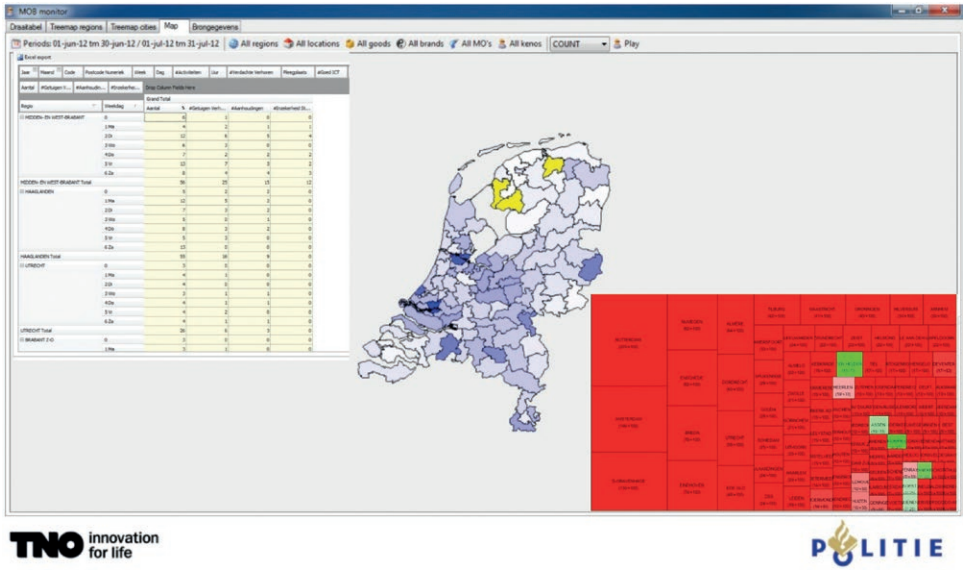
5. Diverse initiatieven worden benaderd vanuit één type vermogensdelict (winkeldiefstal, autocriminaliteit, inbraak, …).
   Gevolg: de informatie-integratie m.b.t. het fenomeen mobiel banditisme komt onvoldoende tot stand. Rondtrekkende dadergroepen / flexibele netwerken beperken zich niet tot één type vermogensdelict. Er is een grotere verbetering in de informatiepositie te behalen indien dergelijke initiatieven vanuit het fenomeen mobiel banditisme worden benaderd.

SYSTEEM DYNAMISCH MODEL MOBIEL BANDITISME (MARVELOUS)

Ten behoeve van het inzichtelijk maken van de structuren in het systeem van mobiel banditisme en de opsporing en vervolging hiervan, is een kwalitatief Systeem Dynamisch model ontwikkeld. Voor het maken van dit model is gebruikt gemaakt van de door TNO ontwikkelde software MarvelTool en MARVELOUS. Figuur 21 geeft een impressie van de samenhang van vijf verschillende ketens rondom mobiel banditisme: Problematiek-keten, Opsporingsketen, Private beveiligingssysteemketen, Strafrechtketen en Natraject. Hierin zijn naast aspecten als *capaciteit en informatiepositie ook aspecten als welvaart, de aantrekkelijkheid van Nederland voor mobiel banditisme en de maatschappelijke relevantie* van de problematiek meegenomen.



Figuur 21
Systeem Dynamisch model Mobiel banditisme (MARVELOUS)



Figuur 22
De Mobiel Banditisme Monitor (MoB Monitor)

DE MOB MONITOR

Als oplossingsrichting voor de eerste bevinding (een snellere en betere awareness over het fenomeen mobiel banditisme in beide ketens) is een demonstrator ontwikkeld als analysehulpmiddel voor het KLPD/Dienst IPol: de MoB Monitor.

Met de MoB Monitor zijn geospaciële en temporele trends, Modus Operandi en betrokken personen/flexibele netwerken op te sporen en te monitoren. Met de MoB Monitor kan bij het KLPD/Dienst IPol, samen met de andere KLPD-analysetools, inzicht verkregen worden in de mogelijke omvang van het fenomeen op landelijk niveau. Op dit moment wordt het inzicht verkregen op basis van de standaard politiegegevens (BlueView).

Het blijkt dat de functionaliteit ook goed geschikt is voor het monitoren van de kwaliteit van de brondata: consistentie en volledigheid van de proces-verbalen en eventuele veranderingen daarin door de tijd.
Figuur 22 geeft drie visualisaties weer van de MoB Monitor: statistiek (met goederenstromen en modus operandi), geospaciële en temporele trends.

CONCLUSIE EN VOORUITBLIK

De bevindingen maken duidelijk dat nog het nodige werk te verrichten valt. Bij alle bevindingen zijn overigens reeds de nodige initiatieven in de keten gaande. In dit werkpakket zijn stappen geïdentificeerd die sneller kunnen worden gezet en tot betere resultaten kunnen leiden.

De volgende stap is geïdentificeerd als meest kansrijke: het op basis van een betere informatiepositie beter (effectiever en efficiënter) samenwerken binnen en tussen beide ketens (i.e. Politie en OM) op dit fenomeen in de eerste zes uur van aanhouding. Dit moet bewerkstelligen dat een betere aansturing gedaan kan worden op de inzet van de schaarse capaciteit in de volgende fasen (drie dagen en drie weken) van aanhouding van personen en/of de identificatie van netwerken die zich bezighouden met mobiel banditisme.

