Discussion Paper

Over het automatisch classificeren van cybercrime cases

Léon Willenborg

15 december 2021

Dit document is het resultaat van een analyse van enkele misdrijven zoals gerapporteerd aan de politie en beschikbaar in de vorm van processen-verbaal. Per geval zijn een aangifte (afkomstig van een slachtoffer) en meestal ook een toelichting daarbij (van de hand van een politiefunctionaris) beschikbaar. Het CBS gebruikt dit materiaal als bron voor statistieken over misdrijven in dit land. In de analyse was de aandacht vooral gericht op cybercrime gevallen. De interesse gold met name het soort informatie dat beschikbaar is in aangiftes en toelichtingen. Die kan in hoge mate variëren, omdat het om vrije tekst gaat geleverd door een groot aantal personen, zowel aangevers als politiefunctionarissen (i.c. verbalisanten). De auteur heeft een dertigtal cases die op cybercrime betrekking hebben bekeken en een handjevol niet-cybercrime misdrijven, ter vergelijking. Deze cases kunnen als een aselecte steekproef worden opgevat uit het beschikbaar gestelde bronmateriaal. De auteur heeft gekeken naar deze cases met het oog op automatische classificatie van misdrijven door een systeem dat op trefwoorden afgaat, zoals een semantisch netwerk (of een machine learning applicatie). De conclusie op basis van dit materiaal is dat het automatisch classificeren van wel/geen cybercrime haalbaar lijkt te zijn, maar dat classificren naar type cybercrime een stuk lastiger lijkt te zijn, zeker voor een aantal typen cybercrime. In het stuk wordt ook de aanbeveling gedaan de toelichting te structureren, zodat de benodigde informatie er eenvoudig uit te halen is. Bovendien voorkomt dit dat men met gevoelige persoonsdata moet werken, wat ongewenst is. Indien dat niet mogelijk is zouden de data eerst geanonimiseerd moeten worden. De auteur heeft dat voor de geselecteerde cases ook gedaan voorafgaand aan de analyse. In dit document wordt toegelicht hoe dat gebeurd is.

Trefwoorden: cybercrime, computercriminaliteit, classificatie, geautomatiseerde verwerking, semantische netwerken, machine learning, tekstanalyse, anonymisering.

1 Inleiding

Dit document[1)] gaat over een probleem in het automatisch verwerken van teksten. Het doel is om in omschrijvingen van aangiftes van slachtoffers van misdrijven bij de politie die misdaden met behulp van speciale software te herkennen die als cybercrime te boek staan. Dat is het primaire doel. Daarnaast wordt ook gekeken naar de mogelijkheid om verder te gaan en 'type cybercrime' te herkennen. Sommige teksten zijn opgesteld door politiemensen bij de aangifte door de aangevers, terwijl andere zijn geschreven door de de aangevers van de misdrijven zelf, namelijk in geval de aangifte via de desbetreffende website van de politie is gedaan.

De teksten zijn dus geschreven door verschillende personen. Ze zijn vaak nogal verhalend, informeel en (soms) gelardeerd met irrelevante details ten aanzien van het misdrijf in kwestie. In principe zou er zelfs sprake kunnen zijn van meerdere misdrijven, sommige mogelijk niet-cybercrime misdrijven (bijvoorbeeld diefstal van een laptop of van een smartphone).

De aangiftes worden, indirect, ook gebruikt als basismateriaal voor statistieken over allerlei vormen van criminaliteit, waaronder cybercrime / computercriminaliteit. De aangiftes worden

1) De auteur is de afdeling SQS erkentelijk voor het beschikbaar stellen van de data die in deze studie zijn gebruikt. Hij dankt Arnout van Delden, Rob van Kan en Quinten Meertens voor het reviewen van verschillende concept-versies van dit document. Hun opmerkingen hebben tot diverse verbeteringen geleid.

echter niet in deze vorm gebruikt door het CBS om deze statistieken te maken. Daartoe ontvangt het CBS gestructureerde data van de Politie.

De aangiftes, die in deze studie wel zijn gebruikt, zijn niet direct geschikt voor het maken van statistieken. Het zijn immers teksten waarin de voor statistische doeleinden bruikbare informatie impliciet aanwezig is en die niet zondermeer voor het maken van tabellen en voor statistische analyse geschikt is. Iedere aangifte moet op zijn merites beoordeeld worden, waarbij nagegaan moet worden of er sprake is van cybercrime of niet, en eventueel, wat voor type cybercrime. In prinicipe zouden mensen dat classificatiewerk kunnen doen. Maar het volume aan data is daarvoor te groot, gegeven de beschikbare verwerkingscapaciteit. Het doel is daarom om dit werk zoveel mogelijk te automatiseren. Het voordeel van het gebruik van software voor deze herkenningstaak is bovendien dat precies bekend is hoe beslissingen tot stand zijn gekomen.[2)] Bovendien is de herkenning herhaalbaar en leidt, indien er niets is veranderd in de parameters, tot dezelfde resultaten. En, uiteraard, software kan dag en nacht gebruikt worden, terwijl personen qua werktijd beperkt inzetbaar zijn. Verder is de geautomatiseerde verwerking sneller dan de puur handmatige, dat wil waarbij geen gebruik wordt gemaakt van software voor automatische tekstherkenning. Maar dit alles is natuurlijk niet gratis. Zo'n classificatiesysteem moet worden gemaakt en onderhouden.

Verder bevatten de aangiftes namen, adressen, telefoonnummers en andere gegevens die als directe identificatoren voor personen kunnen worden aangemerkt. Voorafgaand aan de verwerking van de aangiftes is het zaak dit soort informatie te verwijderen, door anonymisering. De bedoeling hiervan is om directe herleidbaarheid tot personen binnen de organisatie tegen te gaan.

Het huidige document is een verkenning van de mogelijkheid om een semantisch netwerk te maken voor cybercrime uit de aangiftes. Daartoe zijn een aantal teksten met beschrijvingen van misdrijven op het gebied van computercriminaliteit geanalyseerd (en enkele buiten dit gebied). Het doel daarbij was om na te gaan wat de trefwoorden zijn die een misdrijf tot een cybercrime bestempelen (of juist niet).

De focus in dit stuk is cybercrime. Vooral is van belang het onderscheid cybercrime en niet-cybercrime. Er wordt echter ook gekeken of het mogelijk is om een cybercrime nader te typeren. Maar dit is geen hoofddoel van deze studie. Wil men dit kunnen doen moet er eerst een classificatie worden gemaakt van typen computercriminaliteit die (zinvol) te onderscheiden zijn.[3)]

Zoals men een semantisch netwerk zou kunnen bouwen voor cybercrime, zo is dat in principe ook mogelijk voor andere typen misdrijven. Ieder misdrijfspecifiek semantisch netwerk kan men zien als een filter. Teksten met beschrijvingen van misdrijven kunnen door meerdere filters gehaald worden. Dit zou ertoe kunnen leiden dat één omschrijving meerdere misdrijven betreft.

De aanpak die hier als uitgangspunt is genomen voor het classificeren op basis van een semantisch netwerk is beschreven in (10). Omdat het maar om één type misdrijf gaat komt het probleem neer op het classificeren van omschrijvingen als wel/niet cybercrime betreffend. Waar mogelijk wordt in de voorbeelden aangegeven dat een meer verfijnde indeling mogelijk zou zijn,

2) Overigens ligt dat bij het gebruik van machine learning (ML) anders. Dit is meer een black box.

3) Onder cybercrime vallen ook activiteiten van buitenlandse geheime diensten. Deze kunnen als doel hebben om informatie te stelen, te wissen, te veranderen of om de werking van systemen te ontregelen. Dergelijke activiteiten vallen echter buiten de scope van de statistieken over criminaliteit die het CBS publiceert.

dus naar type cybercrime. De trefwoorden die in de omschrijvingen voorkomen en gerelateerd zijn worden gekoppeld aan woorden die gebruikt worden om de categorie cybercrime (formeel) te karakteriseren. Waar de trefwoorden uit de teksten variatie in vorm of betekenis kunnen hebben[4)] zijn die aan de beschrijvingskant gestandaardiseerd. In de teksten zijn we daarom geïnteresseerd aan de variëteit aan trefwoorden. In een tweede slag kan men hieruit woorden afleiden die cybercrime op een gestandaardiseerde, enigszins formele, manier beschrijven.

Het stuk is verder als volgt opgebouwd. In Paragraaf 2 wordt het doel van dit stuk uitgelegd, namelijk om tot een semantisch netwerk voor cybercrime te komen, zoals beschreven in (10). Hierbij wordt uitgegaan van het idee dat de te classificeren aangiftes van cybercrime zijn te karakteriseren met bepaalde combinaties van trefwoorden. Het is geen a priori uitgemaakte zaak dat deze aanpak ook goed werkt. Het punt is dat de aangiftes (en bijbehorende toelichtingen, indien aanwezig) heel divers zijn, qua vorm zowel als qua informatie-inhoud. Soms lijkt er voldoende relevante informatie te zijn, in andere gevallen echter niet. En soms staat wordt informatie verstrekt die niet ter zake doet en zelfs misleidend kan zijn (voor een semantisch netwerk of een machine learning applicatie). Ook maakt het uit wat het doel is: misdrijven zoveel mogelijk volautomatisch te herkennen als cybercrime of, meer ambitieus, computercriminaliteit te classificeren naar type cybercrime. Het is niet realistisch te veronderstellen dat de verwerking volledig geautomatiseerd kan verlopen, met een hoog rendement en met weinig fouten. Realistischer is een aanpak waarbij het grootste deel van het materiaal volautomatisch (en correct) wordt geclassificeerd en een deel semi-automatisch (‘handmatig’). Hierop en op andere mogelijke voordelen van een semantisch netwerk voor cybercrime wordt ingegaan in Paragraaf 3. Dit perspectief moet voldoende aantrekkelijk zijn wil men een inspanning leveren om zo’n semantsich netwerk te realiseren. In Paragraaf 4 wordt vervolgens stilgestaan bij de misdrijven die gewoonlijk onder het begrip cybercrime worden geschaard. Er worden enkele voorbeelden besproken van dat type misdrijf. De bedoeling is niet een uitputtende beschrijving te geven van dergelijke misdrijven, maar te focussen op veel voorkomende typen en met name op die typen welke in Paragraaf 7 worden behandeld. Vervolgens wordt in Paragraaf 5 ingegaan op de informatie in processen-verbaal die worden opgemaakt als een misdrijf wordt gemeld bij de politie. Het gaat met name om de aangifte en de toelichting. Het blijkt nuttig te zijn beide onderdelen te onderscheiden. Vervolgens wordt in Paragraaf 6 nader ingegaan op drie tekstelementen die van belang zijn bij de voor deze studie geselecteerde de voorbeelden van cybercrime, die in Paragraaf 7 worden besproken. Het gaat om *trefwoorden*, die cybercrime in het algemeen, of meer specifiek, bepaalde typen cybercrime, karakteriseren. Het gaat verder om *sleutelwoorden* die een onderklasse van de trefwoorden vormen en die expliciet aangeven dat een misdrijf cybercrime betreft, dan wel een bepaald type cybercrime aanduiden. Tot slot zijn er *placeholders*. Dat zijn een soort variabelen, die tekst uit de oorspronkelijke processen-verbaal verhullen omdat die te identificerend worden geacht. Dan volgt de belangrijke Paragraaf 7, waar enkele voorbeelden van cybercrime cases worden opgevoerd en van commentaar voorzien. De bedoeling is om een indruk te geven van het soort informatie dat in processen-verbaal van de politie beschikbaar is. In Paragraaf 8 worden de bevindingen ten aanzien van de geselecteerde cybercrime cases in Paragraaf 7 besproken, in het bijzonder met het oog op vererking door een semantisch netwerk. Ter contrast worden in Paragraaf 9 enkele voorbeelden van niet-cybercrime cases besproken, die alle dicht liggen bij cybercrime. De bedoeling is om te wijzen op overeenkomsten en verschillen met cybercrime cases. De bevindingen ten aanzien van deze niet-cybercrime cases worden in Paragraaf 10 besproken. In Paragraaf 11 wordt ingegaan op de vraag of een semantisch netwerk voor cybercrime mogelijk is en welke obstakels men daarbij

[4)] Vervoegingen van werkwoorden, zelfstandige naamwoorden in meervoud of enkelvoud, gebruik van synoniemen, etc.

mogelijk ontmoet. Dit alles is vooral geïnspireerd door de bevindingen in Paragraaf 8 en, in mindere mate, door die in Paragraaf 10. In Paragraaf 12, worden de belangrijkste bevindingen van het onderzoek verzameld, worden conclusies getrokken en worden enkele suggesties gedaan voor mogelijke vervolgactiviteiten. De hoofdtekst wordt afgesloten met een korte referentielijst. Deze bevat uitsluitend die referenties, die de auteur heeft geraadpleegd. Het was niet de bedoeling om hier ingangen te geven naar de algemene literatuur over cybercrime, semantische netwerken, machine learning, etc. Dit document wordt gecompleteerd met vijf bijlagen. Deze zijn deels bedoeld als verantwoording en verslaglegging van het uitgevoerde werk en deels als verklaring van kernbegrippen in dit stuk. Bijlage A gaat in op de bewerking van de teksten van de processen-verbaal. Er wordt besproken hoe de teksten zijn voorbewerkt, en hier en daar enigszins aangepast. In een tussenversie van dit document zijn trefwoorden en sleutelwoorden in de cybercrime cases aangegeven. In latere concepten zijn de teksten van de aangiften en toelichtingen verwijderd. De gebruikt trefwoorden en sleutelwoorden zijn echter behouden. Deze zijn verzameld in Bijlage B. Wat verloren is gegaan zijn de trefwoorden per case, en zelfs per type cybercrime. Het is maar de vraag in hoeverre dat echt een verlies is, omdat automatisch classificeren van cases op basis van trefwoorden voor alle typen cybercrime met de politiedata zoals ze nu zijn, onbereikbaar lijkt. Een apart probleem vormde de privacygevoeligheid van het ruwe datamateriaal. De auteur heeft de teksten eerst geanonimiseerd alvorens ze te analyseren. Hoe de teksten geanonimiseerd zijn wordt in Bijlage C uit de doeken gedaan. Bij het anonimiseren zijn zogenaamde placeholders gebruikt, die gevoelige stukjes tekst vervangen en waarbij de naam informatie geeft over de aard van de oorspronkelijke tekstfragmentjes. Deze zijn verzameld in Bijlage D. In Bijlage E, tenslotte, worden kernbegrippen voor dit stuk verklaard.

Tot slot van deze inleiding nog dit:

Opmerking '□' markeert het einde van een **Opmerking**. □

2 Doel van dit document

Het hoofddoel van dit stuk is om na te gaan of een semantisch netwerk voor cyberdata mogelijk is. Of het mogelijk is hangt met name af van de kwaliteit van de data. Om daar een beeld van te krijgen is een random steekproef van anngiftes van cybercrime misdrijven bekeken, en een handjevol niet-cybercrime zaken. Deze laatste betreffen cases die 'bijna cybercrime' zaken betreffen. Het idee daarbij is dat een semantisch netwerk deze misdrijven gemakkelijk zou kunnen misclassificeren.

In eerste instantie gaat het erom dat uit alle aangiftes die gefilterd worden die betrekking hebben op cybercrime. In tweede instantie is het van belang om na te gaan of de cybercrime gevallen die herkend zijn ook nader kunnen worden geclassificeerd, naar type cybercrime. In zekere zin beschrijft dit een ideaalsituatie, waarbij ale aangiftes automatisch zouden kunnen worden geclassificeerd. De praktijk is meestal weerbarstiger. Men mag hopen dat een groot deel van de gevallen zo kan worden afgehandeld. In de regel is er nog een aantal gevallen die 'handmatig', door experts moeten worden geclassificeerd. Dan is het wel zaak dat deze 'lastige gevallen' goed herkend worden.

Een semantisch netwerk voor cybercrime zal gebruik maken van trefwoorden die karakteristiek zijn voor cybercrime, of voor een bepaald type cybercrime. De uitdaging is deze woorden te

vinden in de teksten die bij een aangifte behoren. Dat is enerzijds de aangifte zelf, dat een relaas is over een misdrijf door een slachtoffer, door deze persoon zelf verwoord (bij aangifte via internet) of door een verbalisant die het verhaal van een slachtoffer opschrijft. Het betreft vrije teksten, waar verder geen formele structuur in zit of die volgens een bepaald vorschrift zijn opgesteld. En deze teksten is van en groot aantal personen opgesteld. Sommigen zijn geen experts op het gebied van misdrijven (de slachtoffers) en anderen wel (de verbalisanten). Men kan daarom op voorhand verwachten dat er een grote variatie is van beschrijvingen, vanwege de verschillende misdrijven die voorkomen en de verschillende manieren waarop mensen die beschrijven. Een slachtoffer kan zeer geëmotioneerd zijn of aangeslagen en zaken beschrijven die in die toestand begrijpelijk zijn, maar die niet feitelijk zijn, met het giswerk doorspekt over wat er precies gebeurd is, hoe dat gekomen is, wat de gevolgen zijn, en wat verder nog kan gebeuren. Van een politiefunctionaris als een verbalisant mag men professionaliteit verwachten, geen (of in ieder geval minder) emoties dan bij de slachtoffers en meer zakelijk over de berichtgeving van het gebeurde. Niettemin kan deze het giswerk ook opschrijven omdat dit mogelijk en clou bevat voor de opsporing van een misdrijf of andere misdrijven. Of de verbalisant beschrijft in de toelichting zaken die een gevolg zijn van de aangifte: acties die zijn ondernomen, bewijsmateriaal dat een slachtoffer heeft overhandigd of wil overhandigen, relaties met andere soortgelijke misdrijven vastleggen, etc. Allemaal van belang voor de politie (waar de data natuurlijk primair voor bedoeld zijn) maar niet voor het classificeren van misdrijven, waar we in dit document naar kijken.

Het is dus mogelijk dat de omschrijvingen in sommige gevallen niet geschikt zijn voor een semantisch netwerk om (goed) geclasificeerd te worden. Dat kan omdat een relaas te specifiek is (bijvoorbeeld een bepaald fraudegeval) of omdat er te veel irrelevante informatie wordt geleverd. In zo'n geval zou het goed zijn als zo'n case wordt herkend en apart gezet voor 'handmatige' afhandeling. Het kan ook zijn dat bepaalde trefwoorden wel voorkomen in een omschrijving, maar dat het gebruik ervan misleidend is omdat ze geen betrekking hebben op de aangifte waar het om gaat. Als een persoon zo'n tekst zou lezen zou deze dat begrijpen. Echter een semantisch netwerk dat alleeen op trefwoorden af gaat kan tot en verkeerde indeling besluiten. Zo'n geval zou dan 'geluidloos' verkeerd worden geclassificeerd. Het is ook moeilijk (onmogelijk) om dat te vermijden. Het vereist tekstbegrip, die een semantisch netwerk niet heeft. Dan zou een meer sophisticated taalverwerkingssysteem nodig zijn.

Bij een semantisch netwerk is een eerste en belangrijke stap karakteristieke trefwoorden te vinden, in dit geval voor cybercrime. Dat is niet altijd eenvoudig en vereist experimenteren met data. Daar is in dit stuk geen gebruik van gemaakt; dat is iets voor een vervolgstap. Er zijn trefwoorden aangegeven op basis van algemene kennis van de schrijver dezes, die geen expert is op het gebied van misdaadstatistieken. Het is een eerste stap, die bedoeld is om een richting aan te geven waar een oplossing gezocht moet worden (volgens de auteur).

Bij het maken van een semantisch netwerk hoort ook het generaliseren en abstraheren van specifieke trefwoorden. Het betreft een puur taalkundige exercitie waarbij schrijfwijzen geüniformeerd worden (zelfstandige naamwoorden in enkelvoud, werkwoorden in onbepaalde wijs, etc.) en synoniemen geïntroduceerd. Dit is enerzijds gericht op het verkrijgen van zogenaamde C-woorden en anderzijds om de herkenning van trefwoorden te verruimen in het geval nieuwe cases worden verwerkt. Deze stap is in dit stuk verder niet bekeken. Het gaat hier om de opsporing van specifieke gevallen van D-woorden. Voor de gebruikte terminologie zie (10).

Opmerking In dit stuk ligt de nadruk op automatische classificatie met behulp van een semantisch netwerk (SM). Dit zou echter ook door machine learning (ML) gedaan kunnen

worden. Beide benaderingen maken namelijk gebruik van trefwoorden voorkomend in de omschrijvingen (aangiftes en toelichtingen). Echter zij zijn verschillend van aard. SM is knowledge-based is en ML is data-driven. Beide benaderingen kennen hun eigen mogelijkheden en beperkingen. Een ML-systeem kost minder inspanning om toe te passen, maar kan als nadeel hebben dat het als een blackbox werkt.[5)] Men begrijpt niet precies hoe een classificatie tot stand komt, dat wil zeggen, welke informatie daarbij precies gebruikt is. [6)] Een SM kost meer tijd om te bouwen, maar heeft als voordeel dat men goed kan sturen met de informatie die gebruikt wordt om cases te classificeren. De te gebruiken trefwoorden kan men immers zelf kiezen. Dat heeft nog als bijkomend voordeel dat men kan begrijpen en uitleggen hoe de classificatie van een case tot stand is gekomen. Het zou mooi zijn als men de voordelen van beide benaderingen zou kunnen combineren. Zie Paragraaf 11.5 voor een suggestie. □

3 Nut van een semantisch netwerk voor cybercrime

Voordat we op de details in gaan van deze verkenning is het goed om vooraf duidelijk te maken wat het nut van een semantisch netwerk voor cybercrime kan zijn. Zo'n netwerk bouwen en onderhouden kost de nodige inspanning. Het moet dan wel duidelijk zijn dat de kosten tegen de baten opwegen. En men dient te overwegen welke alternatieven er zijn en wat de kosten en baten daarvan zijn.

Met een semantisch netwerk is de bedoeling om de cybercrime data afkomstig van de politie softwarematig te kunnen verwerken, en hopelijk voor een groot deel volautomatisch. Software moet dan de meerderheid van de cases volautomatisch correct verwerken. Dat laatste betekent dat (in het ideale geval) cases die cybercrime betreffen ook als zodanig worden geclassificeerd. En ook cases die daar geen berekking op hebben als niet-cybercrime worden getypeerd.

Om allerlei redenen kan men niet verwachten dat een programma dat gebruik maakt van een semantisch netwerk alle cases volautomatisch kan verwerken. Dat heeft enerzijds te maken met het feit dat met trefwoorden wordt gewerkt en niet met een diepgaande taalanalyse van de teksten. Anderzijds heeft het te maken met de input zelf, dus de processen-verbaal waar de informatie vandaan komt. Die informatie is in de vorm van vrije tekst en afkomstig van veel personen, zowel slachtoffers als politiefunctionarissen. Deze omschrijven in eigen woorden wat er is gebeurd. Soms is deze informatie helder en to the point. Andere keren is het wijdlopig, is duidelijk dat het slachtoffer weinig kennis heeft van computers en de gevaren waaraan hij of zij is blootgesteld op internet. Soms wordt er gespeculeerd over wat er gebeurd kan zijn. Soms worden andere zaken genoemd. Ook de aard van het misdrijf kan een rol spelen bij de begrijpelijkheid van een case door een semantisch netwerk. Sommige cybercrime misdrijven verlopen steevast volgens eenzelfde scenario, terwijl andere heel specifiek, en misschien zelfs wel uniek, zijn in hun verloop.

5) Dat is overigens niet per se het geval. Bij gebruik van een decision tree is de interpreteerbaarheid van de resultaten meestal geen probleem.
6) En men weet dus ook niet of het terecht is dat die informatie is gebruikt.

Als een systeem gebaseerd op een semantisch netwerk het merendeel van het materiaal goed verwerkt (dat zijn de wat simpelere gevallen) dan kunnen experts op cybergebied zich richten op de moeilijkere gevallen die vaak aandachtig gelezen moeten worden om precies te begrijpen wat er gebeurd is. Zij dienen bij hun 'handmatige' classificatie wel ondersteund te worden door tools die hen benodigde informatie aanreiken zodat ze snel de aangeboden cases kunnen classificeren.

Een groot voordeel van het gebruik van een semantisch netwerk is dat formeel is vastgelegd welke kennis over cybercrime men precies gebruikt om cases te classificeren. En als het semantisch netwerk niet is veranderd, is het resultaat ook reproduceerbaar. Dat kan men meestal niet zeggen bij 'handmatig' geclassificeerde misdrijven. Meestal blijft achterwege vast te leggen waarom een expert bepaalde beslissingen heeft genomen; dat zou namelijk de voortgang van zijn werk te veel hinderen. Maar deze werkwijze impliceert wel dat de resultaten niet gegarandeerd herhaalbaar zijn als de cases opnieuw door henzelf of door een collega zouden worden geclassificeerd.