Hiervoor moet nagedacht en geëxperimenteerd worden over de blauwdruk van deze samenwerking tussen Politie en OM op basis van een meer geïntegreerde ondersteunende informatie(verwerking). De eerste versie van het prototype MoB Monitor vormt hier een eerste bouwsteen in. Hierbij zijn drie dimensies onderkend in de genoemde samenwerking:
1. Nationaal/regionaal binnen de afzonderlijke opsporingsketen en strafrechtketen;
2. Nationaal en regionaal tussen opsporingsketen en strafrechtketen;
3. Internationaal (tussen nationale opsporingsketen en strafrechtketen enerzijds en Europol/Eurojust anderzijds).

Het werkpakket ‘Slimmer Samenwerken’ zal zich hier in 2013 op richten.

4.6 FYSIEKE FENOMENEN MET DIGITAAL COMPONENT

Betrokken | Carlijn Broekman (carlijn.broekman@tno.nl) Mirjam Huis in 't Veld, Marc Zinck, Joke Kort, Tom Bakker, Gijs Koot, Susan Tielkemeijer en Feyke Stadt

- Criminelen zien op open bronnen op internet wie op vakantie is, wie een nieuwe inboedel of een nieuwe auto gekocht heeft, en bieden gestolen goederen via marktplaats aan;
- Pedofielen zoeken contact op met jonge kinderen, vragen om foto's, telefoonnummers en video's die voor meerdere doeleinden worden gebruikt (onder andere chantage);
- Grote groepen mensen, al dan niet (notoire) geweldplegers gebruiken sociale media om tijd en datum van ontmoeten af te spreken.

Hoe verwerpelijke praktijken opgespoord kunnen worden vanuit technologische innovatie wordt al onderzocht. Anomaliedetectie en beeldanalyse zijn twee voorbeelden van technologieën die in ontwikkeling zijn om signalen van delicten vanuit de data aan het licht te brengen. Een relatief nieuwe benadering is echter om op een gestructureerde manier te kijken vanuit de gedragingen en gedragswetenschap. "In de fysieke wereld herkennen we potentieel verdacht gedrag; ik ben er van overtuigd dat deze kennis naar een digitale variant te vertalen is" Hylco Wijnants, RTR (Regionale Toezicht Ruimte) en Hoofd Bewaken en Beveiligen SGBO (Staf Grootschalig en Bijzonder Optreden).

Door vanuit kennis over gedrag naar de informatie op open bronnen op internet te kijken kunnen wellicht nieuwe methoden en werkwijzen geïntroduceerd worden. Wellicht kunnen patronen die mogelijk duiden op delicten ontdekt worden. In het werkpakket "Fysieke fenomenen met een digitale component" is de onderzoeksvraag dan ook: Kunnen verwerpelijke praktijken (sneller) aan het licht gebracht worden door gedragingen op open bronnen op internet te signaleren?

GEDRAG IN DE FYSIEKE WERELD

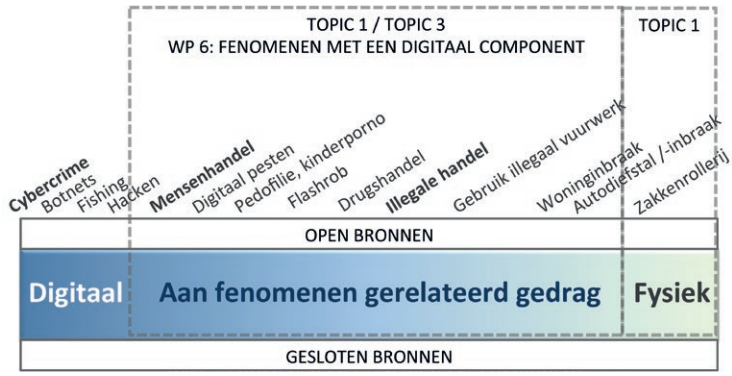
In topic 1 van het onderzoeksprogramma wordt onderzoek gedaan naar afwijkend gedrag, om kwaadwillenden vroegtijdig (automatisch) te signaleren. Hierbij zijn de uitdagingen het benoemen, en met behulp van slimme camera's automatisch herkennen van afwijkend gedrag. Afwijkend gedrag moet hierbij niet verward worden met verdacht gedrag. Afwijkend gedrag kan geheel verklaarbaar zijn, maar wijkt af omdat de massa zich anders gedraagt. Slechts een klein deel van het afwijkende gedrag leidt ook daadwerkelijk tot de constatering van verdacht gedrag (die bovendien gradaties van ernst kent).

GEDRAG OP INTERNET

De brede toepassingen van internet maken dit medium voor criminelen zeer bruikbaar. Het is dan ook heel aannemelijk dat het grootste deel van de delicten die in de fysieke wereld plaatsvinden, een digitale component hebben. De grootte van het digitale component verschilt per fenomeen, of zelfs per delict. Deze digitale component(en) kunnen voor, tijdens en/of na het plegen van het delict zitten.

DIGITAAL COMPONENT VOOR, TIJDENS EN/OF NA EEN DELICT

Wanneer iemand op internet kijkt wie een nieuwe auto heeft gekocht, deze vervolgens steelt, en te koop aanbiedt via internet, maakt hij voor, en na het delict gebruik van internet.



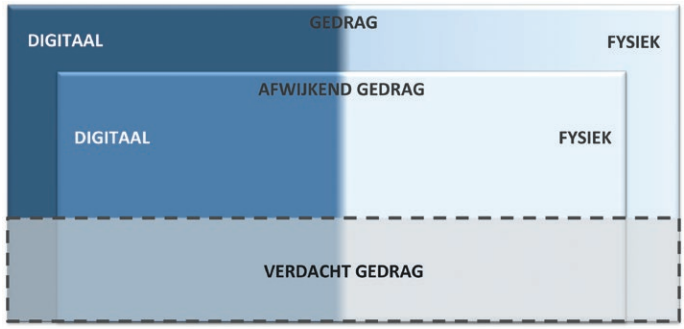
Figuur 23
Fenomenen hebben in grote of minder grote mate een digitale component. Gesloten bronnen en cybercrime vallen buiten de scope van dit onderzoeksprogramma. Op deze vorm van criminaliteit richt topic 5 zich.

De verwachting is dat, net als bij fysiek gedrag ook bij digitaal gedrag signalen te benoemen zijn die verband houden met het delict. Bij observatie vanuit een gedrag-perspectief wordt gekeken naar de modus operandi, in plaats van naar de effecten op zich (de data). Deze nieuwe manier van kijken zal resulteren in het stellen van andere vragen, en daarmee het verkrijgen van nieuwe inzichten

Net als in de fysieke wereld geldt ook voor de digitale wereld dat afwijkend gedrag niet verward moet worden met verdacht gedrag. Na het benoemen van afwijkend gedrag is het de uitdaging om uit de afwijkende gedragingen verdacht gedrag te destilleren. Een andere uitdaging is om verdacht gedrag dat niet vanuit afwijkende gedragingen onder de aandacht is gekomen toch te signaleren.

DIGITAAL AFWIJKEND GEDRAG IS NIET ALTIJD VERDACHT GEDRAG

Het is niet gebruikelijk dat een veertigjarige man grotendeels jonge kinderen in zijn Facebook-netwerk heeft zitten. Echter, voor leraar van een basisschoolklas is het wel te uit te leggen.



Figuur 24
Niet alleen in de fysieke wereld, maar ook in de digitale wereld is afwijkend gedrag te signaleren. Afwijkend gedrag hoeft niet, maar kan wel verdacht gedrag zijn.

Bij deze nieuwe benadering van kijken naar open bronnen op internet wordt de kennis van TNO over gedragswetenschap en over digitale open bronnen samengevoegd, met als doel nieuwe inzichten krijgen, die bijdragen aan handhaving en opsporing.

RESULTAAT 2012

Het onderzoek waarbij kennis van gedrag en afwijkend gedrag wordt samengevoegd met kennis van open bronnen op internet is in de tweede helft van dit jaar gestart. Het onderzoek bestaat uit drie verschillende onderzoekslijnen. Voorlopige resultaten en de toegevoegde waarde van de resultaten zijn hier opgesomd.

1. Verkenning potentie gedragsperspectief

Vanuit het gedragsperspectief in het algemeen, en vanuit afwijkend gedrag in het bijzonder kijken naar open bronnen op internet is een relatief nieuw onderzoeksveld. Het doel van het onderzoek voor 2012 is daarom een inventarisatie naar de potentiële toegevoegde waarde van kennis over digitaal gedrag in open bronnen, voor handhaving en opsporing. Deze inventarisatie wordt gemaakt door vijf onderzoeksmethoden te combineren:

1. Desk research in open bronnen en kranten, naar gebruik van open bronnen op internet door criminelen en bij handhaving en opsporing;
2. Literatuurstudie;
3. Enquête op internet onder deskundigen en burgers (nationaal en internationaal);

4. Besloten (diepte) interviews met deskundigen;
5. “Red-teaming SWOT” analyse (red team perspectief; welke kansen en bedreigingen, sterkten en zwakten bieden open bronnen op internet voor criminelen).

Deze exercitie zal resulteren in een long-list aan fenomenen, en de hieronder vallende delict-typen, met mogelijke invullingen van de digitale componenten voor, tijdens en na het delict. De mogelijkheden die open bronnen op internet bieden voor criminelen (kansen en sterkten) en voor veiligheidsautoriteiten (bedreigingen en zwakten) worden verlevendigd in de red-teaming SWOT. Door te denken vanuit de (on)mogelijkheden die criminelen hebben, is het beter mogelijk om criminelen te vinden; ‘je gaat daar zoeken waar je jezelf zou verstoppen’. De enquêteresultaten tot nu toe zijn veelbelovend. Ze laten zien dat bijna 60% van de respondenten verwacht dat criminelen sporen nalaten op open bronnen op internet[5]. Respondenten noemen verschillende signalen van activiteiten op open bronnen op internet die verband kunnen houden met delicten.

De inventarisatie van de toegevoegde waarde die het kijken naar open bronnen op internet vanuit het gedragsperspectief zal resulteren in een conclusie en aanbevelingen. Deze aanbevelingen zijn gericht op vervolgonderzoek en diverse vormen van aanpak, maar bevatten daar waar mogelijk ook pragmatische aanbevelingen die nu al toegepast kunnen worden.

2. ContextCreator experiment

Eerder onderzoek heeft TNO al in staat gesteld om afwijkende, en zelfs dreigende tweets te destilleren uit de massa aan tweets die dagelijks verstuurd wordt. Het is echter nog een grote uitdaging om in een selectie van afwijkende tweets vast te stellen of het om verdacht gedrag gaat, en er dus daadwerkelijk een dreiging is, of dat de tweet grootspraak betreft. Ook is het lastig een inschatting te maken van wanneer een kantelpunt wordt bereikt waarop gezellige drukte overslaat in chaos. De berichten zijn lastig op waarde te schatten doordat een context mist. Hierdoor wordt óf op alle afwijkende berichten geacteerd, óf er wordt niet gereageerd. Op alles reageren is een overreactie die veel capaciteit kost, en lijkt niet nodig. Het tegenovergestelde, niet reageren, is ook is niet wenselijk. Wellicht zijn sommige tweets wel degelijk vanuit een slechte intentie verstuurd. De hybride oplossing waar nu vaak voor gekozen wordt is het fingerspitzengefühl. Om het percentage afwijkend gedrag, in verhouding tot verdacht gedrag, te verkleinen worden acties naar aanleiding van afwijkende tweets soms groots in het nieuws gebracht. Om meer structuur te geven aan het omgaan met de grote aantallen tweets die afwijkend, en zelfs dreigend zijn, is een quasi[6]-experiment ontworpen. Hierbij is een context rondom een afwijkende tweet te creëren door te 'porren'. Dit kan de informatiepositie verbeteren, om zo in te schatten of een bericht serieus genomen moet worden. Bovendien kan er ook een preventieve werking vanuit gaan.