Een ander voordeel van het formeel vastleggen van de kennis over cybercrime in een semantisch netwerk is dat gestuurd kan worden welke gegevens men wenst te gebruiken in de aangiftes. Dit is anders dan bij machine learning (ML), waar aan de software wordt overgelaten welke informatie in de data wel/niet wordt meegenomen. De software bepaalt dit louter op basis van de training set, en legt zelf een link tussen de achtergrondkenmerken en de classificaties van de cases door experts bepaald.

Een voor de hand liggend voordeel van een volautomatisch classificatiesysteem is dat dat 24/7 beschikbaar is, en niet beperkt is tot werktijden die voor medewerkers gelden. Het interactieve deel is natuurlijk minder flexibel en hangt wel af van de werktijden en beschikbaarheid van experts.

Deze experts zijn trouwens ook nodig om het semantisch netwerk te onderhouden. Dat betekent vooral het opvoeren van nieuwe cybercrime misdrijven, het opsporen van nieuwe trefwoorden en sleutelwoorden.[7)] Omdat de trefwoorden worden vastgelegd in het semantisch netwerk, kunnen andere experts daar ook kennis van nemen en eventueel ingrijpen.

Omdat te verwachten is dat een semantisch netwerk in de loop van de tijd zal veranderen (door gebruik van nieuwe kennis) is het van belang (vanwege de reproduceerbaarheid) om te zorgen dat oude 'toestanden' behouden blijven. Men kan dit doen door timestamps mee te nemen, maar dat levert waarschijnlijk een heel complex systeem op. Handiger is regelmatig (voor iedere aanpassing) een snapshot van het semantische netwerk vast te leggen. Dit is in feite gewoon een kopie van de data die op dat moment in het semantische netwerk worden gebruikt.

7) Dit staat nog los van de beveiliging van de data door middel van anonimisering met behulp van placeholders. Het is de vraag of dat niet beter door andere experts kan gebeuren, namelijk die die belast zijn met data security. Nog beter zou zijn als de politie veilige data aan het CBS zou aanleveren.

4 Wat is cybercrime?

We geven hier een korte beschrijving van computercriminaliteit, om het onderwerp enigszins af te bakenen.[8] Wanneer men op Wikipedia[9] kijkt blijkt dit onderwerp in diverse talen tot een wat andere indeling te leiden.[10] Verschillen kunnen ook veroorzaakt worden doordat niet alle vormen van cybercrime overal voorkomen, dus dat er geografische verschillen zijn.

Essentieel voor cybercrime is echter dat computers en netwerken worden gebruikt waar informatie op staat die aan iemand of een bedrijf of instelling toebehoort en die anderen onrechtmatig inzien, kopiëren, veranderen, wissen, verspreiden of gebruiken. Ook kan er sprake zijn van het verstoren van de normale werking van een server (zoals bij DDoS-aanvallen) of van een computer of computernetwerk, tenzij een bedrag wordt betaald aan criminelen (ransomware). Ook kan het internet worden misbruikt om compromitterende informatie te verspreiden (cyberpesten), of daarmee dreigen, tenzij een bedrag wordt betaald, hetgeen dan een vorm van afpersing betreft.[11]

Het volgende overzicht geeft een aardig beeld van (een deel van) cybercrime.[12]

- **Bedreiging**: Het valselijk beschuldigen of bedreigen via een sociaal netwerk of e-mail.
- **Chantage**: Door te dreigen met het publiek maken van compromitterende informatie (bijvoorbeeld naaktfoto's) op internet (ihb op social media).
- **Computervredebreuk**: ongeoorloofd toegang verschaffen tot een computersysteem.
- **DDoS-aanval**: DDoS = Distributed Denial of Service. Ook wel als Website aanval aangeduid. Door een spervuur van e-mailtjes een computersysteem uitschakelen of onbruikbaar maken. Hiervoor wordt vaak een botnet gebruikt. Hier kan ook mee worden gedreigd en is dan een vorm van afpersing.
- **Digitaal haatzaaien**: Het valselijk beschuldigen of bedreigen via een sociaal netwerk of e-mail.
- **Fraude met behulp van computers**: Valsheid in geschrifte met betrekking tot computerdata.
- **Fraude met online advertenties**: Een fraudeur plaatst een advertentie voor de verkoop van goederen en laat zich wel betalen zonder te leveren. Andersom is ook mogelijk: de fraudeur reageert op een advertentie en laat goederen leveren zonder die te betalen.
- **Hacking**: Ongeoorloofd computerdata verwijderen of aanpassen.
- **Helpdeskfraude**: Ook wel Technical support scam of Microsoft support scam genoemd. Zich voordoen als een medewerker van de helpdesk van een softwarebedrijf (vaak Microsoft) en zo toegang krijgen tot een computer van een slachtoffer en zijn/haar bankgegevens.

8) Naast cybercrime wordt ook gedigitaliseerde criminaliteit onderscheiden. Dit betreft eigenlijk gewone criminaliteit waarbij gebruik wordt gemaakt van ICT. By cybercrime wordt ICT als middel en als doel gebruikt. In de praktijk wordt het onderscheid echter niet altijd strikt gemaakt. Zo beschouwt het CBS 'fraude met computers' als cybercrime' terwijl men dat eigenlijk tot de gedigitaliseerde criminaliteit zou moeten rekenen. Door echter de misdrijven op te sommen die men tot cybercrime rekent is het onderwerp goed af te bakenen.

9) Dit is een laagdrempelige site, maar niet een met gezag. Zie daarvoor bijvoorbeeld `https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime` of `https://ec.europa.eu/home-affairs/what-we-do/cybercrime_en`.

10) Vergelijk bijvoorbeeld de volgende artikelen: `https://nl.wikipedia.org/wiki/Computercriminaliteit`, `https://en.wikipedia.org/wiki/Cybercrime`.

11) Een onderwerp als sextortion dat in de Engelse versie van Wikipedia als voorbeeld van cybercrime wordt genoemd, lijkt slechts deels een cybercrime te betreffen. Het is vooral een zedendelict waarbij ook nog sprake is van wederrechtelijke vrijheidsberoving. Dit zijn ernstiger misdrijven dan het verspreiden van compromitterende informatie.

12) Hier worden de begrippen kort verklaard. Van sommige typen cybercrime wordt in Bijlage E een uitgebreidere beschrijving gegeven. Het gaat dan om de typen cybercrime die in Paragraaf 7 aan bod komen.

- **Identiteitsfraude**: Via list en bedrog, of gestolen, identiteitsgegevens van een persoon gebruiken voor oplichting van andere slachtoffers, om zo buiten beeld te blijven.
- **Man-in the-middle aanval**: Berichten onderscheppen en veranderen.
- **Phishing**: Methode waarbij via misleiding persoonlijke gegevens worden ontfutseld bij, of stiekem gekopieerd van iemand, bijvoorbeeld inloggegevens voor een bankaccount, met de bedoeling hier geld van te stelen.
- **Ransomware**: Gebruik van malware waarmee bestanden versleuteld worden en tegen betaling weer ontsleuteld; de malware wordt verstuurd via e-mail.
- **Spoofing**: Het vervalsen van persoonskenmerken met als doel om tijdelijk een valse identiteit aan te nemen. Dit kan bijvoorbeeld gaan om e-mail, website, IP-adres, telefoonnummer en biometrische kenmerken.
- **WhatsApp-fraude**: Ook wel aangeduid als 'vriend-in-nood fraude'. Bij vriend-in-nood fraude krijgt iemand via WhatsApp zogenaamd een dringend verzoek van een vriend(in), familielid of bekende om snel geld over te maken. In werkelijkheid komt het appje van een oplichter die zich voordoet als een bekende die op slinkse wijze geld wil aftroggelen van de geadresseerde. Deze vorm van fraude komt op WhatsApp verreweg het meeste voor maar kan ook plaatsvinden via e-mail, SMS, Snapchat of Telegram.

In de voorbeelden in Paragraaf 7 komen niet alle typen cybercrime aan de orde. Het gaat daar alleen om

- DDoS-aanval.
- Ransomware.
- Helpdeskfraude.
- Phishing.
- Hacking.
- Fraude met computers.
- Fraude met online advertenties.

Dat is overigens geen bewuste keuze geweest. Deze onderwerpen zijn door het lot bepaald. De auteur dezes heeft een willekeurige selectie van cases gemaakt uit de politiebestanden die hem ter beschikking waren gesteld. Deze bleken betrekking te hebben op de genoemde typen cybercrime.

Daarnaast zijn er nog misdrijven waarbij wel computers en software een rol spelen, maar die niet als cybercrime worden gezien. Bijvoorbeeld het stelen of vernielen van een laptop. In Paragraaf 9 worden enkele van dergelijke niet-cybercrime gevallen getoond en besproken, ter contrast met de cybercrime cases.

5 Aangiftes en toelichtingen

Een slachtoffer van een misdrijf kan daarover aangifte doen bij de politie. Dat kan via een website van de politie of door naar een politiebureau te gaan. In het laatste geval vertelt het slachtoffer zijn verhaal aan een politiefunctionaris, een verbalisant genaamd, die het optekent in

een proces-verbaal. Dat is de aangifte. De informatie die in een proces-verbaal[13)] staat staat is wisselend van kwaliteit. Soms. is het slachtoffer iemand met kennis van zaken voor wat betreft cybercrime, of computers. Andere keren is het een volslagen leek. De informatie die verstrekt wordt kan kort en zakelijk zijn of lang, gekleurd door emoties en met de nodige speculaties wat er gebeurd kan zijn. De mate van bruikbaarheid van de aangifte als middel om er een misdrijf mee te classificeren is daarom ook sterk wisselend.

De verbalisant kan besluiten aanvullende opmerkingen te maken over de case in een toelichting. Een toelichting hoeft niet altijd aanwezig te zijn bij een aangifte. De verbalisant lijkt tamelijk vrij te zijn in de keuze van het soort informatie dat hij/zij opneemt in een toelichting, afgaande op de voorbeelden in deze studie. Soms is het een samenvatting van het misdrijf met een labelling van het soort misdrijf. Dit is in de regel de beste informatie om een misdrijf mee te classificeren. Soms echter bevat het procesmatige of procedurele opmerkingen over acties die door de politie en anderen (bijvoorbeeld een officier van justitie) zijn ondernomen, of een vermelding van door het slachtoffer geleverd bewijsmateriaal. Deze informatie is van geen nut bij het classificeren van cases. Als deze informatie aanvullend is, is er meer tekst dat het semantisch netwerk moet verwerken. In het beste geval levert het niets op. In het slechtste geval leidt het af van waar het echt om gaat. Als alleen dit soort proces- en procedurele informatie aanwezig is (wat ook voorkomt) dan is de toelichting in die case niet nuttig voor het classificeren ervan als cybercrime of als type cybercrime.

Of een case een geschikte bron is voor trefwoorden en sleutelwoorden hangt niet alleen af van het kennisniveau met betrekking tot computers en cybercrime van de aangever, maar ook van het type cybercrime. Sommige zijn tamelijk generiek (zoals phishing, ransomeware en helpdeskfraude), in de zin dat het patroon volgens welke ze verlopen standaard is, terwijl andere heel specifiek zijn. Dat laatste is bijvoorbeeld het geval bij computerfraude. Voor het vinden van nieuwe trefwoorden zijn vooral de generieke misdrijven van belang. Daarvoor zijn niet heel veel cases nodig zijn om een geschikte set trefwoorden te vinden. De specifieke cases daarentegen zijn vaak minder interessant als (rijke) bron van trefwoorden, omdat ze niet zo snel een tweede keer voorkomen.

Maar dit zijn slechts impressies van de auteur op grond van de gevallen die in deze studie aan bod kwamen. Uiteindelijk zullen experts dit moeten beoordelen. We gaan ervan uit dat extractie van nieuwe trefwoorden en sleutelwoorden voor een semantisch netwerk door experts zal gebeuren, daarbij ondersteund door speciale software. Het zijn waarschijnlijk vaak de niet-generieke gevallen die de experts te zien krijgen, omdat die niet door het semantisch netwerk automatisch geclassificeerd kunnen worden. Dat wordt dan speuren naar nieuwe trefwoorden. De generieke gevallen die naar verwachting vaak wel automatisch geclassificeerd zullen worden, moeten dan steekproefsgewijs door expert worden bekeken, om na te gaan of er toch niet interessante woorden in voorkomen die als trefwoorden kunnen worden gebruikt.[14)] Zo'n inspectie op steekproefbasis is ook goed om een indruk te krijgen van de kwaliteit van de automatische classificatie.

Het is jammer dat de processen-verbaal die het materiaal opleveren voor de cybercrime (en andere misdrijven), en dan speciaal het toelichtingendeel, niet gestructureerd zijn door gebruik

[13)] In dit stuk wordt daarvoor ook wel 'aangifte' gebruikt. Dit moet niet verward worden met het onderdeel van een proces-verbaal met dezelfde naam.

[14)] In Paragraaf 11.2 wordt uitgebreider bij dit aspect stilgestaan.

van duidelijke rubrieken—zoals de aard van het misdrijf—die meteen de sleutel zouden zijn—letterlijk, zelfs—tot het automatisch classificeren van misdrijven. Als het type cybercrime ook nog eens is voorgecodeerd zou de classificatie van de cybercrime cases een fluitje van een cent zijn. Men zou het aangiftedeel dan niet eens meer nodig hebben, tenzij voor controle. Als ook de naam van de aangever in een apart veld zou worden genoemd, en in de toelichting alleen als 'de aangever' (oid) worden aangeduid, is ook de privacy-gevoeligheid van de data geen probleem meer. Het is uiteraard niet aan het CBS om hierover te beslissen. Maar het is ook niet vreemd om deze suggestie aan de politie te doen. Wellicht ontmoet men daar een luisterend oor en de welwillendheid om een dergelijke verandering op termijn te realiseren. Het is ook in het belang van de politie dat het dan eenvoudiger wordt statistieken te maken over misdrijven in Nederland, in het bijzonder op het gebied van de cybercrime.

6 Trefwoorden, sleutelwoorden en placeholders

De D-words in (10) zullen we in dit stuk aanduiden als trefwoorden. De trefwoorden zijn kenmerken van misdrijven, maar ze bepalen die niet uniek. De meeste trefwoorden zijn van toepassing op meerdere misdrijven. Er zijn echter ook trefwoorden die één type cybercrime karakteriseren. Deze trefwoorden noemen we sleutelwoorden. 'Phishing', 'ransomware' zijn enkele voorbeelde als het gaat om typen cybercrime. Maar woorden als' cybercrime' zijn dat ook, omdat ze zo'n misdrijf onderscheiden van andere niet-cybercrime misdrijven. Dat onderscheid is belangrijk in deze studie. En uiteraard, aanduidingen van typen cybercrime (zoals 'phishing') impliceren 'cybercrime'. Ook een sleutelwoord hoeft niet per se uit één woord te bestaan, maar kan zijn samengesteld uit meerdere woorden, zoals 'fraude met computers'.

Wat het vinden van trefwoorden betreft zijn er drie doelen, namelijk trefwoorden vinden die:

1. **aangeven dat cybercrime aan de orde is**. Dit soort trefwoorden zouden we 'sleutelwoorden voor cybercrime' kunnen noemen. In veel gevallen wordt in de toelichting bij de aangifte de aard van het misdrijf genoemd, soms zelfs met een specifieke aanduiding van het type cybercrime. In het geval zo'n aanduiding aanwezig is het misdrijf (in principe) getypeerd. Er staat 'in principe' omdat niet gegarandeerd is dat deze aanduiding ook correct is.
2. **aangeven welk type cybercrime van toepassing is**. Dit soort trefwoorden zou men 'sleutelwoorden voor bepaalde typen cybercrime' kunnen noemen. Andere, minder specifieke aanduidingen van het misdrijf worden daarmee (in principe) overbodig. Ook hier staat 'in principe' omdat zo'n niet per se correct of het meest gedetailleerd mogelijke hoeft te zijn. Er zou 'computerfraude' kunnen staan. Dat impliceert 'cybercrime'. Er zou ook 'fraude' kunnen staan, terwijl uit de aangifte duidelijk is dat het om computerfraude gaat. In het laatste geval is de aanduiding 'fraude' weliswaar correct, maar niet precies genoeg.
3. **op zichzelf niet specifiek zijn voor een bepaald type cybercrime, maar dat wel gezamenlijk kunnen zijn**. Dit soort trefwoorden zijn als het ware kenmerken van het misdrijf in kwestie. Ze zouden kunnen dienen om af te leiden om wat voor type misdrijf het gaat. Dat is nuttig in geval sleutelwoorden ontbreken. Maar ook om te verifiëren of zo'n afleiding hetzelfde misdrijf oplevert als een sleutelwoord suggereert.

In Bijlage A, in het bijzonder onderdeel A.8, wordt nader ingegaan op de werkwijze die in deze studie is gevolgd om tot een overzicht van trefwoorden, sleutelwoorden (en ook placeholders) te komen.

7 Commentaar bij de geselecteerde cybercrime cases

In de navolgende deelparagrafen worden enkele cybercrime cases geanalyseerd. Iedere paragraaf gaat over één case. Bij de bespreking van een case wordt gekeken naar de mogelijkheid om deze als cybercrime te herkennen en naar de mogelijkheid om het type cybercrime vast te stellen. Het eerstgenoemde doel is het belangrijkste. Het tweede doel blijkt ook veel lastiger te zijn. Daar zijn allerlei oorzaken voor aan te geven. Dit komt verderop in de tekst ter sprake.

De volgorde van de cybercrime typen die hier worden bekeken is ruwweg van uniform (weinig variatie in de aanpak) tot pluriform (grote variatie bij de misdrijven in deze categorie). Een voorbeeld van het eerste type zijn DDoS-aanvallen, terwijl fraude cases heel uitlopend zijn. Dit lijkt tevens een ordening van makkelijk naar moeilijk om de desbetreffende misdrijven softwarematig te herkennen, respectievelijk te classificeren.

7.1 DDoS aanval

7.1.1 Voorbeeld DD-1

Zowel in de toelichting als de aangifte wordt de aard van het misdrijf genoemd: DdoS aanval. In de toelichting verklaart de aangever wat dat is en hij blijkt ter zake deskundig te zijn. DDoS-aanvallen zijn allemaal van dezelfde vorm, zoals de aangever van dit misdrijf ook goed beschrijft. Aan de DDoS aanval was kennelijk geen chantage gekoppeld, in die zin dat deze pas zou stoppen na betaling door de instelling. De aangever rept er althans niet over.

7.2 Ransomware

7.2.1 Voorbeeld RA-1

Dat het hier om cybercrime gaat staat expliciet in de toelichting. De aangever meldt feitelijk een geval van ransomware. Deze aanduiding wordt echter niet gebruikt, noch in de toelichting, noch in de aangifte. Mogelijk zijn de (door de auteur) aangemerkte trefwoorden voldoende om dit geval als ransomeware te typeren. Maar helemaal zeker is dit niet, omdat het er niet zoveel zijn. Opvallend is dat de melder de oorzaak van dit probleem niet weet. Veel slachtoffers van ransomware zijn zich wel bewust van het moment waarop het mis ging: toen ze een bijlage van een bepaald mailtje openden. Maar in dit geval heeft het slachtoffer geen idee hoe het probleem ontstaan kan zijn. Het slachtoffer heeft niet betaald. De schade is beperkt gebleven.

7.2.2 Voorbeeld RA-2

De aard van het misdrijf wordt genoemd in de aangifte, maar niet in de toelichting, zij het verkeerd gespeld: ‘ransomeware’ in plaats van ‘ransomware’. (Misleid door woorden als ‘somewhere’, ‘something’ en ‘somebody’?) In het voorbeeld komt verder het woord ‘crypt’ voor. Staat dat voor ‘cryptoware’? Mogelijk is dit een vaker gebruikte contractie en dient het te worden opgenomen in de trefwoordenlijst. Wellicht is het een synoniem van ‘cryptoware’.

7.2.3 Voorbeeld RA-3

Dit misdrijf is meteen als cybercrime te classificeren omdat dit sleutelwoord voorkomt in de toelichting. Hier is in feite sprake van ransomware maar dit woord komt noch in de toelichting noch in de aangifte voor. Er staan echter voldoende trefwoorden in de tekst om af te leiden dat het in dit geval om dit type cybercrime gaat. In de oorspronkelijke tekst wordt de naam van het encryptieprogramma genoemd. Dat is waarschijnlijk al voldoende om tot de classificatie ‘ransomware’ te komen voor dit misdrijf. Het sleutelwoord ‘cybercrime’ wordt genoemd in zowel de toelichting als de aangifte.

7.2.4 Voorbeeld RA-4

In dit geval is duidelijk dat het om ransomware gaat omdat dit woord in zowel in de toelichting als in de aangifte wordt genoemd.

7.2.5 Voorbeeld RA-5

In dit voorbeeld wordt het misdrijf niet expliciet als cybercrime betiteld en ook het type cybercrime wordt niet genoemd. Het is duidelijk dat het hier om ransomware gaat, wat uit de overige trefwoorden is af te leiden. Dat zou ook meteen duidelijk zijn in de oorspronkelijke data waar de gebruikte malware met name wordt genoemd, welke in de hier gebruikte geanonimiseerde versie vervangen is door een placeholder (<encryptiesoftware>) Er komen trefwoorden in de tekst van de aangifte voor met spelfouten erin, zoals ‘ressetten’, ‘backup’s’.

7.2.6 Voorbeeld RA-6

Ransomware wordt niet expliciet genoemd in toelichting of aangifte. Wel ‘computervredebreuk’ en ‘afpersing’. Deze woorden samen zou men als synoniem voor ransomware kunnen opvatten. In ieder geval volgt uit ‘computervredebreuk’ dat het om cybercrime gaat. In de toelichting staat dit woord ook expliciet. Als men de oorspronkelijke (dus onbeveiligde) data zou gebruiken, zou uit de tekst vermoedelijk meteen duidelijk worden dat het hier om ransomware gaat.

7.2.7 Voorbeeld RA-7

In de toelichting wordt ransomware expliciet genoemd, waarmee het misdrijf door getypeerd is. Melder noemt allerlei wetsartikelen. Zijn die correct of terecht aangehaald? Meer algemeen kan men de vraag stellen: moet men dit soort informatie verstrekt door melders van misdrijven zondermeer geloven? Men kent immers de deskundigheid van degene die ze te berde brengt niet. Als men toch waarde hecht aan die informatie (na verificatie!) levert dat trefwoorden voor het semantische netwerk op. De informatie in de toelichting is van de politie en het ligt voor de hand deze als meer betrouwbaard te beschouwen is dan die in de aangifte. In dit geval is de aangifte tamelijk uitgebreid. Het is ook een rijke bron van trefwoorden.

7.2.8 Voorbeeld RA-8

Ransomware wordt niet expliciet genoemd, maar valt wel af te leiden. Zeker uit de oorspronkelijke tekst in de brondata. Maar ook met behulp van de overige kenmerken. Als die oorspronkelijke tekst niet beschikbaar is bij classificatie van het misdrijf dan is er nog 'redding': in de toelichting komt het sleutelwoord 'cybercrime' voor. Vanwege die omzekerkeid over de beschikbare oorspronkelijke tekst is 'cybercrime' ook als sleutelwoord gemarkeerd. In de toelichting staat het trefwoord 'opslag of verwerking van gegevens'. Dat zijn eigenlijk twee trefwoorden, gecombineerd tot één: 'opslag van gegevens' en 'verwerking van gegevens'. In een semantisch netwerk zouden deze drie combinaties als trefwoorden dienen te worden opgenomen.

7.2.9 Voorbeeld RA-9

Dit voorbeeld betreft ransomware, hoewel dat niet expliciet in de tekst wordt genoemd. In de brontekst wordt niet de naam van de encryptiesoftware genoemd maar wordt wel de tekst die dit programma op het scherm toont vermeld. Daarmee is meteen duidelijk dat het om ransomware gaat. Maar ook in de geanonimiseerde tekst zou de naam van een geschikt gekozen placeholder hierop moeten wijzen. (Dat geeft het belang aan van goed gekozen namen voor placeholders!) Echter ook met behulp van overige kenmerken in de tekst is het mogelijk tot ransomware te besluiten. In de aangifte staat dat het om computervredebreuk gaat (in de aangifte verkeerd gespeld als 'computer vredebreuk'), zodat duidelijk is dat het om cybercrime gaat, ook al is de naam van het encryptieprogramma of de tekst die het op het scherm laat zien, verhuld. Het lijkt alsof de kwalificatie 'computervredebreuk' als naam voor dit misdrijf niet helemaal op zijn plaats is. Niet specifiek genoeg en te zwak. De aangever heeft niet betaald en heeft zijn computer opnieuw laten installeren. Onduidelijk is of de aangever data kwijt is. Zo niet, dan zou deze persoon geen schade hebben geleden, behalve mogelijke kosten voor het opnieuw installeren van de software en ongemak omdat hij een tijd zijn computer niet heeft kunnen gebruiken.