5 Deze resultaten zijn gebaseerd op het eerste deel van de enquête-data en de interviews
6 Een quasi-experiment is een experiment waarbij niet alle variabelen gecontroleerd kunnen worden

CONTEXTCREATOR, EEN VOORBEELD

Tweet: “vanavond rellen @Marciniplein, ik stek een mes tussen je ribben@maxdriksen”. Hierop kan gekozen worden voor de ‘por-optie’ de verzender te gaan volgen als politie-account. Hiermee wordt iemand uit de anonimiteit gehaald. De ervaring van de politie heeft geleerd dat iemand uit de anonimiteit halen een succesvolle preventieve interventie is.

De ContextCreator moet ervoor zorgen dat een tweet beter op waarde geschat kan worden. Dit wordt beoogd door verschillende (subtiele) interactie-alternatieven op te sommen (een zogenaamde digitale “por”). Wanneer een afwijkende tweet gesignaleerd is kan gekozen worden voor de best passende soort “por”. Wanneer zo’n subtiel signaal vanuit de politie is verstuurd is het zaak de reactie van de ontvanger en omgeving te observeren. Deze reactie vormt de context, zodat de eerder gesignaleerde tweet afgedaan kan worden als afwijkend gedrag, of de conclusie getrokken kan worden dat het hier mogelijk gaat om verdacht gedrag. In het laatste geval kan opnieuw bekeken worden welke handeling wenselijk is. De ContextCreator moet het aantal ‘loze’ acties naar aanleiding van sociale media berichten terugdringen, en het aantal ‘terechte’ acties vergroten.

We zijn ons er van bewust dat we rekening moeten houden met de privacy wetgeving en andere juridische kaders voor er op deze manier informatie verzamelt kan worden van internet.

Het quasi-experiment wordt nog uitgevoerd, maar de reacties vanuit de politieorganisatie zijn voorzichtig en enthousiast, mits het op preventie is gericht en eventuele vervolging niet wordt beïnvloedt. Dit quasi-experiment zal zorgvuldig uitgevoerd worden, want er wordt contact gezocht met burgers, en iedereen kan meekijken.

3. Technologie

De grote hoeveelheden berichten op open bronnen maken het in sommige gevallen onmogelijk afwijkingen te signaleren. De aantallen worden te groot om een norm te kunnen herkennen. In dergelijke gevallen kan innovatieve technologie een belangrijke bijdrage bieden. Bijvoorbeeld netwerkanalyse technologie kan helpen bij het definiëren van een norm.

Internet surveillance speelt een rol bij het herkennen van signalen op het internet. Variërend van de Habbo hotel rechercheur en wijkagenten tot meer algemene (nationale en internationale) surveillance is men gericht of generiek op zoek naar signalen die duiden op mogelijke misstanden.

Specifieke vormen van internet surveillance kunnen worden toegepast om gedragstheorieën te valideren en signalen die aangereikt worden door de brede groep (wisdom of the crowd middels de enquête) te toetsen en daarnaast kunnen effecten naar aanleiding van “online porren” (2) waargenomen worden.

VOORLOPIGE ONDERZOEKSAGENDA

Op basis van de onderzoeksresultaten van 2012 zal een onderzoeksagenda voor 2013 worden samengesteld. De resultaten van de enquêtes en interviews tot nu toe tonen dat er grote behoefte is naar meer kennis over digitaal gedrag dat verband houdt met delicten. Vervolgonderzoek kan gericht zijn worden op de digitale modus operandi waarbij open bronnen gebruikt worden.

Ook de verwachtingen van de ContextCreator zijn hoog. Het quasi-experiment dat eind 2012 uitgevoerd wordt zal eerste inzichten bieden. In 2013 kan hier verdiepende kennis opgebouwd worden.

5 DOELSTELLING 2013

In overleg met de behoeftestellers is de focus voor 2013 gelegd op de domeinen handhaving en de strafrechtketen (opsporing). Hierbij wordt handhaving ruim gezien en ligt er een belangrijke link met crisisbeheersing. De ontwikkeling van real-time intelligence is een verbindende ontwikkeling.

De primaire behoefte in het vraagstuk is: Het slimmer (efficiënter en effectiever) afstemmen van informatievraag en informatieaanbod waarbij toegesneden technologie het proces en de mens zo goed mogelijk ondersteunt.

Door de jaren 2011-2014 zal er in de ontwikkeling van de innovatieve (deel)concepten een steeds verdergaande staat van volwassenheid (in breedte en diepte) worden bereikt. Expliciete aandacht zal uitgaan naar die innovaties die kostenbesparend werken.

In 2013 ligt de focus op:

- Innovatie in de toepasbaarheid, effectiviteit en efficiëntie op het gebied van informatie-analysetechnieken (incl. datamining);
- Innovatie in de wijze waarop de professionals in het veld de nieuwe technieken kunnen adopteren/hanteren.

De toepasbaarheid van de innovaties in de werkwijze van de operationele veiligheidsdiensten wordt bij deze focus meegenomen, evenals privacy en vertrouwelijkheid, waar dit relevant is.