7.3 Helpdeskfraude

Microsoft en cybercrime zijn trefwoorden die beide worden genoemd, in zowel de toelichting als de aangifte. Helpdeskfraude, technical support scam of Microsoft support scam worden niet expliciet genoemd. De link met dit type cybercrime is echter snel gelegd op basis van de trefwoorden. In dit geval is de aangeefster niet financieel de dupe geworden van de scam. Haar dochter heeft op tijd geïntervenieerd. Er is hier sprake van een verijdeld misdrijf. Moet dit geval (en soortgelijke gevallen) als misdrijf meetellen in de statistieken? Of moeten verijdelde en gelukte misdrijven worden onderscheiden in de statistieken? Is een verijdeld misdrijf anders dan een (mislukte) poging tot een misdrijf? Of is het een misdrijf, dat echter in de uitvoering mislukt is?

7.3.1 Voorbeeld HD-2

Dit is een misdrijf van het type helpdeskfraude, hoewel deze naam of één van de andere gebruikte aanduidingen (technical support scam of Microsoft support scam) niet expliciet wordt worden genoemd, noch in toelichting noch in de aangifte. Windows en Microsoft wordt echter wel genoemd. Het misdrijf wordt in de toelichting omschreven als 'fraude met betaalproducten', en in de aangifte als 'oplichting'. Met behulp van de overige trefwoorden zou helpdeskfraude mogelijk automatisch afgeleid kunnen worden. De scam die hier plaats vindt komt vaker voor: de 'Microsoft-medewerker' vraagt voor zijn assistentie geld (een klein bedrag). Dat kan echen niet

worden overgemaakt. Het (potentiële) slachtoffer moet daarom een groter bedrag overmaken. De 'Microsoft-medewerker' belooft het teveel betaalde terug te betalen, maar doet dit niet. Er komen enkele samengestelde trefwoorden voor, bestaande uit woorden die niet direct achter elkaar voorkomen, maar die gescheiden worden door woorden die niet tot het trefwoord behoren.

7.3.2 Voorbeeld HD-3

De omschrijving van dit misdrijf, 'helpdesk fraude', 'Microsoft support scam' of 'technical support scam', wordt niet genoemd. Zelfs 'cybercrime' of 'computercriminaliteit' wordt niet genoemd. 'Microsoft' en 'oplichting' echter wel. Met de trefwoorden in toelichting en aangifte is vermoedelijk wel af te leiden dat het om cybercrime gaat. Mogelijk is zelfs af te leiden dat het om helpdeskfraude gaat. De aangeefster heeft een (correct, zo bleek later) telefoonnummer van Microsoft gekregen van de internetprovider. Ze heeft contact opgenomen met Microsoft via dat telefoonnummer, kreeg een 'computer aan de lijn' en heeft doorgegeven wat het probleem met haar computer was. Later werd zij echter teruggebeld door een, naar achteraf bleek, malafide figuur, die beweerde voor Microsoft te werken. De vraag is hoe deze persoon aan de informatie is gekomen over het probleem van de aangeeftster met haar computer. Was de computer van Microsoft gehackt? Is haar telefoongesprek met die Microsoft computer afgeluisterd? In dit geval is de toelichting een samenvating van de aangifte en niet echt een interpretatie van de verbalisant. Hier heeft de 'Microsoft medewerker' bankinformatie aan het slachtoffer ontfutseld waarmee vervolgens bedragen van haar bankrekening zijn afgeschreven.

7.3.3 Voorbeeld HD-4

Computercriminaliteit wordt genoemd. Helpdeskfraude, Microsoft support scam of technical support scam worden niet expliciet genoemd, maar uit de omschrijving volgt dat het dit hier wel het geval is. Uit de trefwoorden valt dat vermoedelijk ook wel af te leiden. 'Microsoft' wordt in ieder geval expliciet genoemd. De aangeefster maakt ook melding van een poging tot een tweede misdrijf—ransomware betreffend—die haar man heeft getroffen. Ze geeft zelf aan dat ze niet weet of beide zaken gelinkt zijn. In ieder geval moet die ransomware zaak los van het misdrijf waar de aangifte over gaat. Omdat ransomware zaak in de aangifte wordt genoemd is het risico dat een semantisch netwerk dit misdrijf als ransomware zou classificeren, terwijl het om heldeskfraude gaat. Men moet het stuk begrijpend lezen om te weten dat het hier niet om het feitelijke misdrijf in de aangifte gaat. Dat is iets wat een semantisch netwerk niet doet (net als een ML toepassing), omdat die louter met (combinaties van) trefwoorden werkt.

7.3.4 Voorbeeld HD-5

In de toelichting wordt het misdrijf 'Microsoft oplichting' genoemd, wat als een synoniem van 'Microsoft support scam' kan worden opgevat. Het misdrijf is daarom goed te classificeren. In dit geval heeft de oplichter bankinformatie van het slachtoffer ontfutseld en heeft die gebruikt om bedragen van zijn bankrekening af te schrijven. Het is duidelijk dat het slachtoffer weinig van computers weet en goed van vertrouwen. Te goed, zodat men hem heeft opgelicht. Het slachtoffer heeft het erover dat hij meerdere keren is benaderd door een persoon die zich uitgaf als Microsoft medewerker. Omdat hij deze peroon / personen niet verstond heeft hij opgehangen en is hij vermoedelijk een aantal keren aan helpdeskfraude ontkomen. Het slachtoffer beweert dat hij door een Microsoft medewerker uit het buitenland is benaderd. (Weet hij zeker dat dit uit het buitenland was? Misschien door een buitenlander verblijvend in Nederland?) In de toelichting en aangifte staan vrij veel trefwoorden die een bepaald type helpdeskfraude typeren

7.4 Phishing

7.4.1 Voorbeeld Ph-1

De karakterisering van dit misdrijf wordt in de toelichting gegeven: phishing, echter, diverse keren foutief gespeld als 'phising' (in toelichting én aangifte). In de aanhef van de aangifte is sprake van 'fraude cq oplichting middels het aanvragen van een bankpas'. Aan het einde van de aangifte wordt echter 'phising' genoemd. In aangifte en toelichting komen veel trefwoorden voor die met bankzaken van doen hebben. Naast 'phising' is een andere opvallende spelfout in de toelichting (2 maal voorkomend) is 'edentifer' in plaats van 'identifier'. Veel van de trefwoorden hebben betrekking op bankzaken, wat van belang is om de context te schetsen van het misdrijf.

7.4.2 Voorbeeld Ph-2

In dit voorbeeld wordt het misdrijf ('phishing') benoemd, in zowel de toelichting als de aangifte. Via een malafide e-mail die van de bank afkomstig leek heeft het slachtoffer bankgegevens aan de oplichter doorgegeven. Die heeft mogelijk ook de nieuwe bankpas gestolen uit de brievenbus van de aangever/ het slachtoffer. Met die pas en de gestolen bankgegevens heeft de oplichter geld kunnen pinnen van de bankrekening van het slachtoffer. De bank heeft de aangeefster schadeloos gesteld, zodat ze niet financieel benadeeld is. Heeft bank ook aangifte gedaan? Zo ja, leidt dat dan niet tot dubbeltellingen van misdrijven? Sommige samengestelde trefwoorden bestaan uit woorden afkomstig van verschillende, opeenvolgende zinnen. Op deze manier zijn betere combinaties te maken dan door alleen woorden in eenzelfde zin te nemen.

7.4.3 Voorbeeld Ph-3

In dit voorbeeld is alleen sprake van een aangifte; een toelichting ontbreekt. Waarschijnlijk is de zaak aangegeven via de politie-website.De aangever betitelt het misdrijf als 'computervredebreuk'. Daaruit leidt men in ieder geval af dat het om 'cybercrime' gaat 'Phishing' lijkt echter een betere karakterisering. Dit woord wordt niet genoemd in de aangifte. Als men echter afgaat op de gebruikte trefwoorden en trefwoordcombinaties dan komt men vermoedelijk hier ook bij uit. De voorbeeld illustreert het verschil dat kan ontstaan als een aangever het misdrijf dat hem / haar is overkomen omschrijft of wanneer een politiefunctionaris (i.c. een verbalisant) dat doet. In dat laatste geval mag men aannemen dat de aanduiding van het type cybercrime dan betrouwbaarder is. Bij het karakteriseren van een misdrijf is het van belang onderscheid te maken naar de bron van de informatie: de aangifte zelf (informatie van het slachtoffer) of uit de toelichting (informatie van de verbalisant, met input van het slachtoffer). De laatste moet dan als betrouwbaarder gelden. Maar als een toelichting ontbreekt en er alleen een aangifte is, moet men voorzichtiger zijn en niet blind varen op de kwalificaties die de aangever gebruikt. Deze is in de regel geen specialist op forensisch gebied. De aangever spreekt van een 'geautomatiseerd werk'. Wordt hiermee 'netwerk' bedoeld?

7.4.4 Voorbeeld Ph-4

Phishing wordt niet genoemd om dit misdrijf te typeren. Wel oplichting en computervredebreuk. Dit geval is opmerkelijk omdat nu de koper de verkoper tracht op te lichten. Vaker ziet men het omgekeerde, waarbij de verkoper zijn op een website geadverteerde waar niet levert aan de koper nadat die betaald heeft. In dit geval probeert de koper van de verkoper bankinformatie te ontfutselen met behulp van een malafide link die hij aan de verkoper opstuurt. Dat is een voorbeeld van phishing. Hij tracht vertrouwen te wekken bij de verkoper door 'eigen' persoons- en bankgegevens op te sturen en op die manier de verkoper over te halen dat ook te doen. Maar

de gegevens van de koper zijn niet echt en vermoedelijk verkregen van een eerder slachtoffer. Identiteitsfraude speelt in dit voorbeeld daarom mogelijk ook een rol. Omdat de aangever op een bepaald moment argwaan krijgt heeft hij niet gedaan wat de oplichter wilde en heeft hij zo financiële schade voorkomen. De aangever is bang dat zijn persoons- en bankgegevens in de toekomst ook zullen worden misbruikt bij een oplichtingszaak en de oplichter door identiteitsfraude buiten beeld blijft. Hij geeft aan dat als dit gebeurt hij aangifte zal doen van dit misbruik. Het gaat hier dus over een vermoeden, een mogelijk gedrag en een mogelijk toekomstig misdrijf. Dit staat los van het misdrijf waar de aangifte over gaat. Dat kan problematisch zijn bij de classificatie van zo'n misdrijf met behulp van een semantisch netwerk, waarbij beslissingen worden genomen op basis van trefwoorden in aangifte of toelichting. Zonder begrijpend lezen kan men niet onderscheiden welke informatie ter zake doet, wat speculatie is en wat geen betrekking heeft op de desbetreffende case.

7.5 Hacking

7.5.1 Voorbeeld HA-1

In dit voorbeeld wordt de aard van het misdrijf expliciet genoemd, namelijk hacken van het social medium account van aangever. De toelichting en de aangifte lijken redelijk veel op elkaar. Het heeft niet zo veel zin in een toelichting de aangifte uitgebreid weer te geven. Beter kort samenvatten en conclusies trekken. Dat gebeurt kennelijk niet altijd, zoals dit voorbeeld laat zien. Het is een wat onduidelijk verhaal. Wat is de pointe precies van het misdrijf? Wat is de reden van de hack? Heeft de aangever er nadeel of schade van ondervonden? Het is lastig om goede trefwoorden aan te geven in dit voorbeeld.

7.5.2 Voorbeeld HA-2

Het enkelvoudige sleutelwoorden voor cybercrime als'hacking' en 'computervredebreuk' worden genoemd in de aangifte. Maar ook woorden als 'oplichting', 'verduistering' en 'diefstal van geld' die niet niet per se op cybercrime betrekking hebben. Het gaat hier dus om meer dan hacking. Is diefstal van geld niet het belangrijkere delict en hacking slechts het middel daartoe? Of is er hier sprake van meerdere, even zwaar tellende delicten? Er wordt meegedeeld dat de aangever tot twee maal toe slachtoffer is geworden van wegsluizen van geld (naar het buitenland). Gaat het dan om twee delicten in de statistieken? De aangever weet niet veel van computers en zijn relaas is daarom dat van een leek op dit gebied. Hij heeft het vooral over de financiële schade die hij heeft geleden als gevolg van de hacks waar hij slachtoffer van is geworden. Hij heeft geen idee hoe die hebben kunnen plaatsvinden. De verbalisant geeft aan dat mogelijk relevante opsporingsinformatie is verdwenen doordat harde schijven van de computer van de aangever deels zijn overschreven. Dit voorbeeld illustreert dat een aangever niet altijd deskundig hoeft te zijn op computergebied en de informatie die zo iemand verstrekt niet altijd bruikbaar is om een goed beeld te krijgen van het misdrijf. In dit geval omschrijft de aangever wel met een aantal informatieve trefwoorden wat hem is overkomen.

7.5.3 Voorbeeld HA-3

De aard van het misdrijf wordt in dit voorbeeld genoemd: 'hacking', meer specifiek zelfs 'modemhacking'. Dit soort misdrijven wordt ook wel 'telecomfraude' genoemd. Door deze actie is het slachtoffer financieel benadeeld. Dus naast hacking is er ook sprake van oplichting. Hoe het misdrijf technisch heeft plaats gevonden is niet helemaal duidelijk. Er is meerdere keren gebeld vanaf de huistelefoon van het slachtoffer naar een bepaald telefoonnummer, kennelijk

een betaalnummer. Degene die dit nummer exploiteert heeft daar duidelijk baat bij. Naar de huistelefoon is vaker gebeld. Er werd niets gezegd door de beller, maar deze heeft mogelijk tijdens zo'n 'gesprek' kans gezien 'in het modem' te komen en een verbinding te maken met het betaalnummer. De aangever betaalde voor de telefoonkosten. Dit is een vermoeden hoe het gegaan is, niet meer. Het is niet helemaal uit te sluiten dat de zoon van aangever (of een ander lid van het huishouden) heeft gebeld naar het betaalnummer in kwestie. Het grote voordeel voor de oplichter van dit type misdrijf is dat deze helemaal buiten beeld kan blijven.

7.5.4 Voorbeeld HA-4

Het social medium account van aangeefster is gehackt. 'Hacken' wordt expliciet genoemd in toelichting en aangifte. De aangeefster suggereert dat iemand op haar telefoon zou hebben 'ingebroken' terwijl zij aan het zwemmen was en haar telefoon in haar vakantiehuisje was achtergebleven. Dat lijkt niet zo waarschijnlijk. Temeer omdat ze aangeeft dat niemand haar wachtwoord kent (bedoeld is waarschijnlijk dat zij dat wachtwoord bewust met een ander heeft gedeeld). Misschien is de verbinding in het vakantiepark niet goed beveiligd. Misschien is haar social media account op een andere manier gehackt, mogelijk zelfs voordat zij in het vakantiepark verbleef. Dat allerlei vrienden van haar ook berichten krijgen is op zich niet vreemd. Er wordt ook een ander misdrijf genoemd, namelijk dat het social medium account van de zoon van de aangeefster is gehackt (waarvan hij geen aangifte heeft gedaan). Een wijdlopig en een voor deze case maar beperkt relevant relaas. Gelukkig staat het sleutelwoord 'hacken' in toelichting en aangifte, zodat het misdrijf te classificren is. In de aangifte wordt ook nog 'identiteitsfraude' genoemd. Er zijn 'namens haar' berichten gestuurd aan 'vrienden' op haar social medium account. Dat lijkt niet een gangbare interpretatie van het begrip. Haar account is gehackt en de hacker heeft via haar account vrienden van haar een advertentietekst gestuurd, waarschijnlijk om ze hiermee op te lichten. Dit is een voorbeeld dat moet worden gemeden als bron van trefwoorden, wat de auteur dezes ook heeft gedaan. Problematischer is het om zo'n case te moeten classificeren als er geen sleutelwoorden in staan, wat hier echter niet het geval is. Echter is één van de sleutelwoorden die genoemd worden ('identiteitsfraude') ook enigszins controversieel De hacker heeft zich immers niet voorgedaan als de aangeefster. Hij heeft alleen haar mail gebruikt. In de toelichting wordt 'identiteitsfraude' ook niet genoemd, alleen 'hacken'. Een interessante vraag is hoe je zo'n geval als dit in een automatische classificatieprocedure herkent?

7.5.5 Voorbeeld HA-5

De aard van het misdrijf wordt in de, zeer korte, toelichting genoemd, namelijk hacking. Daarmee is het classificeren van deze case eenvoudig. De aangifte daarentegen staat qua lengte in sterk contrast met de aangifte. Dat is een uitgebreid verhaal met veel details, sommige relevant, andere niet en van weer andere is het niet duidelijk of ze iets met het misdrijf van de aangifte te maken hebben. Hoe de hack tot stand is gekomen wordt niet duidelijk. De aangeefster vermeldt dat ze een internetcafé in het buitenland heeft bezocht. Dat suggereert dat de hack mogelijk daar heeft plaatsgevonden, Maar is dat ook zo? Ook vermeldt de aangeefster dat niet alleen iets mis is met haar laptap, mobiele telefoon en een of ander device (tablet wellicht). Maar ook met de mobiele telefoon van een vriendin van haar. Ook staat er: '... dat blijkt vermoedelijk de hacker te zijn'. Het lijkt op het eerste oog een stellige bewering, maar het gebruik van 'vermoedelijk' zwakt deze weer af. Er staat eigenlijk: 'het lijkt de hacker te zijn'. Een vermoeden dus. Ook vreemd is dat de aangeefster anderen (haar vriendin en de broer van deze vriendin) laat werken, respectievelijk meekijken, op haar laptop. Voor iemand die zegt toegang te hebben tot verrouwelijke gegevens van haar cliënten gaat de aangeefster wel erg gemakkelijk om

met computerveiligheid. Een goede bron voor trefwoorden is deze case niet. Maar hij is ook niet helemaal nutteloos. Ik heb een poging ondernomen er enkele te vinden. De case is echter gemakkelijk te classificeren omdat het sleutelwoord 'hacking' wordt gebruikt. Echter hoe goed die vlag de lading dekt is onduidelijk. Er kan bijvoorbeeld ook vertrouwelijk informatie van haar cliënten gestolen zijn, waar de aangeefster geen weet van heeft. Maar dat is een algemeen probleem bij hacking. Als men een dergelijke case automatisch moet classificeren is het misschien goed in eerste instantie te kijken of er sleutelwoorden in de toelichting staan, en, als die veel korter is dan de aangifte, het hierbij te laten en het aangiftedeel te skippen.

7.5.6 Voorbeeld HA-6

Het misdrijf dat hier beschreven staat lijkt op Whatsapp fraude. De aangifte is een wijdlopig verhaal waarin gedetailleerd beschreven wordt wat er gebeurd is, waarbij ook anderen (vriendin en collega's) erbij worden gehaald. Er staat gelukkig in de toelichting dat het om hacken gaat, zodat dit voorbeeld als zodanig is te classificeren. Maar feitelijk gaat het om een poging daartoe, omdat de oplichting tijdig doorzien is door een oplettend familielid. Als bron van trefwoorden lijkt alleen de toelichting geschikt. Er zijn andere aangiftes die beter als bron voor trefwoorden kunnen dienen. Het gaat in deze aangifte soms over anderen. Er staat ook een vermoeden in van haar vriendin. Van deze case alleen de toelichting gebruiken voor classificatie lijkt de beste strategie. Er is een groot verschil in lengte van de toelichting en van de aangifte. Dat is mogelijk een aanwijzing om de aangifte te skippen en alleen de toelichting te gebruiken, zowel bij het classificeren (met een semantisch netwerk) als bron van trefwoorden.

7.5.7 Voorbeeld HA-7

In dit voorbeeld is sprake van hacking, hetgeen in toelichting en aangifte wordt genoemd. Er is door de melder een bestelling gedaan van een mobiele telefoon, zonder toestemming (en weten) van de eigenaar van het account bij een winkel. Dat is dus misbruik van bestellingen, een vorm van oplichting. In dit geval is de toelichting de bron van de relevante informatie om deze zaak te typeren. Hier is in feite sprake van meerder misdrijven (hacking en misbruik voor bestellingen). De aangifte is kort en zakelijk. De aangifte bevat slechts een beperkt aantal trefwoorden. Hij zou daarom ook helemaal geskipt kunnen worden als bron van trefwoorden.

7.6 Fraude met computer

7.6.1 Voorbeeld FC-1

In dit voorbeeld is de aangifte zelf een betere bron van informatie dan de toelichting. Er is sprake van een eerder misdrijf (een inbraak / insluiping) dat vermoedelijk verband houdt met het misdrijf waar het in dit voorbeeld om gaat. Het vermoeden van de aangever is dat het wachtwoord van de computer van de melder gezien is door de inbreker (vermoedelijk de vorige eigenaar van het bedrijf). Het wachtwoord staat vermeld bij de computer.Hier wordt een mogelijke verklaring hoe men aan bepaalde informatie is gekomen en wie de mogelijke dader is. De aangever noemt ook een mogelijk motief voor de vermoedelijke dader. De melder heeft behalve het bedrijf ook het e-mailadres van dat bedrijf overgenomen. Bij het classificeren van een misdrijf als dit met behulp van een semantisch netwerk is het verwarrend dat in de toelichting ook sprake is van een inbraak of insluiping. Dit betreft een andere zaak dan waar het in dit voorbeeld om gaat, ook al zijn de twee misdrijven mogelijk gelinkt. Als bron van trefwoorden is dit voorbeeld niet erg geschikt omdat het zo'n specifiek geval van oplichting is.

7.6.2 Voorbeeld FC-2

De toelichting bevat geen interpretatie van hetgeen de melder heeft verteld. Het is een beschrijving van twee vervolgacties naar aanleiding van de aangifte. Informatie over de aard van het misdrijf is in de aangifte zelf te lezen (oplichting). Maar het kan preciezer: het gaat om een vorm van phishing. De melder wordt misleid door een e-mail waarvan hij denkt dat deze afkomstig is van zijn telecomprovider. In werkelijkheid is deze echter gestuurd door een oplichter. De betaling voor een zogenaamd niet betaalde rekening komt uiteindelijk ten goede aan deze oplichter. De aangifte bevat een uitgebreid relaas van het gebeurde. In dit geval is de aangifte zelf informatiever dan de toelichting. Het misdrijf in kwestie is echter minder specifiek geclassificeerd ('oplichting') dan mogelijk was ('phishing'). In dit geval is een toelichting wel handig die concludeert dat het om cybercrime gaat, en meer in het bijzonder, om phishing. Dat zou dan in dit geval afgeleid moeten worden op basis van trefwoorden. Het is onduidelijk of dat zou lukken met een semantisch netwerk.

7.6.3 Voorbeeld FC-3

De typering van dit misdrijf is volgens de toelichting 'telecomfraude'. De aangever heeft het over 'computervredebreuk'. Geen van beide lijkt echter een goede aanduiding van het misdrijf. 'Phishing' lijkt de lading beter te dekken. Immers er is sprake van een mailtje met een 'malafide' link, waarvan het slachtoffer denkt dat die bonafide is en afkomstig van zijn telecomprovider. Dat is echter niet zo; de link is van een oplichter. Door de malifide link aan te klikken en de aanwijzingen te volgen, levert hij gebruiksnaam en inlogcode. Hiervan maakt de oplichter gebruik door op kosten van de aangever een smartphone te bestellen. Dat het in deze case om cybercrime gaat volgt uit beide sleutelwoorden 'telecomfraude' en 'computervredebreuk', hoewel die niet adequaat zijn.

7.6.4 Voorbeeld FC-4

Het misdrijf in dit voorbeeld zou men met kunnen typeren met 'internetoplichting'. De toelichting classificeert het misdrijf niet en in de aangifte is sprake van 'oplichting'. Die zou wat specifieker kunnen zijn omdat het op internet is gebeurd met een door een oplichter aangepaste website. De aangever en zijn vrouw zijn op een bonafide website geweest om een hotelkamer te boeken. De website was kennelijk gehackt, waardoor de betaling van de koper niet aan het (bonafide) bedrijf is gedaan, maar aan een oplichter. Vanwege het gebruik van een gehackte website is dit misdrijf een vorm van cybercrime. Uiteraard is het ook oplichting. Omdat het een specifiek fraudeverhaal betreft, is ervan af gezien om de aangifte in deze case als bron van trefwoorden te gebruiken.

7.7 Fraude met online advertenties

7.7.1 Voorbeeld FO-1

Dat het hier om oplichting draait is duidelijk: 'oplichting' wordt expliciet genoemd in aangifte en toelichting. Het is een vorm van 'internetoplichting', waarbij het internet louter als medium wordt gebruikt om kopers en verkopers met elkaar in contact te brengen. Het woord 'online handelssite' wordt in de aangifte genoemd. Dit type oplichting komt vaak voor. Toelichting noch aangifte bevatten trefwoorden die een (sterke) verbinding met cybercrime leggen.

8 Bevindingen mbt de geselecteerde cybercrime cases

In deze paragraaf zijn de belangrijkste bevindingen verzameld met betrekking tot de geselecteerde cybercrime cases die in Paragraaf 7 zijn besproken. De commentaren daar geven een wisselend beeld te zien als het gaat om de typering van deze cases op basis van trefwoorden. En ook als het er om gaat ze als bronnen voor trefwoorden te gebruiken.

In de bespreking van deze bevindingen wordt een onderverdeling gemaakt: opmerkingen die betrekking hebben op het aangiftedeel (in deelparagraaf 8.1), op het toelichtingendeel (in paragraaf 8.2) en opmerkingen die beide betreffen (in paragraaf 8.3). De bespreking van de aangiftes en toelichtingen gaat verder in paragraaf 8.4 waar verder wordt ingegaan op aangiftes en toelichtingen als basisteksten voor het classificeren van misdrijven. In paragraaf 8.5 worden aangiftes en toelichtingen bekeken als bronnen voor trefwoorden.

8.1 Aangiftes

Ten aanzien van de aangiftes kunnen we het volgende opmerken.

- De aangifte is bij iedere case aanwezig.
- De aangiftes zijn afkomstig van (in de regel) verschillende slachtoffers /melders.
- De slachtoffers / melders zijn (in de regel) niet deskundig ten aanzien van het beschrijven van misdrijven.
- Aangiftes zijn in de vorm van open tekst. De teksten van de aangiftes van de verschillende misdrijven verschillen behoorlijk in stijl, opbouw, het soort informatie dat wordt verstrekt, de aanwezigheid en soort van fouten, etc. De aangifte is soms een wijdlopig verhaal, met de nodige speculatie over wat gebeurd kan zijn of nog kan gebeuren. Het is begrijpelijk dat deze teksten vaak gekleurd zijn door emotie.
- In een aangifte kan een sleutelwoord voorkomen. Het is echter de vraag of dat betrouwbaar genoeg is om een case hiermee zondermeer mee te clasificeren, in ieder geval als het om type cybercrime gaat. Vermoedelijk wel als het gaat om classificeren op wel / niet cybrcrime.
- In afgiftes komen taalfouten voor.

Dit alles overziend kan men zeggen dat aangiftes soms een bruikbare basis vormen om misdrijven mee te typeren, maar niet één die altijd zondermeer betrouwbaar genoeg is.

8.2 Toelichtingen

Voor wat de toelichtingen betreft zijn de volgende opmerkingen aan de orde:

- De toelichting kan ontbreken in een aangifte.
- De toelichtingen zijn afkomstig van diverse politiefunctionarissen (verbalisanten). Zij zijn niet persoonlijk betrokken bij de zaken die ze beschrijven, anders dan de slachtoffers / melders. De teksten zijn daarom zakelijk van aard.
- Verbalisanten mogen vertrouwd worden geacht met het beschrijven van misdrijven.

- De toelichtingen zijn open tekst; er is geen structurering in rubrieken. Er lijken geen eisen te zijn ten aanzien van het invullen van toelichtingen.
- Toelichtingen bevatten vaak, maar niet altijd, de meest bruikbare informatie om een misdrijf te typeren.
- De toelichting is niet altijd een bondige samenvatting van het misdrijf met een interpretatie van een verbalisant. Soms ontbreekt die interpretatie zelfs. Soms wordt een toelichting gebruikt om acties te beschrijven die op touw zijn of worden gezet bij politie of justitie, naar aanleiding van de desbetreffende aangifte.
- Sleutelwoorden in toelichtingen vormen een betrouwbare basis voor het typeren van de bijbehorende cases, aangezien ze van politiefunctionarissen afkomstig zijn.
- In toelichtingen kunnen taalfouten voorkomen, zoals niet ongebruikelijk is in spontaan geschreven teksten die niet uitvoerig zijn geëdit.

In het ideale geval zouden toelichtingen dé basis voor de classificatie van misdrijven moeten zijn. Ze zijn imers opgesteld door ter zake deskundige personen. Helaas is de informatie die in een toelichting staat niet altijd relevant voor het classificeren van misdrijven. Nog vervelender is dat toelichtingen zelfs helemaal kunnen ontbreken in cases. Indien toelichtingen altijd verplicht zouden moeten worden ingevuld door verbalisanten bij iedere case, gestructureerd zouden zijn opgezet met zoveel mogelijk voorgecodeerde keuzemogelijkheden, zouden ze de perfecte bron zijn voor informatie over misdrijven. Helaas zijn ze dat in de huidige data niet.

8.3 Aangiftes en toelichtingen samen

Als we naar aangiftes en toelichtingen samen kijken kunnen we de volgende zaken opmerken:

- De kwalificaties van de misdrijven in toelichting en aangifte kunnen verschillend zijn. Men mag aannemen dat die in de toelichting betrouwbaarder is omdat die gedaan is door een politiefunctionaris, die in de materie thuis is.
- De toelichting zou, in het algemeen, zwaarder moeten wegen dan de bijbehorende aangifte, want afkomstig van een professional die weet wat hij moet beschrijven en die als niet-betrokkene een misdrijf beschrijft.
- Door met alleen trefwoorden te werken in een semantisch netwerk kan men geen onderscheid maken in een tekst (van aangifte of toelichting) tussen wat relevant is voor de case en wat irrelevant is (want een speculatie of een verwijzing naar een andere case). Daarvoor zou men de teksten ‘begrijpend’ moeten kunnen lezen. Dat is bij een semantisch netwerk niet het geval.
- Is het verstandig om de classificatie van een type cybercrime in een aangifte of toelichting zonder meer over te nemen? De wijze waarop een aangever zijn case typeert is mogelijk niet correct of niet precies genoeg. Moet het CBS daarom proberen om op basis van kenmerken een case zelf te classificeren? Er is geen garantie dat dit altijd lukt. Dit zou ook gedaan kunnen worden als controle op de classificatie zoals te vinden in de aangifte of toelichting.
- Sommige typen cybermisdrijven verlopen op een soortgelijke manier (bijvoorbeeld DDoS-aanvallen en ransomware) terwijl andere heel specifiek zijn (bijvoorbeeld computerfraude). Die van het eerste type zijn makkelijk te classificeren, die van het laatste type moeilijker (eventueel alleen interactief).
- Voor het classificeren naar wel/geen cybercrime zijn, in de regel, zowel aangiftes als toelichtingen bruikbaar.

Met de huidige poilitiedata ontkomt men er niet aan om zowel aangiftes als toelichtingen te gebruiken. In ieder geval zijn aangiftes altijd aanwezig. En in de regel bevatten toelichtingen betrouwbaardere informatie. Maar ze kunnen ook ontbreken, of informatie bevatten die niet relevant is voor de classificatie. Informatie uit aangifte of toelichting hoeven niet (helemaal) met elkaar de sporen. Sommige typen cybercrime zijn echter gemakkelijker te herkennen dan andere, omdat ze op een meer stereotype manier verlopen. Op een of ander manier moeten aangifte en toelichting worden gebruikt om hieruit naar beste vermogen relevante informatie uit te halen om cases te kunnen classificeren. In Paragraaf 11.4 worden mogelijke strategieën besproken.

8.4 Aangiftes en toelichtingen als bases voor classificatie

Uit bovenstaande bevindingen kan men concluderen dat voor het classificeren van misdrijven in de regel de toelichting te prefereren is boven de aangifte, omdat die afkomstig is van een professional, i.c. een politiefunctionaris. Echter een toelichting hoeft niet altijd aanwezig te zijn. En als deze aanwezig is, hoeft ze nog geen bruikbare informatie te bevatten voor het classificeren van het desbetreffende misdrijf, zoals procesinformatie over de afhandeling van het misdrijf door de politie of de relatie met andere misdrijven.

Van de trefwoorden zijn de sleutelwoorden ideaal bij classificeren van cybercrime cases. Deze zijn echter niet altijd de meest precieze. Echter voor het grover classificeren van en case op wel/geen cybercrime zijn ze nuttig.

Helaas is een toelichting open tekst en bestaat niet uit standaard rubrieken. Men mag ervan uitgaan dat een misdrijftypering in een toelichting betrouwbaarder is dan die in een aangifte. Maar wat te doen met een aangifte die geen toelichting bevat? Moet men zondermeer afgaan op wat een slachtoffer aan kwalificaties van het misdrijf dat hem/haar is overkomen? De wijze waarop een aangever zijn case typeert is mogelijk niet correct of niet precies genoeg. Moet het CBS in zo'n geval zelf op basis van trefwoorden in de aangifte een afleiding zien te maken? Een complicerende factor kan nog zijn dat de aangifte informatie bevat die niet terzake doet (speculaties over wat er gebeurd is, irrelevante details, speculatie over mogelijke andere, gerelateerde misdrijven), die misleidend kan zijn voor een semantisch netwerk. Het lijkt daarom beter om een dergelijke case altijd interactief te classificeren, gesteld dat die door een semantisch netwerk als zodanig herkend kan worden.

De vraag is ook of de aangifte zelf moet worden gebruikt bij classificeren als er een toelichting is en deze bruikbare informatie bevat om de desbetreffende case te classificeren. Indien in de toelichting een sleutelwoord als 'phishing', 'hacking', e.d. voorkomt, lijkt de aangifte voor het classificeren overbodig. Als de toelichting zo'n sleutelwoord niet bevat, maar de aangifte wel, dan dient men beter wat voorzichtiger te zijn. Dan zou bijvoorbeeld nagegaan kunnen worden of andere trefwoorden in aangifte of toelichting (indien aanwezig) in dezelfde richting wijzen als het sleutelwoord.

Een aangifte kan in principe betrekking hebben op meerdere misdrijven. Dat mag interessante informatie zijn voor de politie, maar het betreft een kwestie die buiten de scope van dit stuk valt. In dit stuk wordt het gezien als 'ruis' waar men last van kan hebben bij het automatisch classificeren met een semantisch netwerk. Deze 'ruis' werkt verstorend bij het oppikken van het echte 'signaal'. De vraag is echter in hoeverre men er in de praktijk daadwerkelijk hinder van ondervindt. Als het signaal sterk genoeg is (dwz voldoende informatie bevat over het misdrijf dat

de kern is van de aangifte) dan zal een beetje ruis dat signaal niet wezenlijk verstoren en is automatische herkenning van het type misdrijf nog steeds mogelijk.

Sommige cybercrime misdrijven zijn moeilijk te herkennen met trefwoorden omdat het vaak om heel specifieke manieren van oplichting gaat. Zulke gevallen moeten herkend worden als zijnde 'lastig'. Experts moeten proberen deze gevallen ineractief te classificeren. Herkenning van lastige gevallen door een semantisch netwerk is wellicht mogelijk in gevallen waar trefwoorden als 'fraude', 'oplichting', e.d. voorkomen.

8.5 Aangiftes en toelichtingen als bronnen van trefwoorden

Een andere vraag is of een aangifte een goede bron is voor trefwoorden. Die kwaliteit is nogal wisselend. Het lijkt ook van het type misdrijf af te hangen. Bij sommige typen cybermisdrijven ziet men minder variatie in de werkwijze (bijvoorbeeld phishing of ransomware). Bij andere (zoals hacking of computerfraude) veel meer. In die laatste gevallen is er een grotere kans dat er relatief veel informatie wordt gegeven over een specifiek geval van oplichting.

Nieuwe trefwoorden voor een semantisch netwerk moeten door terzake deskundigen moeten worden aangewezen. Deze kunnen de teksten begrijpend lezen en alleen die trefwoorden aanwijzen die volgens hen ter zake doen. De praktijk zal wel uitwijzen in hoeverre een aangifte of toelichting nuttige trefwoorden oplevert. Dit is een heel andere situatie dan bij een semantisch netwerk dat een hele aangifte en toelichting ter beschikking heeft om trefwoorden (en semantische verwante woorden) automatisch te vinden. Daarbij is geen sprake van begrijpend lezen. Dit is weer wel het geval als een case die niet door een semantisch netwerk kan worden geclassificeerd interactief moet worden getypeerd door een terzake deskundige.

9 Commentaar bij de geselecteerde niet-cybercrime cases

De hier besproken voorbeelden zijn afkomstig van dezelfde bronnen als de cybercrime voorbeelden besproken in Paragraaf 7. Ze zijn uitgekozen ter contrast met de cybercrime voorbeelden. Dat is van belang omdat één van de vragen waar het in dit stuk om draait is om cybercrime cases te herkennen uit alle misdrijven in die politiebestanden, bij gebruik van een semantisch netwerk.

Het zou kunnen dat cybercrime cases als niet-cybercrime cases worden geclassificeerd. Dat zou een nadere studie vergen van de voorbeelden in Paragraaf 7 waarbij dan moet worden nagegaan hoe waarschijnlijk het is dat die zouden worden misgeclassificeerd als niet-cybercrime. Daarvoor hebben we echter te weinig niet-cybercrime cases bekeken.[15)] Maar ook omgekeerd is er de kans dat niet-cybercrime cases als cybercrime cases worden gekarakteriseerd.

[15)] Dat is gebeurd omwille van de tijd. In een vervolgonderzoek zouden deze cases sowieso aan de orde komen.

De kans op zulke fouten van de eerste of tweede soort is het grootst als het gaat om randgevallen, cases die aan de ene kant van de grens zitten maar gemakkelijk zouden kunnen worden beoordeeld als behorende tot 'de andere kant'. Om die reden bekijken we hier enkele niet-cybercrime cases in dat licht en vragen ons af hoe groot de kans is dat ze als cybercrime zouden worden geclassificeerd. Die analyse is kwalitatief en beperkt zich tot vier gevallen die naar ons gevoel redelijk dicht liggen bij cybercrime. Dat is zeker het geval als er sprake is van fraude waarbij op een of andere manier een computer daarbij een rol speelt. Dan is esssentieel om te weten welke rol precies. Als gestolen voorwerp of als bron van misleiding en bedrog via gehackte sites, malware, etc. Omwille van de tijd is slechts een kleine selectie van niet-cybercrime misdrijven bekeken.[16)]

Dit onderwerp van misclassificatie is hier slechts aangestipt. Het uitgevoerde onderzoek was daar niet geschikt voor; het is een eerste verkenning van de data. Bovendien zouden veel meer cases nodig zijn om dat goed te beoordelen dan hier zijn gebruikt. Dit onderwerp zou, heel natuurlijk, later aan de orde komen, als een prototype voor een semantich netwerk voor cybercrime zou worden opgezet, getest en verbeterd, in een cyclisch ontwikkelproces.

De misdrijven die hieronder als voorbeelden worden opgevoerd zijn allemaal op een hoop gegooid als zijnde niet-cybercrime (NC) misdrijven. Een verdere onderverdeling is voor onze toepassing niet interessant. Bij het commentaar bij iedere case wordt ingegaan op de aard van het misdrijf en de kans dat deze zou worden geclassificeerd als cybercrime. Die discussie is kwalitatief van aard, op gevoel gebaseerd en niet op harde cijfers.

9.1 Voorbeeld NC-1

De toelichting ontbreekt in dit voorbeeld. Hier is sprake van een poging tot fraude, waarbij in eerste instantie de bedoeling was dat de aangever zogenaamde administratiekosten zou betalen. De aangever vermoedde echter dat de zaak niet in de haak was en heeft geen geld overgemaakt. Daarop werd gedreigd om zijn persoonsgegevens te gebruiken voor identiteitsfraude, door ze door te verkopen aan hackers, als hij niet snel betaalde. In de eerste zin van de aangifte staan aanduidingen die deze misdaad typeren: 'poging tot fraude' en 'chantage'. Door op deze woorden af te gaan zou het delict juist worden geclassificeerd. Er is wel sprake van een poging. De aangever is geen geld kwijt geraakt. Hij loopt echter nog steeds het risico dat zijn persoonsgegevens worden gebruikt door criminelen voor identiteitsfraude. De computer, internet, een website etc. zijn media waarmee werd gecommuniceerd. Maar hier was geen sprake van misbruik van deze middelen. De kans is groot dat deze aangifte—terecht—niet als cybercrime zou worden geclassificeerd.

9.2 Voorbeeld NC-2

Deze aangifte vermeldt meerdere misdrijven: diefstal van een portemonnee (met pinpas) en fraude met bankgegevens: geld is van de bankrekening gehaald vermoedelijk met behulp van de gestolen pinpas. De aangever geeft aan nogal nonchalant met zijn pincode om te gaan. Die zou

[16)] Ook omwille van de tijd is niet systematisch onderzocht in hoeverre cybercrime cases als niet-cybercrime zouden worden aangemerkt. Maar er is wel een beeld ontstaan door het werken met dit materiaal. De indruk is dat voor sommige typen cybercrime die kans heel klein lijkt (phishing, ransomware, bijvoorbeeld) en bij andere dat die kans groter is (bijvoorbeeld fraude met computers).

dus bij anderen bekend kunnen zijn. Verder vertelt de aangever nog dat een goksite waar hij ooit gebruik van heeft gemaakt, maar waar hij door zelfuitsluiting niet meer op terecht kan, nog geld heeft afgeschreven van zijn bankrekening. De aangever vertelt dat ook geld is overgemaakt naar een bankrekening die hij niet kent en waar hij zelf niet voor verantwoordelijk is. Er zijn ook overschrijvingen weer ongedaan gemaakt. Dat suggereert dat iemand toegang heeft tot zijn bankgegevens. Dat staat allemaal los van de diefstal van de pinpas. Mogelijk zijn daarom meerdere partijen betrokken bij de fraude: de dief van de pinpas, de goksite en een mogelijke derde partij die toegang had tot zijn bankgegevens. Maar sommige (of zelfs alle) partijen zouden ook dezelfde kunnen zijn. Hoe het precies zit is onduidelijk. Wat de aangever suggereert is pure speculatie.

In de toelichting wordt alleen gesuggereerd dat geld van de rekening van aangever is afgeschreven na de diefstal van de pinpas. In de aangifte wordt gerept over meer frauduleuze afschrijvingen, die mogelijk niets met deze diefstal te maken hebben. De aangifte is een wijdlopig verhaal, met speculaties en irrelevante informatie (bijvoorbeeld dat de aangever psychologische ondersteuning heeft vanwege het geld dat hij is kwijtgeraakt en dat hij kalmeringsmiddelen gebruikt).

De toelichting zelf gaat over de diefstal van een portemonnee met pinpas en misbruik van de pinpas. Dat wijst niet op cybercrime. In de aangifte wordt dit genoemd en ook dat er geld onrechtmatig is afgeschreven van zijn bankrekening en overschrijvingen zijn teruggeboekt. Dat wijst op bankfraude, waar mogelijk hacking of phishing aan zijn voorafgegaan. Dit wijst wel op cybercrime. Hoewel de aangifte hier helemaal niet over gaat, zou een semantisch netwerk dit wel oppikken en linken aan cybercrime. Daarom is in dit geval het risico aanwezig dat het ten onrechte als cybercrime wordt geclassificeerd. Door begrijpend te lezen wordt deze mogelijkheid uitgesloten. Maar dat is iets dat een semantisch netwerk niet doet/kan.

9.3 Voorbeeld NC-3

Het gaat in dit voorbeeld om inbraak. Daarbij zijn enkele zaken gestolen, waaronder een laptop en een smartphone. Bij het traceren van de dader is gebruik gemaakt van GPS dat op de gestolen laptop was geïnstalleerd.

De toelichting bij deze aangifte is uitvoerig (langer dan de aangifte zelf) om niet te zeggen wijdlopig en vooral procedureel van aard. Dit is anders dan bij de meeste toelichtingen. Het woord ‘inbraak’ komt letterlijk niet voor, echter in het relaas is sprake van ‘insluiping’, ‘inbreker’ en ‘hengelen’. Dat zou de link moeten leggen naar het misdrijf ‘diefstal’. In de toelichting komt ook de zinsnede ‘een deur openbreken’ voor weliswaar niet op de plaats van het delict maar in de woning van de vermoedelijke dader. Dat zou ten onrechte een verbinding leggen met ‘diefstal’, die echter in dit geval toevallig goed zou uitpakken. Zo’n verschil zou een semantisch netwerk niet oppikken. Dat vereist begrijpend lezen om zien dat dit los staat van het delict zelf, iets wat een semantisch netwerk niet doet/kan. Vreemd is dat de toelichting vermeldt dat de dader op heterdaad betrapt is, terwijl deze een tijd later bij zijn eigen wonng werd aangehouden.

De aangifte is ook wijdlopig. Er wordt wel gesproken over de kern van de zaak, namelijk een inbraak. Maar er staat ook informatie in die bijzaak is voor de case: over de indeling van het huis van de slachtoffers bijvoorbeeld en het gebruik van track-and-trace, die tot de aanhouding van de dader heeft geleid. Interessante achtergrondinformatie, maar voor de kern van de zaak niet

van belang. Dat is ook het geval bij de uitgebreide beschrijving van de dader en zijn woonsituatie en wat er in zijn woning is voorgevallen bij zijn aanhouding.

De vraag is of dit geval niet, ten onrechte, door een semantisch netwerk gezien zou worden als een cybercrime, wanneer uitsluitend wordt afgegaan op trefwoorden. Immers de gestolen voorwerpen waren telefoons en een laptop. En er is een computer is gebruikt bij het traceren van de gestolen laptop. Dat zijn allemaal woorden die worden gebruikt (als onderdeel van) trefwoorden bij cybercrime. Samen met het (afgeleide) trefwoord 'inbraak' zou het semantische netwerk mogelijk, en ten onrechte, kunnen afleiden dat het om hacking gaat. Experimenten zullen moeten uitwijzen of dat ook daadwerkelijk zo is.

10 Bevindingen mbt de geselecteerde niet-cybercrime cases

Er zijn slechts drie niet-cybercrime misdrijven bekeken voor dit stuk, die echter alle dicht liggen bij cybercrime, althans vanuit een semantisch netwerk bekeken. Dat betreft twee fraude-zaken en een inbraak (waarbij onder andere een laptop is gestolen). Misdrijven zoals openlijke geweldpleging, bedreiging, fraude met kentekenplaten, e.d. zijn bewust buiten beschouwing gelaten. Zij wijken te veel af van cybercrime, of in ieder geval de typen cybercrime die in dit document zijn beschouwd. Overigens ligt 'bedreiging' dicht bij een cybercrime als 'sexting'. Dat komt in dit stuk echter niet aan bod.

De vraag was in hoeverre en semantisch netwerk deze niet-cybercrime cases toch als cybercrime zou kunnen classificeren. Dat zou alleen kunnen als er trefwoorden in voor komen die wijzen naar cybercrime. In één geval is het vermoeden dat de kans heel klein is en in de andere twee zou er een grotere kans bestaan dat dit het geval is, maar die kans is vermoedelijk nog steeds beperkt. Dit zijn slechts vermoedens. Alleen empirisch onderzoek kan uitwijzen of dat klopt.

Men kan verwachten dat cases waar sprake is van computers (zoals laptops en tablets) en smartphones er kans is op verwarring. Deze apparaten kunnen gestolen worden, zonder dat er sprake is van cybercrime. Indien ze echter ontvreemd worden en de criminelen kans zien ze ook te gebruiken via een bestaand account, zou cybercrime kunnen plaatsvinden. De scheidslijn tussen de misdrijven is hier heel dun. 'Diefstal van laptop' of 'diefstal van gegevens' zijn fundamenteel anders: de eerste is geen cybercrime, de tweede wel. Als men als trefwoorden alleen 'diefstal', 'laptop' en 'gegevens' had zou men het onderscheid niet kunnen maken. Hier is het zaak om het gebruik te maken van het juiste samengestelde trefwoord: 'diefstal van laptop' of 'diefstal van gegevens'. Van dit soort gevallen kunnen er meer zijn. Als sprake is in een aangifte van 'software', of 'Windows' hoeft dit niet per se te betekenen dat daarmee computercriminaliteit is gepleegd.

11 Naar een semantisch netwerk voor cybercrime (SNCy)

Omdat de bruikbaarheid van de aangiften of toelichtingen sterk varieert in kwaliteit en bruikbaarheid voor het automatisch classificeren van (cybercrime) misdrijven, zou het wenselijk zijn als hierop kon worden gefilterd. De door een semantisch netwerk classificeerbare gevallen zouden dan meteen geautomatiseerd afgehandeld kunnen worden. De gevallen waarvoor dit niet mogelijk is zouden aangeboden moeten worden aan experts die deze gevallen interactief proberen te classificeren. Indien het grootste deel van het materiaal automatisch classificeerbaar blijkt en slechts een relatief klein deel interactief moet worden verwerkt, is al grote winst geboekt. Deze aanpak zou nader bekeken moeten worden.