De ontwikkelde kennis wordt gevalideerd door experimenten en/of (expert)workshops in samenwerking met partijen uit het veld zoals de politie.

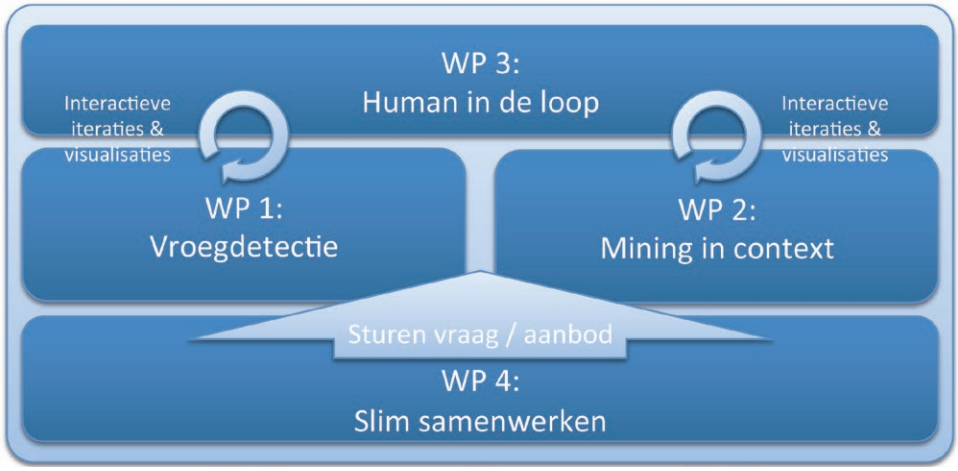
Door de spelers in de veiligheidsketen (Politie, Ministerie van BZK, NCTV, OM, Mininisterie van V&J) wordt op veel plaatsen geëxperimenteerd met inzet van nieuwe media en open bronnen ten behoeve van opsporing (informatie inwinnen en verspreiden): bijvoorbeeld de twitterende wijkagenten en het gebruik van sociale netwerksites bij opsporingsverzoeken. Wat minder zichtbaar zijn de verschillende manieren waarop uit de beschikbare informatie de relevante kennis wordt vergaard ten einde handhaving of opsporing te versnellen. In het rapport data voor daadkracht wordt dat als volgt verwoord: ‘er blijkt een veelheid aan benaderingen te zijn, waarbij elke organisatie zijn eigen systematiek en werkwijze kent. In de praktijk blijven belangrijke elementen van de data buiten beschouwing’ … ‘dat heeft met een grote mate van waarschijnlijkheid tot gevolg dat op het veiligheidsterrein verbanden over het hoofd worden gezien’ …’daardoor worden minder resultaten bereikt dan mogelijk.’

GEWENSTE SITUATIE:

In de gewenste situatie is duidelijk welke informatie nodig is voor het kunnen uitvoeren van de verschillende veiligheidstaken, waar die informatie gehaald wordt (wie genereert die) en hoe deze moet worden inzet om snel het beoogde resultaat te kunnen halen. Technologie is hierin ondersteunend, de effectiviteit en efficiëntie van het informatieproces is leidend.

Voor het bereiken van de doelstelling van het werkpakket in 2013 dienen tenminste de volgende onderzoeksvragen te worden beantwoord, die zijn gedefinieerd in overleg met de stakeholders van topic 3:

1. Vroegsignalering van dreigingen
2. Data mining in context;
3. The human in the loop: Interactie en Visualisatie;
4. Slim samenwerken.



Figuur 25
Samenhang tussen de werkpaketten in 2013

5.1 WP1: VROEGSIGNALERING VAN DREIGINGEN

Projectleider | Henri Bouma (henri.bouma@tno.nl)

Het herkennen en voorspellen van dreigingen, zowel acuut als gradueel opgebouwd over de tijd, gericht tegen personen, objecten, diensten en/of evenementen in het rijks en decentraal domein.

ACHTERGROND

De stakeholders hebben aangegeven dat het tijdig herkennen van dreigingen een hoge prioriteit heeft. De afgelopen jaren is gewerkt aan anomaliedetectie voor internet surveillance. Dit heeft geleid tot een framework dat de inhoud van berichten analyseerd en dat goed kan gaan werken voor het tijdig herkennen van dreigingen. Het framework is getest en dient nu met grotere hoeveelheden en een grotere verscheidenheid aan data gevalideerd te worden.
Naast toepassing van reeds opgedane kennis wordt in het werkpakket een centrale plaats gegeven aan verdere kennisopbouw en vernieuwing van de methode. Hierbij wordt de validatie van het systeem en interactie met de gebruikers benut om verbeterpunten te identificeren om gericht verbeteringen te kunnen aanbrengen. Evaluatie van het verder uitgewerkte framework zal geschieden door middel van een aantal concrete diverse cases, die als ultieme test zullen fungeren voor de ontwikkelde early-threat detection.

ONDERZOEKSVRAGEN

- Hoe goed werkt het ontwikkelde framework op verschillende concrete cases en wat zijn de verbeterpunten?
- Hoe kan early-threat detection worden verbeterd?

RESULTAAT

Demonstratie en evaluatie op diverse cases en gerichte verbetering van het algoritme en methodiek.

5.2 WP2: DATA MINING IN CONTEXT

Projectleider | Egon L. van den Broek (egon.vandenbroek@tno.nl)

DOEL

Het verwerken van data tot informatie in haar context. Onder context wordt hier verstaan: de totale omgeving waarin informatie (bijvoorbeeld een situatie of een gebeurtenis) zijn betekenis krijgt. Dit kan een jeugdbende (groep) betreffen, een wijk (gebied), of bijvoorbeeld een demonstratie of voetbalwedstijd (situatie), waar problemen dreigen te ontstaan dan wel reeds zijn ontstaan. Door een dergelijke context-aware data mining kan de daadwerkelijke waarde van data beter bepaald worden. Hierbij is van belang dat data retrieval, filteren en analyseren allen aangepast kunnen worden afhankelijk van de specifieke situatie.