11.1 Inleiding

We gaan hier nader in op de vraag of een semantisch netwerk voor cybercrime (SNCy) haalbaar is en, zo ja, hoe her eruit zou kunnen zien, of waar rekening mee moet worden gehouden. Bij 'haalbaarheid' spelen een aantal aspecten een rol:

1. **Data**: Informatie-inhoud van het bronmateriaal.
2. **Aanpak**: classificatie op basis van trefwoorden / sleutelwoorden.
3. **Doel**: niveau van classificatie:
   a. wel/geen cybercrime.
   b. naar type cybercrime.
4. **Inspanning**: opzet en onderhoud van een semantisch netwerk.

Het idee bij een semantisch netwerk (in de benadering van, en met de terminologie van (10)) is dat het uitgaat van een set trefwoorden, D -words genaamd, die eerder zijn voorgekomen in cybercrime cases en die geacht worden er karakteristiek voor te zijn. Tot de D-words rekenen we ook samengestelde trefwoorden, die uit meerdere woorden bestaan. Als het gaat om het dichotome onderscheid cybercrime / niet-cybercrime, zijn er D-words die typisch zijn voor cybercrime. Maar ze kunnen ook voorkomen in niet-cybercrime gevallen. Het idee is dat het relatieve aantal typische cybercrime D-words hoog is, of dat bepaalde sleutelwoorden voorkomen om te besluiten dat een case een cybercrime case is of niet. Dat zou een ja / nee beslissing kunnen zijn. Maar in de praktijk is er waarschijnlijk een grijs gebied waarvoor onduidelijk is om wat voor misdrijf het precies gaat. Hier wil men een expert naar laten kijken en beslissen en niet het netwerk een beslissing laten nemen, die moelijk is en tamelijk onbetrouwbaar. Anderzijds wil men de experts niet belasten met relatief simpele cases, die softwarematig kunnen worden afgehandeld en die vermoedelijk het overgrote deel van het materiaal betreffen. Hier zou een gecombineerde aanpak van SM en ML wellicht soulaas kunnen bieden, waarbij D-words worden gekozen door een SM en vervolgens door middel van ML wordt bepaald hoe de D-words als features tot een classificatie leiden. Dit wordt verder besproken in Paragraaf 11.5.

Een complicatie is nog dat in de praktijk allerlei synoniemen worden gebruikt voor dezelfde begrippen. Dat betekent dat verschillende D-words in feite dezelfde betekenis hebben en dus als 'semantisch gelijk' moeten worden beschouwd. Variatie kan ook ontstaan doordat soms een

meervoudsvorm wordt gebruikt en in andere keren en enkelvoudsvorm. Of een werkwoord dat in verschillende vervoegingen voorkomt in teksten. Dat zijn syntactische verschillen die niets met de semantiek van doen hebben en daarom niet relevant zijn. 'Semantische gelijkheid' is een equivalentierelatie die leidt tot een nieuwe klasse van woorden, namelijk C-words. Deze kan men gebruiken als min of meer abstracte concepten geschikt om klassen misdrijven mee te karakteriseren.

11.2 Herkenning van trefwoorden in aangiftes en toelichtingen

Als het gaat om herkenning van D-woorden in cases kan het onderscheid tussen relevante en irrelevante stukken tekst niet gemaakt worden.[17)] Het semantische netwerk zal proberen D-woorden te matchen in toelichting of aangifte (indien aanwezig) van een misdrijf. Een aangifte kan wijdlopig zijn en ook voor de herkenning van een case niet relevante, en zelfs misleidende informatie bevatten (bijvoorbeeld een speculatie over wat er gebeurd kan zijn of wat een gevolg zou kunnen zijn van het misdrijf waar iemand slachtoffer van is geworden of informatie over een vervolgactie van de politie). Daarvoor zouden de teksten 'begrijpend' moeten worden gelezen, wat niet gebeurt door een semantisch netwerk. Dat een semantisch netwerk ze toch gebruikt (moet gebruiken!) is een mogelijke foutenbron. De hoop is echter dat er andere trefwoorden zijn in toelichting of aangifte die daarvoor compenseren.

11.3 Classificeren: wel/geen cybercrime en type cybercrime

Uit het materiaal dat bekeken is in dit stuk lijkt het dichotome probleem (wel/geen cybercrime) nog de meeste kans maakt om met een semantisch netwerk te worden gedaan. De cases die een cybercrime betreffen bevatten vaak een sleutelwoord voor een bepaald type cybercrime. Indien men niet die verwijzing gebruikt maar afleidt dat het om cybercrime gaat identificeert men vermoedelijk vrij veel cases correct. Er zijn echter ook voorbeelden waarin zo'n trefwoord ontbreekt. In dat geval zou men op basis van voorkomende trefwoorden moeten afleiden dat het om cybercrime gaat. Hoe goed dat lukt kan hier niet worden aangegeven. Dat dient nader experimenteel te worden onderzocht. Interessant daarbij is of er ook niet-cybercrime misdrijven zijn die als cybercrime worden geclassificeerd.

De tweede opgave, om in geval van een cybercrime, met een semantisch netwerk te bepalen welk type cybercrime het betreft, lijkt een stuk lastiger. Dat heeft meerdere oorzaken, die besproken zijn in Paragraaf 8. Die oorzaken hebben enerzijds te maken met de informatie in de data en anderzijds met de mogelijkheden om een cybercrime misdrijf te typeren met behulp van sleutelwoorden en trefwoorden. Daarmee is het niet mogelijk onderdelen van de tekst te herkennen die speculatief zijn of die om een andere reden irrelevant zijn. Op voorhand kan men echter niet besluiten hoe ernstig deze 'ruis' is en hoezeer deze de kwaliteit van uitkomsten beïnvloedt. De enige manier om daarachter te komen is door experimenten uit te voeren.

[17)] Dit in tegenstelling bij het bepalen van deze woorden, omdat die door een expert gebeuren, die de teksten begrijpend kan lezen. Zie Paragraaf 7.

11.4 Strategieën

Afgaand op de voorbeelden van cybercrime misdrijven in dit stuk lijkt het duidelijk dat het indelen cybercrime/geen cybercrime haalbaar lijkt. Vaak staat het sleutelwoord 'cybercrime' (of een synoniem als 'computercriminaliteit') in de aangifte of de toelichting. Of er wordt een type cybercrime genoemd (bijvoorbeeld 'phishing'), waaruit 'cybercrime' is af te leiden. Men dient zich wel te realiseren welke informatie men gebruikt: uit de toelichting (van de politie) of de aangifte (van de aangever). Het ligt voor de hand die van de politie betrouwbaarder te achten, omdat die vaker met het bijltje hakken en misdrijven routineus classificeren.

Als echter de opgave is cybercrime misdrijven ook naar type te classificeren wordt het in het algemeen lastiger. In sommige cases worden de sleutelwoorden hiervoor expliciet genoemd in aangifte of toelichting. Als ze in de toelichting staan lijken ze doorgaans betrouwbaarder. In geval ze in de aangifte staan moeten ze misschien met enige voorzichtigheid worden gebruikt. Het komt voor dat toelichting en aangifte verschillende sleutelwoorden gebruiken. Het zou bij een grootschalig experiment met echte data moeten worden geverifieerd of er een verschil in betrouwbaarheid is tussen sleutelwoorden uit de toelichting en de aangifte.

11.4.1 Wel/geen cybercrime

Indien een case geen sleutelwoorden kent moet men het met trefwoorden doen. Ook in dit geval lijkt het goed onderscheid te maken naar de herkomst van de trefwoorden: toelichting of aangifte. In een experiment als boven genoemd kan men nagaan wat de beste strategie is om de gegevens (i.c. de trefwoorden en sleutelwoorden) te gebruiken. We vermelden er hier een aantal:

- alles op één hoop gooien, dus van zowel toelichting als aangifte. Overigens hoeft er niet altijd een toelichting te zijn. In dat geval kan men alleen de gegevens uit de aangifte gebruiken.
- gegevens uit zowel toelichting als aangifte gebruiken, en in geval van conflict (bijvoorbeeld het voorkomen van verschillende sleutelwoorden) die uit de toelichting gebruiken.
- in eerste instantie alleen de gegevens uit de toelichting gebruiken, indien aanwezig. Zo niet, dan de gegevens uit de aangifte gebruiken.
- alleen de gegevens uit de aangifte gebruiken.
- alleen de gegevens uit de aangifte gebruiken. Indien een toelichting aanwezig is alleen de gegevens uit de toelichting gebruiken.

De gegevens (trefwoorden en sleutelwoorden) kunnen ook op diverse manieren worden gebruikt. Bijvoorbeeld als het doel is om te filteren op cybercrime/niet cybercrime kan men de volgende strategieën gebruiken (niet uitputtende lijst):

- gebruik de sleutelwoorden in de toelichting en de aangifte. Indien niet aanwezig gebruik trefwoorden in de toelichting en de aangifte. Er kunnen meerdere sleutelwoorden voorkomen, die ook nog verschillend kunnen zijn. Indien ze allemaal op cybercrime duiden is de afleiding ondubbelzinnig 'cybercrime'. Indien er tenminste één is die naar cybercrime wijst, classificeer als 'cybercrime'.
- gebruik de sleutelwoorden in de toelichting en de aangifte. Indien niet aanwezig, gebruik de trefwoorden in de aangifte.
- gebruik de sleutelwoorden in de aangifte. Indien niet aanwezig gebruik trefwoorden in de toelichting en de aangifte.

– gebruik de sleutelwoorden in de toelichting. Indien niet aanwezig, gebruik de sleutelwoorden in de aangifte. Indien niet aanwezig, gebruik trefwoorden uit de toelichting en de aangifte.

De hier gebruikte sleutelwoorden zijn die welke meteen tot cybercrime leiden ('cybercrime', 'computercriminaliteit', 'cybercriminaliteit', etc) of die een bepaald type cybercrime noemen (bijvoorbeeld 'phishing', 'ransomware', etc.). Deze worden alleen gebruikt om hier 'cybercrime' uit af te leiden.

Ook is er nog een mogelijkheid om te 'spelen met' de toleranties: wenst men veel of weinig risico te lopen? Dit komt in feite neer op veel automatisch classificeren of juist terughoudend te zijn bij twijfel. Die twijfelgevallen moeten dan door een expert, interactief ('handmatig') worden geclassificeerd. Dat is natuuurlijk wel meer werk. De afweging kwaliteit vs. personele belasting speelt hier een centrale rol. Hier zijn wat strategieën om te besluiten welke cases men handmatig wil afhandelen (ook hier een niet-uitputtende lijst). De cases die men interactief wil afhandelen zijn bijvoorbeeld alle cases die

– geen toelichting bevatten.
– geen sleutelwoorden bevatten.
– fraudezaken betreffen.
– relatief weinig trefwoorden bevatten (in de toelichting en de aangifte samen).
– relatief weinig trefwoorden bevatten in de toelichting (indien aanwezig).
– relatief weinig trefwoorden bevatten in de aangifte.

Ook combinaties van deze criteria zijn mogelijk. Wat 'weinig trefwoorden' zijn dient men te definiëren. Bijvoorbeeld in termen van een percentage van woorden ten opzichte van de lengte van een tekst (toelichting, aangifte of beide samengenomen). Hierbij telt bij een samengesteld trefwoord (waaronder een samengesteld sleutelwoord) het aantal woorden waaruit dit bestaat.

De bovenstaande lijsten zijn geen van alle uitputtend. Indien gewenst kunnen andere strategieën worden uitgeprobeerd. In ieder geval geeft het gebruik van meerdere classificatiestrategieën zicht op het de informatiewaarde en betrouwbaarheid van de beide bronnen, de toelichting en de aangifte, waaruit een proces-verbaal kan bestaan. Men kan ook nog variëren met de fouttolerantie: het risico op misclassificaties. Dat is ook een afweging tussen meer volautomatisch afhandelen en het maken van classificatiefouten. Waar ligt de balans?

Opmerking: Men zou nog kunnen proberen na te gaan hoeveel misdrijven worden gerapporteerd in een case en ook om welke misdrijven het gaat. Dit betreft is vermoedelijk een vrij lastig probleem, en mogelijk niet met een SN op te lossen. Het werken met trefwoorden is mogelijk te grof. Begrijpend lezen is vereist, maar dat is een stuk lastiger en valt buiten de mogelijkheden van een SN. De vraag is of het wel om een groot probleem gaat. Vermoedelijk zal het in de meeste cases om één misdrijf gaan, maar om dat zeker te weten is nader onderzoek nodig. Een stap in die richting die misschien wel gezet kan worden is om cases te herkennen die mogelijk meerdere misdrijven noemen en om die door een expert te laten bekijken. Herkenning is welicht mogelijk door te constateren dat de trefwoorden bij meerdere sleutelwoorden (C-words, eigenlijk) passen. □

11.4.2 Type cybercrime

In het geval men cybercrime cases nader wil classificeren naar type cybercrime zijn ook weer een aantal strategieën denkbaar.

- Gebruik sleutelwoorden voor een type cybercrime in zowel toelichting als aangifte. Indien allemaal gelijk, dan is typering van de case eenduidig getypeerd. Indien verschillend, loot één van de mogelijke typen cybercrime, bijvoorbeeld met ongelijke kansen, evenredig aan het aantal keren dat bepaalde typen cybercrime worden geïmpliceerd.
- Gebruik de kenmerken in zowel de toelichting als de aangifte. Vergelijk die met de kenmerken die in het SN zijn geassocieerd met ieder type cybercrime. Bepaal het cybercrime type waarvan de trefwoorden de grootste overlap hebben met de trefwoorden in de case.
- Gebruik de kenmerken in alleen de aangifte. Vergelijk die met de kenmerken die in het SN zijn geassocieerd met ieder type cybercrime. Bepaal het cybercrime type waarvan de trefwoorden de grootste overlap hebben met de trefwoorden in de case.
- Gebruik de kenmerken in alleen de aangifte. Vergelijk die met de kenmerken die in het SN zijn geassocieerd met ieder type cybercrime. Loot nu een type cybercrime, naar rato van de overlap. Hoe meer overlap, hoe groter de kans.
- Gebruik sleutelwoorden voor een type cybercrime in uitsluitend de toelichting, indien aanwezig; zo niet, gebruik de aangifte in plaats daarvan. Indien allemaal gelijk, dan is typering van de case eenduidig getypeerd. Indien verschillend, loot één van de mogelijke typen cybercrime, bijvoorbeeld met ongelijke kansen, evenredig aan het aantal keren dat bepaalde typen cybercrime worden geïmpliceerd.
- Gebruik de kenmerken in uitsluitend de toelichting, indien aanwezig; zo niet, gebruik de aangifte in plaats daarvan. Vergelijk die met de kenmerken die in het SN zijn geassocieerd met ieder type cybercrime. Bepaal het cybercrime type waarvan de trefwoorden de grootste overlap hebben met de trefwoorden in de case.
- Gebruik de kenmerken in alleen de toelichting, indien aanwezig; zo niet, gebruik de aangifte in plaats daarvan. Vergelijk die met de kenmerken die in het SN zijn geassocieerd met ieder type cybercrime. Loot nu een type cybercrime, naar rato van de overlap. Hoe meer overlap, hoe groter de kans. Dit geldt alleen voor de kenmerken in de toelichting.
- Gebruik sleutelwoorden voor een type cybercrime in alleen aangifte. Indien allemaal gelijk, dan is typering van de case eenduidig getypeerd. Indien verschillend, loot één van de mogelijke typen cybercrime, bijvoorbeeld met ongelijke kansen, evenredig aan het aantal keren dat bepaalde typen cybercrime worden geïmpliceerd.
- Gebruik de kenmerken in alleen de aangifte. Vergelijk die met de kenmerken die in het SN zijn geassocieerd met ieder type cybercrime. Bepaal het cybercrime type waarvan de trefwoorden de grootste overlap hebben met de trefwoorden in de case.
- Gebruik de kenmerken in uitsluitend de aangifte. Vergelijk die met de kenmerken die in het SN zijn geassocieerd met ieder type cybercrime. Bepaal het cybercrime type waarvan de trefwoorden de grootste overlap hebben met de trefwoorden in de case.

11.4.3 Verificatiemogelijkheid

In paragrafen 11.4.1 en 11.4.2 staan enkele scenario's de 'varen op' de classificatie gemaakt door een verbalisant of een slachtoffer. Dat zijn de gevallen die sleutelwoorden gebruiken. Andere scenario's proberen (noodgedwongen) uit de trefwoorden af te leiden of het om een cybercrime gaat en, indien dat zo is, om welk type cybercrime het gaat.

Men zou ter verificatie ook eens kunnen nagaan of een classificatie op basis van sleutelwoorden ook hetzelfde oplevert als men die louter op basis van trefwoorden (die geen sleutelwoord zijn). Dat hoeft niet per te lukken omdat het aantal trefwoorden te beperkt is. Maar als het goed gaat is het een ondersteuning van de classificatie op basis van sleutelwoorden. Als zo'n afleiding iets anders oplevert is het zaak om dat onder de aandacht van een expert te brengen. Als een afleiding niet lukt wegens gebrek aan trefwoorden of anderszins, is het ook van belang dit te

melden aan een expert. Die kan kijken af er in de case nog trefwoorden staan die over het hoofd zijn gezien en kan deze alsnog toevoegen aan het SNCy.

11.4.4 Parametriseren van SNCy

Overigens gaat het hier niet over verschillende semantische netwerken, maar hetzelfde data echter parametriseerbaar is, waarbij diverse opties eenvoudig kunnen worden opgegeven door bepaalde parameters te specificeren (gebruik toelichting én aangifte/ gebruik alleen aangifte/ gebruik alleen toegifte etc.), hoe cybercrime typen te kiezen (loten met ongelijke kans/grootste overlap/loten op basis van overlap etc.).

Bij deze experimenten moet blijken welke onvolkomenheden in de data parten spelen en welke niet. Ook kan onderzocht worden wat het effect is van de mate van anonimiseren van de data. Het is mogelijk dat de data minder streng worden beveiligd dan in voor dit onderzoek is gedaan. Als bijvoorbeeld de namen van malware en teksten van deze software bekend zijn dan is meteen duidelijk dat het om ransomware gaat of om phishing, etc. Ook kan dan worden nagegaan welke cybercrime typen goed met een semantisch netwerk kunnen worden getypeerd en welke minder goed. Wat het laatste betreft zal dat vermoedelijk het geval zijn met misdrijven die aan (computer)fraude gerelateerd zijn.

11.5 SNCy vs. MLCy

Het maken van SNCy vergt het nodige voorwerk, dat semi-automatisch kan uitgevoerd. Dit is arbeidsintensief, maar heeft het voordeel boven het toepassen van een machine learning algoritme voor cybercrime (MLCy) dat meer sturing kan worden gegeven aan de informatie die men wenst te gebruiken. Dit heeft voordelen als een gebruiker van de data vraagt om een verantwoording van de toegepaste methode om tot een classificatie van misdrijven te komen. Maar ook voor het CBS zelf is dat goed om te weten en niet zondermeer te vertrouwen op een ‘black box’ ML procedure als een neuraal netwerk.[18)] Het is duidelijk dat de gebruikte classificatiemethode invloed heeft op de uitkomsten. Het is goed om te begrijpen hoe die tot stand zijn gekomen, zeker als er onverwachte resultaten uitkomen.

Overigens is er geen reden om aan te nemen dat cybercrime een uitzonderlijke set misdrijven is ten aanzien van classificatie. Als men in staat is een semantisch netwerk te maken voor dit type misdrijven dan zal dat vermoedelijk ook lukken voor andere misdrijven (en vice versa). Echter waar veel variatie te zien is in hoe bepaalde typen misdrijven worden uitgevoerd (zoals ‘fraude’ of ‘oplichting’), mag men verwachten dat automatische classificatie op basis van trefwoorden lastig is.

De aanpak die hier als uitgangspunt wordt genomen staat in contrast met die bij ML. Het voordeel dat de ML aanpak lijkt te hebben op die met een semantisch netwerk is dat het extraheren van relevante informatie uit een training set volledig (of grotendeels) automatisch gebeurt. Het nadeel is echter dat een statisticus geen idee heeft hoe dit precies in zijn werk gaat. Het ‘leerproces’ bij ML is complex en ondoorzichtig. In algemene zin begrijpt men wat er

[18)] ML gebruik makend van klassieke statistische technieken als logistische regressie of decision trees is een ander verhaal. Deze methoden zijn transparant.

gebeurt, maar niet precies. Welke data worden nou gebruikt en welke niet? Het zou best kunnen zijn dat de verkeerde informatie wordt gebruikt om tot een beslissing (classificatie) te komen.

Een bekend voorbeeld hiervan uit de begintijd van ML is de automatische herkenning van tanks (militaire voertuigen). Een training set was gemaakt met hierin foto's /contouren van zowel Amerikaanse als van Sowjet tanks. Dat systeem leek een tijdje correcte resultaten te geven, totdat het op een bepaald moment mis ging. Een Amerikaanse tank werd als een Sowjet tank herkend (en omgekeerd). Nadere analyse bracht aan het licht dat in de training set alle Amerikaanse tanks bomen op de achtergrond hadden en de Sowjet tanks niet.[19)] Op de foto die aan het systeem werd 'gevoerd' stond echter een Amerikaanse tank zonder bomen op de achtergrond.[20)] Echter de aan- of afwezigheid van bomen op de achtergrond is irrelevant voor de tank op de voorgrond. Die achtergrond is ruis die moet worden weggefilterd. Zo werd een toevallige samenhang tot een beslissend kenmerk verheven. Een persoon zou onmiddellijk herkend hebben dat dat niet de bedoeling is. Maar ML-software weet natuurlijk niet wat essentiële en wat toevallige kenmerken zijn. En de verschillen kunnen subtieler zijn dan een achtergrond met wel of geen bomen.[21)]

Het idee bij een SN voor cybercrime is dat de aanwezigheid van bepaalde trefwoorden in een toelichting of aangifte een aanwijzing vormen dat het om cybercrime gaat, of zelfs een bepaald type cybercrime. Bij de SN-methode bouwen experts zelf zo'n netwerk op. De kans dat hierbij toevallige relaties worden gebruikt kan dan uitgesloten worden geacht.

Tot nu toe zijn SN en ML tegenover elkaar geplaatst. Maar is dat terecht? Zou men de training set voor een ML voor cybercrime niet kunnen baseren op een deel van de tekst, namelijk dat deel dat ook een SN voor cybercrime zou gebruiken? Deze suggestie is hier niet nader onderzocht, maar is mogelijk een interessant onderwerp voor toekomstig onderzoek.

Het is wellicht ook een optie om te onderzoeken of een set misdrijven met daarin door experts aangewezen trefwoorden en sleutelwoorden kan dienen als een training set voor een MLA. Deze wordt dus getraind dat type woorden te herkennen in processen-verbaal met betrekking tot cybercrime. Deze stap is dus feitelijk een filterstap. Vervolgens zou een tweede MLA, helemaal losstaand van de eerste, gebruikt kunnen worden om op basis van deze trefwoorden cybercrime te herkennen en, waar dat het geval is, ook het type cybercrime. Men zou deze twee-staps toepassing:

tekst → trefwoorden → code

een restricted supervised MLA kunnen noemen en de een-staps toepassing

tekst → code

19) Of omgekeerd, maar dat doet niet ter zake.

20) Of van een Sowjet tank met bomen op de achtergrond.

21) Van dit verhaal bestaan vele varianten. Zie bijvoorbeeld `https://www.gwern.net/Tanks`. Het is mogelijk apocrief. Maar het gaat wel over een reëel probleem, namelijk dat een neuraal netwerk (of een andere ML-techniek) predictoren in de training data vindt die sterk correleren met de afhankelijke variabele. Maar de gevonden predictoren zijn niet van dien aard dat men ze zou willen gebruiken omdat ze gebaseerd zijn op een toevallige samenhang. Wat onbevredigend is in de ML-aanpak is dat het afgeleide model (en in het bijzonder de set predictoren daarin) niet bekend is, of niet meteen te begrijpen. Dan is het een kwestie van vertrouwen stellen in het model (en afwachten totdat het faalt). Men zou liever het model willen begrijpen.

een unrestricted supervised MLA.[22] Interessant is om zowel de een-staps als de twee-staps aanpak toe te passen en de resultaten te vergelijken.

Opmerking Het rapport (7), uit 2006, bespreekt enkele mogelijke toepassingen van ML en speculeert over toekomstige ontwikkelingen. Hoewel al een poos geleden geschreven, inspireerde het rapport me tot een idee dat van toepassing zou kunnen zijn bij het automatisch classificeren van cybercrime. Op p. 4 van genoemd rapport staat een opmerking onder het kopje '*Can unlabeled data be helpful for supervised learning?*'. Die deed mij denken aan het EM-algoritme, waarbij een statistisch model wordt geschat in het geval missing data aanwezig zijn, bijvoorbeeld enkele waarden van de afhankelijke variabele terwijl de scores of de onafhankelijke variabelen aanwezig zijn.[23] In de cybercrime context zou dat betekenen dat men, naast geclassificeerde cases (die dus 'tagged' of 'labeled' zijn) ook een aantal ongeclassificeerde ('untagged' of 'unlabeled') cases heeft. Men gebruikt vervolgens alleen de set van tagged cases om een machine learning model te schatten. Hiermee schat men de tags van de unlabeled cases. Vervolgens wordt de training set uitgebreid met deze geïmputeerde gevallen, en wordt het machine learning model opnieuw geschat. Deze nieuwe schattingen gebruikt men om opnieuw de tags te schatten van de cases die aanvankelijk unlabeld waren. Dit hehaalt men een aantal keren. Mogelijk leidt deze iterative procedure tot een vaste set labels voor alle, of een groot deel van de cases die aanvankelijk niet gelabeld waren. □

11.6 Opmerkingen mbt de bouw van een SNCy

Hoewel we niet uitgebreid willen stil staan bij dit onderwerp, willen we er hier toch enige aandacht aan besteden. In een vervolgproject zou hier uitgebreid op in moeten worden gegaan. We spreken hier over conceptuele aspecten. Die zijn belangrijk, maar zeker niet de enige die spelen. Van groot belang zijn zaken als software tools. Dit betreft zowel tools die al bestaan als tools die nog moeten worden gemaakt. In het ideale geval hoeft men niets te programmeren, en is alles al voorhanden. Maar waarschijnlijk is dat een illusie. Daarnaast is van belang te weten hoeveel inspanning het kost om een SNCy te ontwikkelen en te onderhouden. En ook om ermee om te gaan: welk deel van de data kan automatisch (en goed) worden verwerkt en welk deel vereist de inzet van experts. Op dat soort aspecten kan pas zicht worden gekregen na een prototype van een SNCy te hebben gebouwd.

In de eerste plaats is het van belang om een training set te maken met cybercrime cases. We veronderstellen dat deze data geanonimiseerd zijn.[24] Experts moeten dan al die gevallen classificeren, wel/geen cybercrime en indien er sprake is van cybercrime, van welke type. Ook als er sprake is van meerdere misdrijven zou dat moeten worden aangegeven. Vervolgens moeten in alle gevallen trefwoorden en sleutelwoorden worden bepaald. Dit is een intensieve klus en hulp

[22] In beide gevallen gaat het om supervised learning omdat in beide gevallen een traing set wordt gebruikt met 'tagged' cases (zijnde een aanduiding wel/geen cybercrime en in geval van cybercrime, welk type cybercrime). In het een-staps geval echter mag het ML algoritme de hele tekst gebruiken, terwijl die in het twee-staps geval beperkt is tot de daarin voorkomende trefwoorden.

[23] Het EM-algoritme is beschreven in (3) heeft betrekking op een maximum likelihoodscattingsmethode bij een geparametriseerd statistisch model. Echter ook bij andere schattingsmethoden, zoals kleinste kwadraten, is een soortgelijke aanpak te gebruiken. Convergentie moet dan nog wel bewezen worden.

[24] Hoe dat precies moet worden bewerkstelligd is feitelijk ook nog een onderzoekspunt. In deze studie heeft de auteur zelf een benadering gekozen (bij het maken van het tusenrapport) die hem redelijk leek, in de zin dat ze voldoende privacy bood voor betrokkenen en aan de andere kant een werkbaar resultaat opleverde in de vorm van classificeerbare beschrijvingen van misdrijven. Maar of dat echt zo is, vergt nadere reflectie en review door anderen. Het zou ook kunnen zijn dat de hier gekozen aanpak op bepaalde punten te streng is en op andere niet streng genoeg.

van een speciaal tool zou hier van groot belang zijn.[25)] Vervolgens moeten de trefwoorden en sleutelwoorden uit al deze cases worden verzameld, gededupliceerd en nabewerkt. Dit zijn de D-words in de terminologie van (10) Dat nabewerken heeft tot taak om tot C-woorden te komen, waar allerlei irrelevante variatie uit is gehaald: syntactische variatie door vervoegingen van werkwoorden het door elkaar gebruiken van enkelvouden en meervouden,etc. Op semantisch gebied leidt het bepalen van synoniemen van woorden en uitdrukkingen ook tot een reductie. Door het aangeven van hyperniemen/hyponiemen worden relavante relaties gelegd die van het belang zijn bij het classificeren van misdrijven (waarbij bijvoorbeeld van 'phishing' wordt aangegeven dat het een speciale vorm van cybercrime is). Per type cybercrime kan men nu lijsten van C-woorden maken die kenmerkend zijn voor ieder van deze misdrijven. Men kan nu vergelijken hoe de diverse typen cybercrime misdrijven van elkaar afwijken of juist overeenstemmen. En ook of alle typen misdrijven voldoende 'gescheiden' zijn kijkend naar de trefwoorden. Omdat samengestelde trefwoorden voorkomen kan men deze in afzonderlijke woorden ontleden en al deze woorden in één lijst zetten (samen met de enkelvoudige trefwoorden), met weglating van de niet-informatieve woorden (stop-woorden) zoals voorzetsels en lidwoorden. Zo'n lijst voor als het ware het vocabulaire / jargon voor cybercrime. Vervolgens kan men nagaan welke woorden in welke trefwoorden voorkomen bij welke typen cybercrime. Daartoe is het handig om ook te beschikken over allerlei varianten van de C-trefwoorden. Deze kunnen worden geplaatst in de bijbehorende D-lijst met trefwoorden. Die lijst is deels gevuld door informatie uit de training set, maar kan worden aangevuld door varianten die niet zijn waargenomen, maar bekend zijn (bijvoorbeeld andere vervoegingen van werkwoorden dan die zijn waargenomen).

Een aparte categorie trefwoorden vormen de sleutelwoorden. Die kunnen zowel bestaan op cybercrime-niveau ('cybercrime', 'computercriminaliteit', 'cybercriminaliteit', 'computercrime', etc.) en op het niveau van de diverse typen cybercrime ('DDoS-aanval', 'Phishing', 'Ransomware', etc.). De sleutelwoorden zijn de woorden waar SNCy het eerste naar op zoek zal gaan in een nieuwe case. Als zo'n woord er blijkt te zijn, is in ieder geval waarschijnlijk dat het een cybercrime case betreft. Als het sleutelwoord in de toelichting staat is waarschijnlijk hiermee het type cybercrime ook vastgelegd.

Het is ook mogelijk dat een case geen sleutelwoorden bevat. Dat moet op basis van de voorkomende kenmerken worden getracht te bepalen dat het

1. om cybercrime gaat, en
2. welk type cybercrime het gaat, als bekend is dat het een cybercrime is.

Het is daarom ook wenselijk in SNCy een lijst met trefwoorden op te nemen die typisch zijn voor 'cybercrime', echter zonder dat details bekend zijn over het type cybercrime.

11.7 Enkele losse gedachten

[25)] Nog voor de corona-tijd is hierover door de schrijver dezes gesproken met Guido van den Heuvel. Die zou toen proberen zo'n tool te maken. Of dat inmiddels ook gebeurd is en of de tool voldoende is uitontwikkeld en getest is, is mij niet duidelijk. Maar in ieder geval, dit probleem is eerder gesignaleerd en mogelijk deels (of welicht zelfs helemaal) opgelost.

11.7.1 Werkwijze

Achteraf, als alle trefwoorden zijn aangegeven in een tekst, dient beslist te worden om welk type misdrijf het gaat. De meest gedetailleerde aanduiding zou men daarvoor kunnen nemen. Dus als trefwoorden als fraude, oplichting, computerciminaliteit en phishing voorkomen, zou men phishing kunnen kiezen. Als het doel is om 'slechts' de cybercrime gevallen eruit te filteren volstaat 'computercriminaliteit'; 'phishing' is een speciaal geval van cybercrime (hyponiem) en kan ook worden gebruikt, inclusief de semantische relatie en bijbehorende afleiding.

11.7.2 Patronen en misdrijven

Het is wellicht nuttig de misdrijven nader te bestuderen op voorkomende patronen in hun werkwijze. Het is heel goed mogelijk dat er een beperkt aantal patronen is de dat karakteristiek is voor een bepaald type cybercrime. Bij helpdeskfraude valt op dat het altijd zogenaamde Microsoft medewerkers zijn die bij de scam betrokken zijn. Waarom trouwens ook niet Apple-medewerkers?[26)] Bij de scam in de hier bekeken voorbeelden zijn twee aanpakken naar voren gekomen: één waarbij een (lage) fee moet worden betaald, die te laag is om over te maken. Er moet door het slachtoffer meer worden betaald, en de oplichter belooft het teveel betaalde terug te betalen, waat vervolgens niet gebeurd. Bij de tweede weet de oplichter het slachtoffer bankinformatie te ontfutselen en gebruikt die om geld van het slachtoffer over te schrijven naar eigen rekeningen, vermoedelijk vaak in het buitenland. Deze patronen zouden zelfs als basis kunnen dienen om cybercrime te beschrijven en om er statistieken over te maken.

11.7.3 Classificeren op verschillende niveaus

Nu vindt classificatie plaats op verschillende niveaus van detail: cybercrime in het algemeen (zonder nadere detaillering) of een specifiek type cybercrime. Men kan echter besluiten om te classificeren op wel/niet cybercrime (grove classificatie) of op type cybercrime (fijne classificatie) of op een mengvorm daarvan: daar waar mogelijk is typeert men op type cybercrime, en als dat niet lukt maar wel op cybercrime dan neemt men daar genoegen mee. In geval van twijfel, of als het niet lukt om een case automatisch te classificeren, de optie gebruiken om de case interactief te laten typeren.

11.7.4 Contrasteren van typen misdrijven: overeenkomsten en verschillen

De performance van een semantisch netwerk zal beter zijn als de diverse onderscheiden categorieën helder van elkaar gescheiden zijn en ieder zijn specifieke set kenmerken kent. Bij de gegeven indeling van computercriminaliteit zou men paren van cybercrime typen met elkaar kunnen contrasteren en kijken naar overeenkomsten en verschillen. En men zou trefwoorden kunnen proberen te vinden die karakteristiek zijn voor ieder type cybercrime.

Ook kan men nagaan hoe cybercrime cases te onderscheiden zijn van niet-cybercrime misdrijven. Daarbij zou vooral helpen als men ieder type cybercrime zou contrasteren met 'naburige' niet-cybercrime gevallen en zou letten op overeenkomsten en verschillen.

[26)] Zijn Apple-gebruikers er zo van doordrongen dat Apple hen nooit zou benaderen om fouten op te lossen? Of is Apple-software zo goed dat er eigenlijk nooit fouten in voorkomen? Of zijn er veel meer Windows-gebruikers dan Apple-gebruikers? Een interessante vraag met een onduidelijk antwoord.

11.7.5 Cybercrime-classificatie

De verschillende typen cybercrime worden in dit stuk beschouwd als een ongestructureerde verzameling van misdrijven. Het zou wenselijk zijn om een 'classificatie-principe' te hebben waarmee men cybercrime systematisch kan beschrijven. De forensische literatuur kent artikelen die betrekking hebben op deze problematiek. Zie bijvoorbeeld: (1), (4), (9) en (2). In Figure 1 van (1) staat (in essentie) de volgende indeling:

- **Type I** Misdrijven waar de computer het doel is.
  - **Onbevoegde toegang**
    1. Hacking (zonder toestemming kopiëren, modificeren, weglaten of vernietigen van computerbestanden of software).
  - **Malafide software**
    1. Virus
    2. Worm
    3. Trojaans paard
    4. Software bom
  - **Verstoring van computer services**
    1. Onderbreking van computer services
    2. Ontzegging van computer services
  - **Diefstal of misbruik van computer services**
    1. Diefstal van computer services
    2. Misbruik van computer services
- **Type II** Misdrijven waarbij de computer het middel vormt.
  - **Schending van inhoud**
    1. Kinderporno
    2. Haatgedreven misdrijven
    3. Schadelijke inhoud
    4. Militaire geheimen
    5. Copyright misdrijven
    6. Diefstal van intellectueel eigendom
    7. Valsheid in geschrifte / Valse documenten
  - **Onbevoegde verandering van data of software voor persoonlijk gewin**
    1. Identiteitsdiefstal
    2. Online fraude
    3. Privacy
    4. Sabotage (ook mbt kritische infrostructuur)
    5. Internet fraude
    6. Electronisch manipuleren van aandelenmarkten
  - **Oneigenlijk gebruik van communicatie**
    1. Intimidatie
    2. Online geld witwassen
    3. Cyberstalking
    4. Spamming
    5. Samenzwering
    6. Afpersing (inclusief dreigingen ivm kritische infrastructuur)
    7. Drugshandel
    8. Social engineering fraude (zoals Phishing)

Bij het classificeren zou zo'n classificatie-principe heel nuttig zijn, niet alleen om typen cybercrime onderling te onderscheiden, maar ook om cybercrime cases van niet-cybercrime

cases te onderscheiden. Het zou met name kunnen helpen bij het vergelijken en contrasteren van diverse typen misdrijf en het maken van sets van trefwoorden die kenmerkend zijn voor de onderscheiden typen cybercrime. Stel men heeft een type cybercrime C, dat verder wordt onderverdeeld in twee typen C_1 en C_2. Dan is het zinvol om na te gaan hoe C_1 en C_2 precies van elkaar verschillen. Welke trefwoorden karakteriseren C_1 en welke C_2?

12 Conclusies en aanbevelingen

In deze afsluitende paragraaf verzamelen we enkele conclusies die deze studie heeft opgeleverd, op basis van een aantal cybercrime en niet-cybercrime cases (in geanonimiseerde vorm). Verder worden enkele suggesties gedaan voor mogelijk toekomstig onderzoek. De opmerkingen en sugesties zijn gegroepeerd in subsecties met ieder een specifiek thema.

12.1 Anonimisering van cases

De politiedata zijn in hun oorspronkelijke vorm ongeschikt voor statistisch onderzoek omdat ze direct tot personen herleidbaar zijn. Ze dienen daarom eerst geanonimiseerd te worden, om mogelijke herkenning van personen (door collega's) te voorkomen. De auteur heeft dat gedaan voor de cases die voor deze studie zijn geselecteerd. In Bijlage C wordt uiteen gezet hoe hij daarbij te werk is gegaan. Ook wordt daar een suggestie gedaan voor een speciaal SN (daar SNAn genoemd), bedoeld als tool om dit soort politiedata te helpen anonimiseren.

De lezer zij echter ook gewezen op (5) en (8). Deze master scripties zijn onafhankelijk van het onderhavige onderzoek tot stand gekomen. Zij zijn geheel gewijd aan het anonimiseringsprobleem van de politiedata waarvan hier ook gebruik is gemaakt. De auteur nam pas kennis van de inhoud van deze scripties toen hij de anonimisering van de cases voor deze studie al had voltooid en het onderhavige document in een vergevorderd stadium was.

12.2 Trefwoorden en sleutelwoorden eliciteren

Om cases goed te kunnen karakteriseren, lijkt de indruk te zijn uit de gebruikte voorbeelden, dat betrekkelijk veel samengestelde trefwoorden nodig zijn. Enkelvoudige trefwoorden voldoen vaak niet. Sommige cases zijn echter zo specifiek dat het lastig is goede trefwoorden te vinden. Het idee is dat trefwoorden generiek zijn, en dus bij meerdere cases kunnen worden gebruikt.

Het bepalen wat trefwoorden zijn is een zaak van experts. Zij moeten deze aanwijzen in teksten. De auteur vond het niet altijd eenvoudig trefwoorden aan te wijzen (maar hij is dan ook geen expert op het gebied van statistieken met betrekking tot misdrijven). Het vergt ook enige training (ook voor expert op het gebied van cybercrime) om adequate trefwoorden te vinden.

Voor het genereren van trefwoorden en sleutelwoorden zouden experts zeer gebaat zijn men een speciale, ondersteunende software tool. die helpt bij het identificeren van dergelijke woorden in nieuwe cases. Men wil vermijden dat trefwoorden worden aangewezen die al in het semantisch netwerk aanwezig zijn. Het moet een interactieve tool zijn omdat experts uiteindelijk

moeten beslissen wat trefwoorden zijn. Zij moeten door de tool van allerlei relevante informatie worden voorzien bij het verwerken van een nieuwe case waardoor ze snel beslissingen kunnen nemen. Hoe zo'n tool er precies uit moet zien moet volgen uit handmatig werk om genoemde type woorden aan te wijzen.

12.3 Bouw van een prototype SNCy

Of een semantisch netwerk voor cybercrime mogelijk is, is de eerste vraag die moet worden beantwoord. En als het antwoord bevestigend is speelt de vraag hoeveel tijd dat gaat kosten, zowel het opzetten van een SNCy en het onderhouden ervan. En ook is dan van belang wat voor toole beschikbaar zijn ter ondersteuning van bouw en onderhoud.[27)] Het lijkt op voorhand al duidelijk dat het maken van een ontologie voor cybercrime, en het onderhouden daarvan, de nodige inspanning zal vergen. Uiteraard moet men dat afwegen tegen het alternatief dat de verwerking op een andere manier zal geschieden. In het meest extreme geval betekent dit dat het 'handmatig' gebeurt, ondersteund door bepaalde software. Die verwerking is ook arbeidsintensief, foutgevoelig en kan alleen plaatsvinden wanneer experts beschikbaar zijn, zowel in de zin van 'voorhanden' als 'aan het werk'.[28)] Als een SNCy de bulk van de data correct automatisch kan verwerken is al veel winst behaald.

Natuurlijk geeft het bekijken van een beperkt aantal voorbeelden van aangiftes en toelichtingen geen definitief antwoord, maar wel een beeld. Er zijn twee deelvragen:

1. kan zo'n SN cybercrime van andere crime onderscheiden?
2. kan met een SN het type cybercrime worden vastgesteld, als bekend is dat het in een case om cybercrime gaat?

Op de eerste vraag lijkt mij het (voorlopige) antwoord positief te zijn, op basis van het materiaal dat ik gezien heb in deze studie. Maar nader (empirisch) onderzoek is nodig. Met betrekking tot de tweede vraag ben ik sceptischer. In ieder geval zal dat erg van het type cybercrime afhangen. Sommige zijn gemakkelijk te herkennen omdat ze en vrij stereotiep verloop hebben (DDoS aanval, phishing, ransomware) terwijl andere (vooral computerfraude gerelateerd) heel divers zijn. Ook hangt het er sterk van af of de toelichting of de aangifte goede (betrouwbare) sleutelwoorden bevatten. Als die er niet zijn zou men moeten kunnen varen op voldoende trefwoorden in de aangifte of toelichting. In de lastige gevallen (computerfraude gerelateerd) zal vermoedelijk de hulp van een expert onmisbaar zijn. Die moet zo'n case dan interactief ('handmatig') typeren.

Het probleem met de tweede vraag is herkenning via een SN, dat op basis van trefwoorden werkt. In veel gevallen is dat onvoldoende om te begrijpen wat in een aangifte of toelichting staat. Vooral bij aangiftes ziet men verhalen van leken, die er vaak ook op los speculeren. Vaak zijn de misdrijven redelijk uniek, zeker bij fraude. Bovendien zou men dan af moeten gaan op de benamingen die aangevers of verbalisanten gebruiken om een misdrijf te classificeren. De vraag is of dat altijd wel goed gaat en precies genoeg is. Ook het ontbreken van een strakke, heldere

[27)] We spreken hier over een semantische netwerk vor cybercrime. Ook mogelijk was geweest om te spreken over een ontologie voor cybercrime. Het opzetten van zo'n ontologie wordt in het Engels ook wel aangeduid als ontology learning. Voor een eerste oriëntatie op deze onderwerpen (zoals bij vele andere) is Wikipedia wel een goede en algemeen beschikbare ingang. Zie de lijst in Bijlage E waar ook verwijzingen in staan naar divere Wikipedia artikelen.

[28)] Een SNCy is wat dat betreft veel flexibeler. Het kan dag en nacht draaien, 24/7, zolang het CBS-computersysteem 'up and running' is, uiteraard.

indeling van cybercrime in subcategorieën ontbreekt en dat speelt parten. In veel gevallen is de toelichting het grootste houvast voor een classificatie. Maar lang niet altijd. Verbalisanten hebben kennelijk het recht (of de neiging) om die op een eigen manier in te vullen. Als dat strakker geregisseerd/voorgeschreven was en de verbalisant verplicht wordt het misdrijf te duiden was het iets anders. Nu wordt het verhaal vaak naverteld (wat korter misschien) of worden vervolgstappen beschreven. Dat laatste is ook nuttig maar zou eigenlijk in een aparte rubriek moeten worden vermeld.

De teksten die gebruikt worden in omschrijvingen en toelichtingen zijn vrij. Ze zijn opgesteld door verschillende individuen, door slachtoffers die aangifte hebben gedaan en/of door verbalisanten van de politie. Dit zorgt ervoor dat er een grote verscheidenheid is aan de informatie die wordt verstrekt. Dat hangt van de case af, maar ook van degene die de informatie levert of optekent. Soms is dat zakelijk en to the point. Andere keren is dat wijdlopig, met irrelevante details, speculaties over mogelijke gevolgen of vervolg-misdrijven. Soms is ook uit de tekst duidelijk dat er een poging is ondernomen tot het plegen van een misdrijf, maar de aangever heeft geen aantoonbare schade (geld kwijtgeraakt bijvoorbeeld). Voor de statistiek is het relevant om te weten of het gaat om een poging of een daadwerkelijk uitgevoerd misdrijf, waarbij mensen zijn benadeeld. Als een site gehackt is of anderszins persoonsgegevens zijn ontfutseld aan iemand is er gevaar dat iemand in de toekomst nog slachtoffer wordt van een misdrijf. Maar zolang dat niet gbeurd is is er sprake van een mogelijkheid en niet van een realisatie.

Men dient te beseffen dat de basis voor het classificeren is het materiaal dat is opgetekend door vele personen. Zij hebben vaak ook een mening over het type misdrijf dat hen is overkomen. Maar is het goed om zondermeer op deze oordelen af te gaan? Of is het beter naar meer informatie uit een relaas (aangifte en/of toelichting) te kijken en te proberen zelfstandig tot en oordeel te komen? Dat lijkt in sommige gevallen niet nodig, namelijk die gevallen dat een verbalisant (bondig) omschrijft om wat voor type cybercrime het gaat. Dan kan één trefwoord al voldoende zijn. In geval van aangiftes moet men misschien voorzichtiger zijn, zeker als ze via internet door het slachtoffer zijn opgesteld. In het algemeen mag men stellen dat de informatie uit de toelichting geschikter is om en case te typeren dan de aangifte zelf. Alleen hoeft er niet altijd een toelichting te zijn bij een aangifte. En een toelichting kan ook gaan over allerlei vervolgacties die zijn ondernomen na een aangifte en hoeft helemaal geen samenvatting van de case in kwestie te bevatten.

Het zou de statistische verwerking ten goede komen als de toelichtingen in de aangiftes gestructureerd zouden worden, waarbij het liefst zo veel mogelijk gesloten vragen worden gebruikt. Dit zou het maken van statistieken over misdrijven zeer ten goede kunnen komen.

Interessant is om te onderzoeken of ook een semantisch netwerk kan worden ontwikkeld om de ruwe data te beveiligen, waarbij concrete aanduidingen van personen, adressen, plaatsen, landen, talen, uren, valuta, bedrijven, datums, feestdagen, etc. worden vervangen door desbetreffende placeholders. Een vraag die daarbij op komt is of het werk dat hier handmatig is verricht ook (deels) geautomatiseerd uitgevoerd zou kunnen worden. Wellicht is het mogelijk om een semantisch netwerk te maken speciaal voor het anonimiseren van misdaadgegevens, niet alleen van cybercrime.

Het inzetten van een semantisch netwerk kost de nodige inspanning. Het voordeel is dat men sturing kan geven aan de informatie die wel, of juist niet, gebruikt wordt. Een alternatieve aanpak zou zijn machine learning te gebruiken. Daarbij worden voorbeelden van cybercrime cases gebruikt die allemaal interactief (‘handmatig’) worden geclassificeerd. Deze vormen de

training set. Deze wordt gebruikt om nieuwe aangiftes te classificeren. Deze classificatie kan ruw zijn (cybercrime/niet-cybercrime) of meer specifiek, waarbij gepoogd wordt bij de cybercrime cases precieser aan te geven wat voor type cybercrime het betreft.