ACHTERGROND

Open bronnen onderzoek zal een steeds groter onderdeel van veel (recherche) onderzoek worden. Waar analyses van gesloten bronnen reeds door de jaren heen steeds verder geautomatiseerd zijn en ondersteund worden door tools is dit voor open bronnen tot op heden slechts zeer beperkt het geval. Het aantal en de verscheidenheid aan databronnen alsook de resulterende hoeveelheid en verscheidenheid aan data neemt hand over hand toe. Hierdoor wordt het voor een digitaal rechercheur en/of analist steeds moeilijker om tijdig de relevante data op het internet op te sporen en de waarde hiervan in te schatten.

RESULTAAT

De stakeholders hebben aangegeven dat het moeilijk is om (tijdig) de waarde te bepalen van data dan wel informatie te herkennen, terwijl dit wel een hoge prioriteit heeft. Dit werkpakket richt zich op het plaatsen van data in haar context en zo het bovengenoemd probleem te verlichten. Daarom zal in het bijzonder aandacht worden gegeven aan de volgende aspecten van context-aware data mining:

- Diepgaande analyse en ondersteuning van het zoekproces van de rechercheur. Hierbij zal bijvoorbeeld gebruik worden gemaakt van mental maps (om mogelijke tunnel visie te doorbreken), hitlists (om bronnen te categoriseren) en automatisch gegenereerde rapportages (om efficient grotere hoeveelheden data te kunnen analyseren).
- Bepalen van de fysieke en/of de virtuele context van data/informatie. Bijvoorbeeld, is er door de uitzetting van krakers in een stadsdeel reeds een toegenomen spanning onder hen? of kan het profiel van bepaalde verdachten worden bepaald?

- Bepalen van de beschikbare (achtergrond)kennis en informatie behoefte binnen een zaak van een rechercheur of onderzoeksteam. Bijvoorbeeld, hoe was de aanloop naar eerdere rellen, welke signalen waren er toen en in hoeverre zijn vergelijkbare patronen nu zichtbaar? Zijn er trends zichtbaar en waaien trends in de ene stad over naar een andere?

Er wordt geanticipeerd op de optimalisatie van het zoekproces door automatisering waar mogelijk beschikbaar te stellen en hierbij vooral ook data(bronnen) te koppelen.

Het te ontwikkelen context-aware data mining systeem zal gedemonstratreerd en geevalueerd worden. Het systeem zal worden vergeleken met zowel de best practices uit het veld als met het systeem dat in 2012 binnen WP4 (en WP2) van topic 3 ontwikkeld is. Centraal zal staan dat de analist/rechercheur het beoogde systeem naar wens kan aanpassen, zoekstrategieën kan ontwikkelen voor bepaalde domeinen (en deze met een bepaalde frequentie geautomatiseerd uitvoeren) en feedback kan geven aan het systeem op basis waarvan het systeem zich aanpast. Om dit alles te realiseren zal ook nauw worden samengewerkt met de drie andere werkpakketten binnen topic 3.

5.3 WP3: THE HUMAN IN THE LOOP INTERACTIE EN VISUALISATIE

Projectleider | Erik Boertjes (erik.boertjes@tno.nl)

DOEL

Dit werkpakket onderzoekt hoe de mens 'in de loop' kan worden gebracht bij de analyses die in de veiligheidsketen plaatsvinden.

ACHTERGROND

In de andere werkpakketten worden een aantal componenten en methoden ontwikkeld voor automatische informatie analyse. De resulterende analyseketen zal echter niet geheel automatisch werken: de mens speelt nog steeds een belangrijke rol in de keten, bijvoorbeeld omdat:

- Het gedrag van sommige componenten instelbaar is (bijvoorbeeld de drempelwaarde in een anomalie-detectiecomponent). Dit instellen zal door de gebruiker moeten worden gedaan;
- Er uitleg nodig is over de manier waarop automatische analyses tot hun resultaten zijn gekomen, en de betrouwbaarheid van die resultaten;
- De resultaten van analyses niet altijd 100% correct zullen zijn en handmatig moeten kunnen worden aangepast;
- De resultaten van analyses in hun context moeten worden gepresenteerd.

Een belangrijk onderdeel van dit werkpakket is onderzoek naar geschikte vormen van interactie, zoals datavisualisatie. Datavisualisatie is het grafisch weergeven van data met als doel de capaciteiten van het menselijk visueel systeem (het identificeren van patronen) optimaal te benutten. Visueel gepresenteerde gegevens worden sneller en effectiever geïnterpreteerd dan in verbale of numerieke presentaties.

In zowel WP1 als WP2 is het noodzakelijk om de mens nauw te betrekken in de analyse keten.

VROEGSIGNALERING VAN DREIGINGEN (ZIE WP1)

Hier is sprake van een aantal plekken in de keten waar menselijke input belangrijk is:

- Datacollectie: de gebruiker geeft aan op welke onderwerpen gezocht moet worden;
- Feature extractie: de gebruiker krijgt inzicht in de elementen die uit de gevonden data zijn gehaald, en kan de elementen aanpassen en uitbreiden;
- Anomaliedetectie: de gebruiker krijgt inzicht in de manier waarop het systeem anomalieën heeft gedetecteerd en kan eventueel parameters in het algoritme aanpassen.

Visualisatie speelt een belangrijke rol in het presenteren van de resultaten van de anomaliedectectie-keten, bijvoorbeeld in de vorm van een realtime 'early warning' dashboard.

DATA MINING IN CONTEXT (ZIE WP2)

Menselijke interactie vindt hier plaats bij:

- Het door de gebruiker aanpassen van relaties tussen concepten, verwijderen van irrelevante concepten, of het toevoegen van nieuwe concepten. Deze gewijzigde set aan concepten en relaties vormt een nieuwe zoekopdracht: de gebruiker kan op een visuele manier zoekopdrachten samenstellen.

Visualisatie laat de gevonden concepten te midden van hun context zien. Daarnaast wordt de zoekhistorie bijgehouden en in kaart gebracht zodat de gebruiker gemakkelijk de 'afgelegde route' kan zien en eventueel terug kan keren naar een eerdere afslag.

RESULTAAT

Richtlijnen, geïllustreerd met een tweetal proof of concepts, voor het betrekken van menselijke interactie in de beide analyseketens van WP1 en WP2.

5.4 WP 4: SLIM SAMENWERKEN

Projectleider | Kees den Hollander (kees.denhollander@tno.nl)

ACHTERGROND

In het werkpakket Select B4U Collect (2012) is op het fenomeen Mobiel Banditisme[7] een inventarisatie uitgevoerd naar de aanpak en aansturing daarvan in de opsporings- en strafrechtketen (KLPD, Openbaar Ministerie, Ministerie van V&J, Politieregio's), en is op basis van de bevindingen een aantal oplossingsrichtingen voor de geïnventariseerde problemen geschetst..

Uit één van de bevindingen bleek dat een snellere en betere awareness over het fenomeen Mobiel Banditisme in beide ketens gecreëerd moet worden om een effectieve en efficiënte aanpak te waarborgen. Als oplossingsrichting hiervoor is begonnen met de uitwerking van een eerste prototype analysehulpmiddel voor het KLPD (MoB Monitor: spaciële en temporele trends, MO's, betrokken personen en links). Met de MoB Monitor kan bij het KLPD, samen met andere KLPD-analysetools, een eerste inzicht verkregen worden in de mogelijke omvang van het fenomeen op landelijk niveau op basis van de standaard politiegegevens (BlueView).

In combinatie met een aantal andere bevindingen is de volgende stap geïdentificeerd als meest kansrijke oplossingsrichting: het op basis van een betere informatiepositie beter (effectiever en efficiënter) samenwerken binnen en tussen beide ketens (i.e. Politie en OM) op dit fenomeen in de eerste zes uur van aanhouding[8]. Dit moet bewerkstelligen dat een betere aansturing gedaan kan worden op de inzet van de schaarse capaciteit in de volgende fasen (3 dagen en 3 weken) van aanhouding van personen en/of de identificatie van flexibele netwerken.
Hiervoor moet nagedacht en geëxperimenteerd worden over de blauwdruk van deze samenwerking tussen Politie en OM op basis van een meer geïntegreerde ondersteunende informatie(verwerking). De eerste versie van het prototype MoB Monitor vormt hier een eerste bouwsteen in.

Er zijn drie dimensies onderkend in de samenwerking:
1. Nationaal/regionaal binnen de afzonderlijke opsporingsketen en strafrechtketen;
2. Nationaal en regionaal tussen opsporingsketen en strafrechtketen;
3. Internationaal (tussen nationale opsporingsketen en strafrechtketen enerzijds en Europol/Eurojust anderzijds).

7 Op dit moment zijn de top vier vermogensdelicten gepleegd door Mobiel Banditisme: winkeldiefstal en -inbraken, voertuigcriminaliteit en woninginbraken
8 Verificatie met KLPD, Openbaar Ministerie, Ministerie van V&J en Politieregio's op 12 november 2012

DOEL

Doel van dit werkpakket in 2013 is:

- Het ontwikkelen van een blauwdruk van de samenwerking binnen en tussen de opsporings- en strafrechtketen bij de aanpak van Mobiel Banditisme op basis van een meer geïntegreerde ondersteunende informatie(verwerking);
- Het beschrijven (en waar mogelijk demonstreren) van de functionaliteit van deze geïntegreerde ondersteunende informatie-omgeving;
- Het beschrijven van de toepasbaarheid van deze geïntegreerde ondersteunende informatie-omgeving voor andere cases.

ONDERZOEKSVRAGEN

- Welke informatie(producten) hebben de verschillende betrokkenen in de opsporingsketen en strafrechtketen nodig om in de eerste zes uur van aanhouding te kunnen beoordelen of een verdachte en/of incident (potentieel) onderdeel uitmaakt van een groter flexibel netwerk in het kader van Mobiel Banditisme? Wat is de inhoud van die informatie(producten)?
- Welke instanties en bronsystemen binnen de beide ketens zijn in staat om die informatie(producten) te maken en/of aan te leveren? Wat zijn de mogelijkheden en onmogelijkheden om op basis hiervan een geïntegreerde ondersteunende informatie-omgeving te creëren?
- Welke benodigde informatie(producten) en informatieverwerkende activiteiten worden in de huidige situatie niet ondersteund door (bron)systemen en/of applicaties? Hoe zou dergelijke funcationaliteit eruit moeten/kunnen zien?
- In hoeverre zijn de mogelijkheden om tot een geïntegreerde ondersteunende informatie-omgeving te komen ook toepasbaar voor andere cases en fenomenen?

RESULTAAT

Een oplossingsrichting voor een snellere awareness en analyse binnen de drie dimensies van samenwerking bij de aanpak van Mobiel Banditisme in de context van de zes-uurs-aanhoudingsperiode en een eerste inzicht in de toepasbaarheid hiervan voor andere cases en fenomenen.