12.4 Testen van classificatiestrategieën

12.4.1 Strategieën genoemd in Paragraaf 11

In deze paragraaf zijn een aantal classificatiestrategieën genoemd om misdrijven te classificeren, grof (wel/geen cybercrime) en meer verfijnd, indien een case cybercrime betreft (type cybercrime). Het ligt voor de hand deze strategieën eens uit te testen als een prototype van SNCy is geïmplementeerd. Vervolgens kunnen de uitkomsten onderling worden vergeleken en kan geprobeerd worden goed van minder goede strategieën te scheiden. Andere hier niet genoemde strategieën komen natuurlijk ook in aanmerking om te worden uitgeprobeerd.

12.4.2 Classificeren mbv trefwoorden, ter controle

Het lijkt een goede praktijk om niet zondermeer af te gaan op sleutelwoorden die in een aangifte of toelichting worden genoemd om cases te classificeren. Het loont de moeite ook eens te proberen met behulp van SNCy op basis van trefwoorden af te leiden wat voor case men heeft: wel/geen cybercrime en in geval van cybercrime, om wat voor type cybercrme het gaat. Uitgezocht moet worden of dat vaak lukt, hoe vaak men het moet toepassen (bijvoorbeeld steekproefsgewijs, met welke steekproeffractie?) of dat het altijd moet gebeuren, ter controle, en of dat haalbaar is en ook nodig (mischien blijken sleutelwoorden betrouwbaar genoeg, bijvoorbeeld in het geval wel / geen cybercrime). In geval er dezelfde resultaten uitkomen geeft dat wat meer vertrouwen in de uitkomst. En als het niet uitkomt is het zaak de case eens te laten inspecteren door een expert.

12.5 Structurering van toelichtingen

In de huidige processen-verbaal die de politie gebruikt is de toelichting in te vullen als vrije tekst. Het zou zeer voordelig zijn als daar enige stuctuur in zou worden aangebracht. In Paragraaf 5 is dit punt aan de orde gesteld. Met enkele vrij simpele veranderingen zou heel veel gewonnen zijn. Het maken van statistieken over misdrijven (in het bijzonder cybercrime) zou een stuk simpeler zijn en het zou dan niet nodig zijn gevoelige persoonsgegevens te gebruiken omdat de aangifte daan overbodig zou zijn. En in de toelichting zou de aard van het misdrijf zijn aangegeven. Het vragenlab zou nog advies kunnen geven hoe de toelichting te structureren. Daar kunnen gevoelige rubrieken bij zitten. Die hoeft het CBS niet te krijgen voor het maken van statistieken over misdrijven in Nederland. Het is uiteraard niet aan het CBS om hierover te beslissen. Maar het kan ook geen kwaad het onder de aandacht te brengen. Het levert voor zowel de politie als het CBS grote voordelen op, tegen geringe extra kosten.

12.6 Enkele losse opmerkingen

Hier nog enkele kwesties en vragen die bij me opkwamen bij het doorspitten van de aangiftes in Paragrafen 7 en 9:

Pogingen tot een misdrijf Soms is in een aangifte sprake van poging tot een misdrijf. Bijvoorbeeld een poging tot het gebruik van ransomware of phishing. De aangever is er niet ingetrapt, kreeg op tijd argwaan of is door een familielid gewaarschuwd, etc. Telt zo'n geval nu op dezelfde manier mee in de statistieken als een case waarbij de aangever de dupe is geworden van een misdrijf en is benadeeld, materieel of anderszins? En hoe zit het met een voornemen tot een misdrijf? En het aanzetten tot een misdrijf? Tellen die wel/niet mee in de statistieken? Misdrijven waarvoor geen aangifte is gedaan tellen vermoedelijk sowieso niet mee omdat ze (bijna per definitie) niet bekend zijn bij de politie (tenzij een aangever erover rept).

Gevaar voor dubbeltellingen? Bestaat het risico dat misdrijven dubbel worden geteld. Bijvoorbeeld in het geval van bankfraude, ten gevolge van phishing. Het slachtoffer doet aangifte, maar de bank misschien ook. Wordt er altijd een link gelegd tussen beide aangiftes?

Meerdere misdrijven in aangifte Als in een aangifte meerdere misdrijven worden genoemd, moeten die dan allemaal apart worden 'geturfd'? Of is de insteek: één misdrijf per aangifte? Als de bedoeling is dat alle misdrijven in een aangifte apart meetellen in de statistieken dan moeten aangiften door meerdere 'misdrijffilters' worden gehaald. Hoe goed lukt het om automatisch meerdere misdrijven uit een aangifte te halen?

Classificatie cybercrime Er is behoefte aan een systematiek om cybercrimes in te delen naar type. Gewoonlijk volstaat men met een opsomming van voorbeelden, zoals in Paragraaf 4. Maar dit is geen systematische indeling. Wat nodig is is een aantal principes, indelingscriteria, waarop een onderverdeling kan worden gebaseerd. Die zou zodanig moeten zijn opgezet dat ook nieuwe vormen van cybercrime hierin kunnen worden ondergebracht, dan wel dat de systematiek eenvoudig (en natuurlijk) kan worden uitgebreid zodat deze nieuwe vormen van computercriminaliteit daarin passen. Zo'n systematische indeling van cybercrime is van belang voor het maken van goede statistieken over dit onderwerp, door het CBS. En ook voor andere instanties die met dergelijke statistieken te maken hebben. Een systematisch opgezette classificatie is daarvoor de basis. [29)]

12.7 Tot besluit

De belangrijkste conclusie die ik aan dit onderzoek wil verbinden is dat de grootste stap voorwaarts zou worden gemaakt als de toelichting gestructureerd zou worden. Als hierbij ook de rubriek 'type misdrijf' zou worden opgenomen als verplicht in te vullen veld, is een ideale situatie geschapen, zeker als de voornaamste mogelijkheden (bijvoorbeeld typen misdrijven) zouden zijn voorgecodeerd. Een politiefunctionaris vult dit veld in (een deskundige) en het CBS kan deze informatie overnemen. Het CBS hoeft niet zelf te classificeren, en ihb hoeven geen gevoelige data naar het CBS te worden gestuurd. Of, als men dit wil vermijden, hoeven de data voorafgaand aan de analyse te worden geanonimiseerd (idealiter door de politie, anders door het CBS). Het structureren van de toelichting lijkt niet zo moeilijk. Het CBS kan een concreet voorstel hiertoe uitwerken. Het is dan aan de politie om hier gebruik van te maken, eventueel na aanpassing van dit voorstel.

Zolang echter de toelichtingen bestaan uit open tekst en er eigenlijk geen sturing is op de inhoud hiervan (de huidige situatie) zal het CBS het met deze data moeten doen. Hieronder enkele suggesties voor mogelijke activiteiten.

[29)] Mogelijk bestaat die al. De auteur heeft dat verder niet onderzocht omdat dat buiten de scope van deze studie viel.

Deze verkenning nodigt uit om aan de slag te gaan met een serieus experiment met een flinke hoeveelheid (geanonimiseerde) politiedata. Op basis hiervan kan dan gepoogd worden een prototype SNCy te bouwen en proefondervindelijk na te gaan hoeveel procent van de cases automatisch kan worden geclassificeerd, met welke strategie dat het beste kan, en wat de kwaliteit is van de resultaten dit oplevert, dat wil zeggen, correct geclassificeerde cases. Vervolgens moet worden nagegaan hoeveel cases nog interactief moeten worden geclassificeerd door experts. Daarbij dient ook onderzocht te worden waarom deze gevallen niet automatisch geclassificeerd konden worden en wat er ontbrak om dat wel te kunnen doen. Het is belangrijk dat dit interactieve classificeren ondersteund wordt door software die ervoor zorgt dat de experts alle relevante informatie die in het systeem zit beschikbaar wordt gesteld aan de experts, zodat zij hun werk snel en goed kunnen doen.

Deze experts zijn overigens ook nodig om in nieuwe cases nieuwe trefwoorden en sleutelwoorden te vinden, en mogelijk nieuwe vormen van cybercrime, met hun eigen trefwoorden en sleutelwoorden.

De inzet van een SNCy is geslaagd als het merendeel van de misdrijven correct kan worden geclassificeerd in de ruwe vorm: wel / geen cybercrime. Het classificeren van cybercrime gevallen naar type cybercrime is een apart geval. Dat is lastiger omdat de data op dit punt vaak minder, of minder betrouwbare, informatie bevatten, althans voor sommige typen cybercrime. De mogelijkheden om te classificeren en de kwaliteit van het resultaat hangen sterk af van het type cybercrime.

Ook kan bekeken worden of een MLCy kan worden gebruikt om misdrijven te classificeren op (type) cybercrime. Onderzoek hiernaar is al aan de gang. De vraag daarbij is of dat unsupervised of supervised moet. SNCy is een aanpak die ‘zeer supervised’ is en daarom ook de nodige investering in tijd en moeite vergt. De vraag is of een supervised ML-aanpak mogelijk is, wellicht geïnspireerd door een SN-aanpak. Deze suggestie is wat meer uitgewerkt in Paragraaf 11.5 onder de naam van twee-staps procedure. Vergelijking met de één-staps procedure, waarbij ML rechtstreeks op de (beveiligde) politiedata wordt toegepast, ligt voor de hand. Een interessante vraag hierbij is in hoeverre de ruis in de data (speculaties, e.d.) het classificeren beïnvloeden.

Referenties

[1] A. Alkaabi, G. Mohay, A. McCullagh & N. Chantler (2011). Dealing with the Problem of Cybercrime, in: I. Baggili (ed.), Digital Forensics and Cyber Crime, Springer, pp. 1–18.

[2] A. Chandra & M.J. Snowe (2020). A Taxonomy of Cybercrime: Theory and Practice, *Int. J. of Accounting Information Systems*, 20 pages.

[3] A. Dempster, N. Laird & D. Rubin (1977). Maximum Likelihood from Incomplete Data via the EM Algorithm. *J. of the Royal Stat. Soc., Series B*, pp. 1–38.

[4] S. Ibrahim (2016). Social and Contextual Taxonomy of Cybercrime: Socioeconomic Theory of Nigerian Cybercriminals, *Int. J. of Law, Crim. & Justice*, pp. 44–57.

[5] M. Lemain-van der Nest (2021). Named Entity Recognition: Identifying NER indicators in Dutch Police Reports, Master thesis, Computational Lexicology and Terminology Lab, Department of Language and Communication, Faculty of Humanities, Free University Amsterdam.

[6] T. Mitchell (1997). *Machine Learning*. McGraw-Hill.

[7] T. Mitchell (2006). The Discipline of Machine Learning. Report, Machine Learning Department, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, USA.

[8] A. Shrestha (2021). BERTje-based Automatic Anonymization of Dutch Police Reports, Master thesis, Computational Lexicology and Terminology Lab, Department of Language and Communication, Faculty of Humanities, Free University Amsterdam.

[9] H. Singh Brar & G. Kumar (2018). Cybercrime: A Proposed Taxonomy and Challenges, *J. of Computer Networks and Communication*, 11 pages.

[10] L. Willenborg (2021). Semantic Networks for Automatic Coding (v2), Discussion paper, CBS, Den Haag.

Bijlage

A Selectie en voorbewerking van de geselecteerde cases

De teksten van de aangiftes en toelichtingen uit de politiebestanden zijn voorbewerkt voordat ze zijn geanalyseerd en de resultaten in dit stuk zijn opgenomen. In deze bijlage wordt aangegeven wat er met het ruwe (maar geanonimiseerde) bronmateriaal is gedaan voordat de analyse ervan is gestart. Die analyse heeft een aantal concrete resulaten opgeleverd die in dit document zijn terug te vinden, namelijk een inzicht in het soort informatie dat te vinden is in de aangiftes en toelichtingen. Dat vindt zijn weerslag in de opmerkingen per case. Het andere resultaat zijn de trefwoorden en sleutelwoorden die de auteur in de bestudeerde teksten heeft aangewezen. In eerste aanleg zijn die trefwoorden in de teksten zelf gemarkeerd met behulp van door de auteur geproduceerde macro's in een LaTeX document, waar de (geanonimiseerde) teksten in waren opgenomen. Een probleem daarbij was dat trefwoorden soms uit meerdere woorden kunnen bestaan (samengestelde trefwoorden) en dat zulke samenstellingen na elkaar in een tekst (aangifte of bijbehorende toelichting) kunnen staan. Die moeten onderscheiden worden. Dat is zo gedaan dat ze ook visueel gescheiden zijn door te werken met verschillende codes.

Aanvankelijk was het idee om de (geanonimiseerde) aangiftes en toelichtingen plus de gemarkeerde trefwoorden in dit stuk op te nemen. Het voordeel zou zijn dat men de trefwoorden per case ziet. Van dat idee is afgezien omdat het zou leiden tot een vertrouwelijk document dat slechts door een heel kleine groep van CBS-ers (belast met het maken van statistieken over misdrijven) toegankelijk zou zijn. Door geen (geanonimiserde) persoonsdata in het verslag op te nemen zou weliswaar de informatiewaarde enigszins afnemen maar zou de potentiële lezerskring een stuk groter worden, omdat dit stuk niet meer vertrouwelijk is.

Deze beslissing betekende achter wel dat nog wat extra werk nodig was: de trefwoorden moesten uit de teksten worden gehaald en bewerkt om ze in tabellen op te kunnen nemen is dit stuk. De teksten van aangiftes en toelichtingen zijn alle verwijderd uit de tussenversie van dit document. Alleen de opmerkingen per case zijn gehandhaafd, afgezien van mogelijk enkele redactionele aanpassingen.

Hieronder zijn enkele relevante aspecten van dat proces van kennisextractie beschreven. Deels als verantwoording en deels met het oog op toekomstig gebruik.

A.1 Keuze van de cases

De keuze van misdrijven voor deze studie zou men random kunnen noemen, in die zin dat op geen enkele manier met de inhoud van de omschrijvingen en bijbehorende toelichting rekening is gehouden, behalve dat het om cybercrime moest gaan en niet over een ander type misdrijf, zoals fraude of diefstal. Er is ook niet voor gezorgd dat alle onderscheiden typen cybercrime (in voldoende mate) in de voorbeelden zijn gerepresenteerd. Wat de steekproef heeft opgeleverd zit erin en niet meer.

A.2 Informatie-extractie uit de politiebestanden

De brondata waren Excelbestanden van de politie. Omdat het aantal geselecteerde cases niet zo groot was is besloten de benodigde informatie door middel van'copy-paste' uit de politie bestanden te zetten naar een tekstbestand.[30)] Het bleek het handigste om hele cases te kopiëren en de niet benodigde varabelen te verwijderen uit het doelbestand. De benodigde informatie per case was alleen de aangifte en (indien aanwezig) de toelichting. De teksten van aangiftes en toelichtingen kwamen uiteindelijk terecht in een (voorloper) van een belangrijke tussenversie van het onderhavige document, aangeduid als het 'tussenrapport' (zie Paragraaf A.7). Daar zijn de teksten verder 'geLaTeXiseerd'. Verdere bewerkingen staan in navolgende paragrafen beschreven.

A.3 Teksten van aangiftes en toelichtingen

De aangiftes en toelichtingen zijn vrije teksten, die in hoge kunnen worden ingevuld door aangevere en verbalisten. Aangezien dit veel verschillende personen en cases betreft, is er een grote diversiteit aan stijlen, woordkeuzes, formuleringen, etc. In de teksten zitten slordigheden en taalfouten. Die kunnen menselijke lezers meestal zonder probleem correct verwerken. Bij softwarematige verwerking van de teksten dient er echter rekening mee te worden houden. Ook dit waarschijnlijk helemaal geen struikelblok. Het vergt alleen extra programmeerinspanning.

De teksten zijn licht geëdit om hun leesbaarheid te vergroten. Zinloze fragmenten voor onze toepassing zijn soms weggelaten (bijvoorbeeld opsommingen van 'slechte' e-mailadressen omdat die toch allemaal door placeholders zouden zijn vervangen, of een opmerking dat een aangever zich niet goed behandeld voelt, etc.). Het gaat in dit stuk over informatie die relevant is voor het classificeren van misdrijven, in het bijzonder die met betrekking tot cybercrime. Het gaat hier niet over de letterlijke teksten zoals die door een automatisch classificatieprogramma moeten worden gelezen, en waarbij dit te maken krijgt met bepaalde imperfecties in de teksten van aangiftes en toelichtingen. Dat is uiteraard ook relevant, maar het moet in een ander document aan bod komen, waar de classificatiesoftware (een semantisch netwerk, bijvoorbeeld) wordt beschreven.

A.4 Voorbewerking van de teksten van aangiftes en toelichtingen

In de teksten waren niet-ASCII karakters hersteld, zoals 'ï', 'ë','é', etc. omwille van de leesbaarheid. Deze correcties waren handmatig uitgevoerd.

Aanpassingen waren gemaakt om een woord foutloos in LaTeX weer te kunnen geven. Een voorbeeld betreft woorden met underscores, zoals `A_B_C.txt` . Om fouten te vermijden in de LaTeXcode moesten extra underscores worden geïntroduceerd, zoals `A\_B\_C.txt`. In de afgedrukte tekst zijn de underscores dan verdwenen en staat er A_B_C.txt.

Spellingsfouten zijn soms verbeterd, om de leesbaarheid te verhogen. Er is geen poging gedaan ze allemaal op te sporen en verbeteren. Dat zou een verkeerd beeld van de kwaliteit van de teksten geven. Dat is voor de exercitie in dit stuk geen probleem, maar wel als men software gebruikt om de teksten-met-fouten te lezen en 'begrijpen'. Deze software dient rekening te

[30)] Omdat dit vaak lange teksten waren bleek het lastig te zijn om de alleen deze velden te copy-pasten.

houden met allerlei fouten in de teksten. Soms is interpunctie toegevoegd of aangepast. Maar dat is incidenteel gebeurd, niet systematisch. Bij de automatische verwerking zou dat vermoedelijk niet tot een eenvoudigere verwerking van de teksten geleid hebben. De leesbaarheid was er echter mee gebaat.

Omwille van de leesbaarheid zijn soms LaTeX commando's ingevoegd in de brontekst, zodat de afgedukte tekst lijkt op de originele tekst in Excel. Dat doel om gelijkenis met de originele tekst na te streven is echter niet tot in extremo doorgevoerd.

A.5 Verwijdering van procesinformatie uit de toelichtingen

Soms wordt in een toelichting vermeld wie de verbalisant was, wat voor stukken zijn ingeleverd als bewijsmateriaal, wat voor acties zijn ondernomen en door wie, etc. Dit soort procesinformatie over een case is niet relevant voor het doel van het onderhavige document en is daarom weggelaten. De hoop (en de verwachting) is dat dat geen wezenlijke invloed heeft als een semantisch netwerk alle informatie vermeld bij een case zou moeten verwerken.

In de aangiftes staat soms ook irelevante informatie voor het clasificeren van de case. Die is echter niet weggehaald. Immers daarmee zou men het classificeren (aanzienlijk) kunnen versimpelen. Dat is niet de bedoeling.

A.6 Groepering van de cases

De omschrijvingen en bijbehorende toelichtingen zijn gegroepeerd naar type cybercrime, zoals phishing, hacking, etc. Hierbij zijn de aanduidingen gevolgd die in de cases zelf worden genoemd. In enkele gevallen zijn meerdere labels te koppelen aan een misdrijf. Dan is er één gekozen die het belangrijkste lijkt en die is gebruikt om de cases te labelen en op basis hiervan te groeperen.

A.7 Tussenrapport

Om tot de huidige, definitieve versie te komen is eerst een tussenversie gemaakt met (geanonimiseerde) teksten van aangiftes en toelichtingen van de geselecteerde cases. Deze tussenversie is als een vertrouwelijk stuk behandeld, louter voor intern gebruik. Hieruit zijn de trefwoorden, sleutelwoorden en placeholders uit de LaTeX brontekst gekopieerd met behulp van Notepad++. Vervolgens zijn alle (geanonimiseerde) aangiftes en toelichtingen uit de brontekst verwijderd. De trefwoorden, sleutelwoorden en placeholders zijn daarna weer toegevoegd aan de tekst, in aparte paragrafen. De huidige tekst is vrij van tot personen herleidbare gegevens. [31)]

[31)] Overigens zij benadrukt dat dit tussenrapport geen enkele formele status heeft. Het was slechts een tussenversie om tot het huidige document te komen.

A.8 Markering van trefwoorden, sleutelwoorden en placeholders in het tussenrapport

Per cybermisdrijf waren trefwoorden in de LaTeX brontekst met de aangiftes en toelichtingen aangegeven in het tussenrapport. Dit was gedaan om het geheel overzichtelijk te houden. Het zou een stuk lastiger zijn geweest als de trefwoorden 'cumulatief' zouden zijn bijgehouden. Duplicaties van trefwoorden binnen iedere case waren echter vermeden. Later zijn de trefwoorden voor alle cases verzameld en gededupliceerd. Bij dit proces is verloren gegaan welke trefwoorden bij welke case hoorden en zelfs bij welk type cybercrime ze voorkwamen. De trefwoorden die uit het tussenrapport zijn geëxtraheerd vormen daarmee een middel om cybercrime in het algemeen te typeren.

Wat in dit stuk als trefwoord is aangemerkt zou in de context van (10), dus in die van semantische netwerken, een D-word[32)] worden genoemd. Zij kennen een grote mate van diversiteit ten gevolge van het gebruik van deze woorden in natuurlijke, geschreven taal (door vervoegingen, gebruik van diverse werkwoordsvormen, meervoud/enkelvoud, synoniemen, afkortingen, verschrijvingen, spelfouten, etc.) Indien D-words ontdaan worden van deze (conceptueel niet essentiële) variatie blijven zogenaamde C-words over, waar concepten mee kunnen worden gedefinieerd (combinaties van C-words) en codes (gekarakteriseerd door enkele concepten).

Wat trefwoorden betreft, zijn er twee aspecten te onderscheiden: Het trefwoord als

- object om te herkennen door SNCy, in toelichting of aangifte, wanneer het wordt gebruikt om cases te classificeren.
- kandidaat-taalelement om in SNCy te worden opgenomen, om zijn 'kennis' bij te werken.

Voor de trefwoorden die in het tussenrapport gemarkeerd waren, was dit tweede aspect van belang.

In het tussenrapport waren per case trefwoorden, sleutelwoorden en placeholders gemarkeerd, die karakteristiek zijn voor cybercrime of het type cybercrime en die dus basismateriaal vormen voor een SNCy.

De trefwoorden waren in het tussenrapport van het huidige document herkenbaar als TREFWOORD, dus door een afwijkende kleur, lettertype en lettergrootte. Soms waren placeholders ook als trefwoord aangemerkt, bijvoorbeeld in <ENCRYPTIESOFTWARE>. Dat was alleen het geval als het oorspronkelijke woord (of tekst) beschikbaar was. De placeholder zelf was in de geselecteerde cases nooit een enkelvoudig trefwoord maar kon wel onderdeel zijn van een samengesteld trefwoord. Bij een naam van een placeholder als '<encryptiesoftware>' is nog wel sprake van een trefwoord, maar als de naam van de placeholder '<software>' of '<computerprogramma>' was geweest was de aanduiding te vaag geweest en was er geen sprake geweest van een trefwoord.

Soms kon niet worden volstaan met (losse) woorden maar was het nodig combinaties van woorden te markeren, die als groep een eenheid vormen, en die ook als trefwoord worden

[32)] De 'D' van description, dus woorden die letterlijk in omschrijvingen voorkomen, zoals in het geval van dit document toelichtingen en aangiftes

aangeduid.[33] Omdat meerdere samengestelde trefwoorden direct na elkaar, zelfs in één zin, kunnen voorkomen en duidelijk dient te zijn welke woorden bij elkaar horen en één trefwoord vormen, zijn drie aanduidingen gebruikt om samengestelde trefwoorden te kunnen onderscheiden: zoals in deze woordencombinatie, of zoals in `dit samenstel van woorden`, dan wel zoals in IN DIT GEHEEL VAN WOORDEN. Zo is geen verwarring mogelijk welke woorden één trefwoord vormen, ook als het stuk zwart-wit wordt afgedrukt. Trefwoorden komen meestal binnen één zin voor, maar er zijn uitzonderingen. Voor de duidelijkheid worden direct op elkaar volgende samengestelde trefwoorden onderscheiden.[34]

Sommige trefwoorden zijn bepalend of het om een cybercrime gaat, of om het type cybercrime. Deze sleutelwoorden zijn apart aangegeven: om cybercrime aan te geven als CYBERCRIME of als fraude met computers. Kortom een sleutelwoord voor cybercrime is een trefwoord in een omrande box geplaatst. Indien het sleutelwoorden betreft die een type cybercrime aanduiden is dat aangegeven als een trefwoord dat in een dubbel omrande box geplaatst is, als in PHISHING of in DDoS aanval.