6 SLOTWOORD

We verwachten bij het uitwerken van de werkpakketten van 2013 tot concrete handvatten te komen voor stakeholders waardoor zehun eigen informatieverwerking in goede banen kunnen leiden en stroomlijnen. De resultaten zijn ondersteunend voor het verder professionaliseren van het informatie- of intelligencegestuurd werken van de veiligheidsorganisaties. Het vormt de basis voor de processen intelligence, handhaving, opsporing, noodhulp en crisisbeheersing.

Concrete toepasbaarheid ligt vooral op het domein van de toezichtcentrales/meldkamers (Nationale Politie, KMar), (digitale) analysewerkzaamheden (onder andere BZK, NCTV, IPol, RIO), (internet) recherchewerkzaamheden (Nationale Politie, KMar) en ondersteuning van de informatiefunctie in het front-office/back-office concept (Nationale Politie).

In 2013 wordt de samenwerking met de huidige partijen gecontinueerd en verder uitgebreid om zo samen met u te bouwen aan een effectieve manier voor het omgaan met grote hoeveelheden informatie in de veiligheidsketen.

Wij hopen van harte dat u dit boekje zult aangrijpen als uitnodiging tot verdere samenwerking met TNO voor een veilige maatschappij.

BIJLAGE A. KENNISDELING

Op diverse momenten in het jaar zijn onderwerpen uit topic 3 onder de aandacht gebracht van diverse belanghebbenden. Hieronder een greep uit die bijeenkomsten:

- 3 april 2012
  Presentatie op vakdag opsporing: Sociale media en opsporing (BRR/BBR) Haaglanden

- 18 april 2012
  Symposium sociale media NIFV: social media monitoring. Zie meer info: http://www.nifv.nl/web/show/id=193299/contentid=3595

- 24 april 2012
  Presentatie van de resultaten werkpakket 'Anomaliedetectie' op conferentie 'SPIE Defence and Security' (VS)

- mei 2012
  Bezoek Minister Ivo Opstelten (Veiligheid en Justitie) aan TNO

- 18 juni 2012
  Programma onderdeel op HDIeF (Herkenning Digitale Informatie en Fingerprinting)

- 3 juli 2012
  Stakeholdersoverleg vraaggestuurde programma bij TNO

- 30 augustus 2012
  Bezoek Erik Akerboom (NCTV) aan TNO

- 10 september 2012
  Real-time intelligence bijeenkomst politie, VR's en industrie

- 16 oktober 2012
  Presentatie van de resultaten werkpakket 'Anomaliedetectie' op conferentie 'Information Technologies and Security' (Moldavie)

- 9 november 2012
  Bijeenkomst ProjectX (Social media analyse). Zie meer info: http://www.hetccv.nl/agenda/2012/11/bijeenkomst-project-x.html en http://www.hetccv.nl/dossiers/project-x/index

- 14 november 2012
  Bezoek Marc van Nimwegen, (Procureur Generaal, Openbaar Ministerie) en Hans van den Broek, (directeur Beleid & Strategie Openbaar Ministerie) aan TNO

- 15 november 2012
  Beurs voor Nederlandse Industrie voor Defensie en Veiligheid.

- 19 november 2012
  Virtueel buurtonderzoek bij woninginbraken (co-creatie 2.0). De scriptie van Richard Vriesde en Ellis Jeurissen, waarin bijdragen van TNO zijn verwerkt, is te vinden op http://www.criminaliteitswijzer.nl/wiki/index.php/Afbeelding:Scriptie_Co-creatie_2.0_Jeurissen&Vriesde_SLL8.pdf. Het landelijk programma Woninginbraak gaat met hun aanbevelingen aan de slag.

- 22 november 2012
  Vakdag opsporing Hollands Midden: cocreatie in opsporing

- 27 november 2012
  Presentatie op het congres Raad van korpschefs

- 10 december
  Stakeholdersoverleg vraaggestuurde programma bij TNO

In de veiligheidsketen is het noodzakelijk dat grote hoeveelheden informatie snel verwerkt worden tot bruikbare kennis. De hoeveelheid beschikbare informatie neemt de afgelopen jaren explosief toe, waardoor doorgaan op de huidige (veelal niet-geautomatiseerde) wijze van informatieontsluiting een te grote inzet van de menskracht zou vergen. Meer informatie is niet altijd beter en wegen de kosten voor het verzamelen en analyseren van informatie wel op tegen de resultaten? De uitdagingen waarmee de spelers in de veiligheidsketen worden geconfronteerd hebben betrekking op een overvloed aan informatie (informatie-overload), een tekort aan menselijke verwerkingscapaciteit (personele krapte) en de noodzaak om proactief te analyseren en te beslissen (sneller voorin de keten komen). Daarnaast is er aansluiting nodig op de paradigma verschuiving die nieuwe en sociale media als vorm van communicatie met zich meebrengen; communicatie vindt in steeds mindere mate hiërarchisch of lineair plaats, maar juist diffuus door en met het publiek.

Dit boekje neemt u in vogelvlucht mee langs de resultaten van het onderzoek dat in 2012 door TNO is verricht op het onderwerp: Slimmer omgaan met grote hoeveelheden informatie. Dit onderzoek is onderdeel van het programma Veilige Maatschappij dat TNO in opdracht van het Ministerie van Veiligheid en Justitie uitvoert.

Het boekje is bedoeld voor alle stakeholders op gebied van openbare orde en veiligheid. Door het lezen van dit boekje krijgt u zicht op de kennis die beschikbaar en in opbouw is en op welke wijze dit binnen het domein van openbare orde en veiligheid zijn toepassing kan vinden.

TNO innovation for life