Als in de toelichting of aangifte van een misdrijf de aard van het misdrijf werd genoemd dan is het desbetreffende trefwoord als sleutelwoord gemarkeerd (bijvoorbeeld PHISHING). Als ook nog het trefwoord 'cybercrime' voor kwam dan is dat aangegeven als CYBERCRIME en niet als CYBERCRIME. Immers uit phishing volgt dat het om cybercrime gaat. Als er geen aanduiding van het type cybercrime werd gebruikt in een case, maar wel het woord 'cybercrime' voor komt, dan is dat gemarkeerd als sleutelwoord, dus als CYBERCRIME. Idem voor synoniemen als COMPUTERCRIMINALITEIT.

Een derde type woord dat men tegen komt in de voorbeelden over cybercrime in Paragraaf 7 zijn zogenaamde placeholders. Deze hebben de vorm '<tekst>', waar 'tekst' een aanduiding is van het type informatie waar de placeholder voor in de plaats is gekomen. Voorbeelden van placeholders die men in de voorbeelden tegenkomt zijn <naam>, <adres>, <bedrijf>, ... Oorspronkelijk stonden op de plaats van deze placeholder namen als: 'Jan N. Alleman', 'Prof. Dr. Ir. P. Akkermansstraat 10, Juinen', 'De Letter Zetter',...[35]

Meer over placeholders is te vinden in Bijlage C. We merken hier nog op dat placeholders in principe ook kunnen voorkomen in trefwoorden. Het idee daarbij is dat de naam van de placeholder voldoende informatief is. Bijvoorbeeld als die zou luiden <virusscanner>, maar niet als er zou staan <programma>. Als de oorspronkelijke tekst er zou staan kan die tekst direct identificerend zijn voor een misdrijf, bijvoorbeeld als de naam van een ransomware programma zou worden genoemd of de tekst die zo'n programma op het scherm produceert. Dit zou een mogelijkheid kunnen zijn als andere criteria voor de anonimisering van de politiedata zou worden gekozen dan hier is gebeurd.

[33] In een eerdere versie van dit stuk werden samengestelde trefwoorden (bestaande uit meerdere woorden) onderscheiden van enkelvoudige trefwoorden (bestaande uit één woord). Er was toen sprake van trefwoorden en trefwoordcombinaties. Evenzo van sleutelwoorden en sleutelwoordcombinaties. Dit onderscheid is opgegeven omdat het tot moeizaam taalgebruik leidde. En tot praktische problemen: wat immers te doen als een woord in een tekst ten gevolge van een spelfout als twee woorden was geschreven, zoals 'computer fraude' in plaats van 'computerfraude', of omgekeerd? Tenslotte is in (10) sprake van D-words—equivalenten van trefwoorden—die ook samengesteld kunnen zijn uit meedere woorden. Aangezien het huidige document leunt op (10) ligt het voor de hand dat ook te doen met overeenkomstige begrippen.

[34] Soms komt het voor dat twee samengestelde trefwoorden overlappen. Voor deze situatie schiet de huidige systematiek tekort. In zo'n geval wordt een keuze gemaakt voor een trefwoord.

[35] Uiteraard allemaal fantasienamen.

Om de trefwoorden en sleutelwoorden te markeren in de LaTeX-code zijn een aantal macro's gedefinieerd, waarbij onderscheid is gemaakt tussen enkelvoudige of meervoudige trefwoorden of sleutelwoorden (die laatste kwamen niet voor in de geselecteerde cases). De macro's zorgden ervoor dat de trefwoorden en sleutelwoorden opvielen in de tekst, door hun kleur en/of omkadering (bij sleutelwoorden). De macro's zijn als volgt:

```
% enkelvoudig trefwoord voor cybercrime.
\newcommand{\kw}[1]{{\large{\sc{\color{red}#1}}}}

% enkelvoudig sleutelwoord voor cybercrime.
\newcommand{\kws}[1]{\fbox{{\large{\sc{\color{red}#1}}}}}

% enkelvoudig sleutelwoord voor type cybercrime .
\newcommand{\kwss}[1]{\fbox{\fbox{{\large{\sc{\color{red}#1}}}}}}

% samengestelde trefwoord voor cybercrime variant 1.
\newcommand{\kc}[1]{{\large{\sf{\color{teal}#1}}}}

% samengesteld trefwoord voor cybercrime variant 2.
\newcommand{\kcc}[1]{{\large{\tt{\color{purple}#1}}}}

% samengesteld trefwoord voor cybercrime variant 3.
\newcommand{\kccc}[1]{{\large{\sc{\color{blue}#1}}}}
```

De volgende twee macro's waren ook gedefinieerd, maar bleken voor de geselecteerde cases niet nodig omdat daar samengestelde sleutelwoorden (voor cybercrime in het algemeen of een specifieke vorm daarvan in het bijzonder) niet bleken voor te komen. Het is echter niet gezegd dat ze nooit voorkomen. Om die reden vermelden we ze hier.

```
% samengesteld sleutelwoord voor cybercrime.
\newcommand{\kcs}[1]{\fbox{{\large{\sf{\color{teal}#1}}}}}

% samengesteld sleutelwoord voor type cybercrime.
\newcommand{\kcss}[1]{\fbox{\fbox{{\large{\sf{\color{teal}#1}}}}}}
```

Verschillende varianten voor samengestelde tref- of sleutelwoorden zijn gemaakt omdat er zinnen zijn in aangifte of toelichting waar meerdere van dergelijke samengestelde woorden voorkomen. Dan moet duidelijk zijn welke woorden bij elkaar horen, zoals hierboven is uitgelegd. Maar ook was het prettig om in de tekst een afwisseling van kleuren te zien. Bovendien verhoogde dat de zichtbaarheid van de samengestelde trefwoorden in het tussenrapport.

De placeholders waren gemakkelijk in de LaTeX-tekst te identificeren: het waren de woorden tussen rechte haken, zoals <naam>. Anders dan bij trefwoorden en sleutelwoorden waren placeholders niet speciaal zichtbaar gemaakt in het tussenrapport.

A.9 Extractie van de gemarkeerde woorden uit het tussenrapport

De LaTeX-code met de gemarkeerde trefwoorden, sleutelwoorden en placeholders was een belangrijke tussenversie van het huidige document, het tussenrapport. Het feit dat deze woorden ieder op een bepaalde manier waren gemarkeerd, maakte het relatief eenvoudig ze 'uit te lezen' uit die tussenversie en apart te zetten, per type. Dat is gedaan met behulp van de editor Notepad++.

Met behulp van de macro's die in de vorige subparagraaf zijn opgevoerd was het mogelijk om de trefwoorden en sleutelwoorden op te sporen in de tekst om ze er vervolgens 'uit te halen' en in een apart document te zetten. Bijvoorbeeld enkelvoudige trefwoorden waren te herkennen in het tussenrapport als tekstfragmenten van de vorm `\kw{tekst}`. Ook placeholders waren in het tussenrapport eenvoudig te herkennen als teksfragmenten van de vorm `<tekst>`. In Notepad++ zijn dergelijke tekstfragmenten gemakkelijk op te sporen door gebruik te maken van de regex optie onder 'zoek'. Om de enkelvoudige trefwoorden te vinden typt men in de reguliere espressie `\\kw\{[a-z]+\}`. Bedenk dat het escape symbool \ hier drie keer is gebruikt omdat \, { en } ook (meta)symbolen zijn die in reguliere expressies (regexes) worden gebruikt. Met de optie 'Mark all' konden alle gezochte enkelvoudige keywords worden gevonden en met 'Copy marked text' konden de trefwoorden worden gekopieerd en geplakt in een aparte file en verder worden bewerkt. Net zo met de andere markeringen, hierboven genoemd, inclusief de placeholders.

B Trefwoorden en sleutelwoorden in de geselecteerde cybercrime cases

Om tot de trefwoorden en sleutelwoorden te komen die in deze bijlage te zien zijn is de auteur als volgt te werk gegaan. Nadat hij eerst alle cybercrime cases die voor de analyse waren geselecteerd heeft hij ze eerst geanonimiseerd. Vervolgens heeft hij in de (geanonimiseerde) bronteksten (in LaTeX) de woorden gemarkeerd die volgens hem als trefwoorden zouden kunnen worden aangemerkt, zowel enkelvoudige als meervoudige. Ook heeft hij sleutelwoorden als zodanig gemarkeerd. Daarna heeft hij met behulp van Notepad++ de gemarkeerde woorden uit de LaTeX brontekst gehaald, nabewerkt en hier in tabellen verzameld.

De trefwoorden bestaan enerzijds uit enkelvoudige trefwoorden (het merendeel) en anderzijds uit samengestelde trefwoorden. De enkelvoudige trefwoorden staan in Tabel B.1 (eerste deel) en in Tabel B.2 (tweede deel). De samengestelde trefwoorden staan in Tabel B.3. Verder worden nog sleutelwoorden onderscheiden, die wijzen naar specifieke cybercrimes. Deze zijn in (TabelB.4 samengebracht.

Bij de trefwoorden zou het mogelijk geweest zijn om deze uit te splitsen naar het type cybercrime, op basis van de cases waarbij ze zijn aangetroffen. Dat is hier echter niet gebeurd.[36)] Zoals de trefwoorden hier vermeld staan zijn ze alleen geschikt om cybercrime misdrijven te onderscheiden van andere type misdrijven. Met de sleutelwoorden zou men een verbijzondering kunnen maken naar type cybercrime. Probleem is alleen dat in de huidige brondata sleutelwoorden helaas niet standaard aanwezig zijn.

In het kader van een semantisch netwerk zouden de trefwoorden en sleutelwoorden D-woorden zijn. Merk op dat spellingfouten voorkomen, zoals: ‘edentifier’, ‘phising’ en ‘ransomeware’, ‘ressetten’ in plaats van ‘identifier’, ‘phishing’ en ‘ransomware’, ‘resetten’, respectievelijk) of woorden waarvan de betekenis niet helemaal duidelijk is, maar wel wijst op cybercrime, zoals ‘crypt’.

In Tabellen B.1 en B.2 treft men verder spellingsvarianten aan die tot eenzelfde C-woord zouden leiden, zoals: ‘bankrekeningen’/ ‘bankrekening’; ‘bank’ / ‘huisbank’ / ‘internetbankieren’; ‘bestand’ / ‘bestanden’; ‘betalen’ / ‘betaling’ / ‘betaalknop’; ‘emailberichten’ / ‘email’ / ‘mails’/ ‘mailtje’ / ‘mail’ / ‘nepemail’ / ‘gemaild’; ‘decrypter’ / ‘decryption’; ‘fraude’ /‘fraudeafdeling’ / ‘fraudedesk’ / ‘fraudehelpdesk’; ‘klikken’ / ‘klikte’; ‘ontgrendeld’ / ‘ontgrendeling’; ‘openen’ / ‘opende’; ‘pintransactie’ / ‘pintransacties’; ‘programma’ / ‘programmaatje’ / ‘programmatuur’;‘versleutelde’ / ‘versleuteld’ / ‘versleutelen’/ ‘versleuteling’; ‘toegang’ / ‘toegankelijk’; ‘virusscanner’ / ‘virusscanners’.

In Tabellen B.1 en B.2 treft men ook woorden aan die men in de context van de toepassing als synoniemen kunnen worden behandeld, zoals: ‘besmetting’ / ‘infectie’ / ‘geinfecteerd’; ‘beveiligingssoftware’ / ‘firewall’; ‘computer’ / ‘laptop’; ‘computervredebreuk’ / ‘cybercrime’; ‘malware’ / ‘virus’; ‘gegevens’/ ‘bestanden’; ‘fraude’ / ‘oplichting’; ‘geldautomaat’ /

[36)] De auteur is sceptisch over de mogelijkheid om (alle) soorten cybercrime te onderscheiden op basis van trefwoorden, zoals in de hoofdtekst aangegeven. Herkennen van een cybercrime zou echter wel een optie moeten zijn.

‘geldmachine’; ‘IT’ / ‘ICT’/ ‘ICTer’ /’computerspecialist’; ‘gestort’ / ‘overgeboekt’ / ‘overgemaakt’; ‘ontregeld’ / ‘ontoegankelijk’ / ‘vergendeld’ / ‘versleuteld’.

Dit zijn redelijk uitvoerige lijsten, maar niet noodzakelijkerwijs compleet. De bedoeling was overigens ook niet om complete lijsten te maken.

Uit deze voorbeelden ziet men dat de grens tussen ‘spellingvarianten’ en ‘synoniemen’ niet scherp is. Men zou al deze voorbeelden ook kunnen zien als ‘synoniemen’. In de praktijk ligt deze keuze ook voor de hand.

Men dient zich te realiseren dat zich in aangiftes en toelichtingen meestal meerdere trefwoorden bevinden. Zo’n combinatie van woorden levert de kracht om een case als een cybercrime case te herkennen, of zelfs de aard van dit type misdrijf (bij afwezigheid van een sleutelwoord). In termen van een semantisch netwerk heeft men dan te maken met ‘concepten’. We gaan hier verder niet op in omdat dit aspect niet is uitgewerkt in dit stuk. Het is een onderwerp dat pas in een later stadium aan de orde komt.

aanvragen	advertentie	afpersing
afzender	alarmlijn	antivirusscanner
app	bankgegevens	bank
bankhandelingen	bankomgeving	bankpas
bankpasnummer	bankrekening	bankrekeningen
bankzaken	bedrag	bedreiging
bedrijfsadministratie	bedrijfsgegevens	beeldscherm
benadeeld	besmetting	bestand
bestanden	bestel	besturingssysteem
betaalautomaat	betaald	betaalknop
betalen	betaling	betalingsinstructies
betrouwbaar	betwist	beveiligingssoftware
bijlage	binnendringen	binnengedrongen
boekhoudprogramma	browser	blanco
bureaublad	code	computeraccount
computercriminaliteit	computer	computers
computerspecialist	computervredebreuk	creditcardnummer
crypt	cybercrime	cybercriminelen
ddos	decrypter	decryption
edentifer	email	emailadres
emailberichten	encrypted	fileserver
firewall	fraudeafdeling	fraudedesk
fraude	fraudehelpdesk	geblokkeerd
gecodeerd	gedwongen	gegevens
gegijzeld	gehackt	geinfecteerd
geklikt	geldautomaat	geldmachine
geld	gemaild	geopend
gepind	gestort	gewist
goederen	hack	hacken
hacker	hackers	hardwaretest

Tabel B.1 Enkelvoudige trefwoorden (deel I).

herstellen	huisbank	icter
identiteitsbewijs	identiteitskaart	infectie
internet	internetadres	internetbankieren
internetfraude	it	iter
klikken	klikte	laptop
levering	link	linken
locker	logo	losgeld
mailadres	mailbox	mailprogramma
mail	mails	mailtje
malware	mappen	meegekeken
microsoft	modemhacking	nepemail
netwerk	onbekend	onbruikbaar
onderschept	ontgrendeld	ontgrendelen
ontoegankelijk	ontregeld	ontsleuteld
ontsleutelen	opende	openen
opgelicht	oplichting	opzettelijk
overgeboekt	overgemaakt	pincode
pinpas	pintransactie	pintransacties
programma	programmaatje	programmatuur
rekeningnummer	rekeningoverzicht	reparatie
resseten	rose	scherm
screenprint	server	sleutel
software	stoornis	systeem
tekst	telefoon	telefoonabonnement
telefoonnummer	terugstorten	toegang
toegankelijk	transactie	veiligheidsmaatregelen
verdwenen	vergoeding	vergrendeld
vermogensspaarrekening	vernieling	versleuteld
versleutelde	versleutelen	versleuteling
virus	virusscanner	virusscanners
websites	zipbestand	

Tabel B.2 Enkelvoudige trefwoorden (deel II).

account geblokkeerd	bankpas niet ontvangen
bedrag afgeschreven	bedrag afgeschreven
bestanden ongedaan maken	bestanden verwijderd
betaald scannen	computer geblokkeerd
computer toegang krijgen	drukte webpagina
emailadres verwijderd	gebeld bedreigingen
gmail gehackt	hacker in modem
identiteitsgegevens overschreven	ingelogd in modem
kon niet activeren	liggen stil
link aangeklikt	link aanklikken
link geblokkeerd	microsoft betalen
modem ingebroken	naar priverekening
opende mail	personalia invullen
regels volgen	weggesluisd in seconden

Tabel B.3 Samengestelde trefwoorden.

computercriminaliteit	computervredebreuk
cybercrime	fraude
hacking	oplichting
phishing	phising
ransomeware	ransomware
telecomfraude	verduistering

Tabel B.4 Sleutelwoorden.

C Anonimisering

C.1 Vooraf

Dit onderwerp was geen doel voor dit onderzoek, maar betrof een bijkomend probleem dat moest worden opgelost voordat aan de analyse begonnen kon worden, om herkenning binnen de CBS- organisatie te voorkomen. Dit is een standaard praktijk binnen het CBS. De auteur heeft de geselecteerde cases geanonimiseerd. In deze appendix wordt uitgelegd hoe dit gedaan is.

C.2 Filosofie en werkwijze

Er is voor gekozen om hele specifieke informatie te verwijderen door anonimisering, zoals namen van personen, straten, plaatsen, bedrijven, landen, talen, valuta, typen smartphones, laptops, etc. maar ook aanduidingen van specifieke functies in een bedrijf of van personen die in een bepaalde relatie stonden tot de aangever. Het idee hierbij was om iedere mogelijkheid tot herkenning weg te nemen. Zo zouden enerzijds de cases beveiligd worden tegen herkenning en anderzijds hun bruikbaarheid voor het typeren van het desbetreffende misdrijf niet of nauwelijks aantasten.[37)]

Namen van personen, adressen, plaatsnamen, landennamen, links naar webpagina's, bedragen, tijdsaanduidingen (datums en tijdstippen), etc. zijn allemaal geanonimiseerd, en nog veel meer. Als ergens een naam van een persoon stond is die vervangen door een placeholder <persoon>. Placeholders zijn te herkenen als <tekst>, waarbij de tekst informatie geeft over wat er stond. Zo komen placeholders als <datum>, <bedrijf>, <plaats>, <bank> voor en nog diverse andere.

Soms komen in een aangifte meerdere personen voor. Als die bij naam worden genoemd wordt voor iedere naam <naam> als placeholder gebruikt. Er wordt geen onderscheid gemaakt tussen de verschillende personen. Er werd daarom niet gewerkt met <naam1>, <naam2>, etc. Dat bemoeilijkte het lezen van zo'n geanonimiseerde aangifte echter wel, maar dat is verder niet van belang voor het classificeren van cases.

De informatie die geanonimiseerd is is meestal niet relevant voor het herkennen van het type misdrijf. Dat is echter niet altijd het geval. Het zou bijvoorbeeld kunnen zijn dat een aangever de naam van een virusprogramma noemt. Als die naam niet vervangen zou zijn door een placeholder zou onmiddellijk duidelijk zijn om welk soort cybercrime het gaat. Die informatie kan verloren zijn gegaan door een generieke naam voor dit soort programma's te gebruiken. Dit verlies moet men maar accepteren omwille van de privacy. Daar staat tegenover dat er meestal voldoende trefwoorden overblijven. Sleutelwoorden zijn nooit vervangen door placeholders.

De herkenning van zaken, personen, bedrijven, etc. wordt door het gebruik van placeholders echter aanzienlijk bemoeilijkt, zo niet onmogelijk gemaakt.[38)]

[37)] Wel zijn namen van malware of teksten die malware produceerde op beeldschermen vervangen door placeholders. Maar er bleef voldoende andere informatie over die typering van het misdrijf mogelijk maakte met behulp van de geanonimiseerde data.

[38)] Buitenstaanders kunnen op grond van deze geanonimiseerde omschrijvingen niemand (aantoonbaar) herkennen. Alleen zouden slachtoffers en verbalisanten de geanonimiseerde omschijving 'hun' misdrijf kunnen herkennen. Maar daarmee zou voor hen niets nieuws worden onthuld.

C.3 Idee voor een semantisch netwerk voor anonymisering (SNAn)

Voor het anonimiseren zou men ook gebruik kunnen maken van een semantisch netwerk. We zullen zo'n SN aanduiden als een SNAn. De D-words zijn de woorden die men wil onderdrukken, zoals namen van personen, bedrijven, adressen, plaatsen, fabrieken, banken, instellingen, etc. Bij ieder D-word hoort de naam van een placeholder. Als een dergelijk D-word gevonden wordt in een tekst (aangifte of toelichting) wordt het vervangen door de bijbehorende placeholder. Het verschil met een semantisch netwerk voor cybercrime qua werking is dat het low-level werkt, dat wil zeggen per D-word wordt een label gegenereerd. Het gaat er niet om, zoals bij een semantisch netwerk voor cybercrime om een totaal van labels te gebruiken om te kunnen classificeren.

We geven een aantal voorbeelden van vervanging van gevoelige tekstinformatie door placeholders.[39)][40)]

- Jan N. Alleman → <naam> (of: <persoon>).
- Verlengde Korte Langstraat 5, Tweyfelinge → <adres>. Een optie zou kunnen zijn om eerst af te leiden: <straat> <nummer>,<plaats> en hieruit weer <adres>.
- Bedrijf Zonder Naam BV → <bedrijf>.
- Café De blaffende haring → <horecagelegenheid> (of: <bedrijf>).
- Gribus Volksbank → <bank>.
- 'Als u dit leest hebt u een probleem!' → <schermtekst> (tekst gegenereerd door malware, dat dit virus kan identificeren).
- Koeterwaals → <taal>.
- 9000 ₹ (roepie) → <bedrag> <valuta>.
- NiftyEncrypter → <encryptiesoftware> (of: <virus>; of: <software>).
- 29 februari 2014 → <dag> <maand> <jaar> → <datum> (dat de dag niet bestaat is geen probleem en is zeer waarschijnlijk het gevolg van een typefout of een herinneringsfout).
- Hoofd Bijzaken → <functie>.
- Black Eye Phone → <type smartphone> (of: <device>).

Dit is slechts een beperkte greep uit de gebruikte (of mogelijke) placeholders, bedoeld om het gebruik van placeholders te illustreren. Zie bijlage D voor een lijst met placeholders die voor de geselecteerde cybercrime cases is gemaakt. Overigens is het niet altijd simpel om te beslissen wanneer een placeholder moet worden gebruikt en wanneer niet.

In cases komen vaak namen voor van personen. Die moeten worden vervangen door een placeholder. Het is echter ondoenlijk (en ook onwenselijk) om alle mogelijk voorkomende personen in Nederland in de SNAn op te nemen. Persoonsnamen zouden daarom in teksten softwarematig herkend moeten kunnen worden. Een probleem is dat er ook bedrijven zijn met persoonsnamen. Denk bijvoorbeeld aan Albert Heijn, Dirk van den Broek, Simon Lévelt. En bedrijven moeten als bedrijf worden herkend (en geanonimiseerd) en niet als persoon. Ook kan

39) Het is overigens niet gezegd dat alles wat in dit voorbeeld gesuggereerd wordt ook moet worden opgenomen in een SNAn. Daarvoor moet eerst duidelijk zijn hoe politiedata met betrekking tot aangiftes en toelichtingen geanonimiseerd moeten worden voordat ze kunnen worden gebruikt voor het maken van statistieken over cybercrime.

40) Zie ook (8), dat onafhankelijk van het onderhavige stuk is geschreven. De auteur is gewezen op deze master thesis door Quinten Meertens, naar aanleiding van zijn review van een ver gevorderd concept van het onderhavige document. De auteur heeft derhalve geen gebruik kunnen maken van de inzichten en bevindingen in deze scriptie. De geïnteresseerde lezer heeft die mogelijkheid wel.

er best een persoon zijn die Albert Heijn heet, maar die niets met de winkel AH van doen heeft. Die moet dan als persoon herkend worden.

In principe zou de SNAn toegang moeten hebben tot een lijst met adressen in Nederland, die bestonden in een bepaalde periode (waar ook de politiedata 'in vallen').[41)] Men zou ook aparte lijsten kunnen maken van in Nederland voorkomende straatnamen en plaatsen. De koppeling tussen die twee hoeft niet te bestaan. Namen als 'Dorpstraat' en Kerkstraat' komen echter in veel plaatsen voor. Door de straatnaam-plaats te ontkoppelen kan ontdubbelen van straatnamen plaatsvinden en ook van plaatsen (bijvoorbeeld namen als 'Katwijk' en 'Bergen' komen in Nederland meer dan één keer voor). Ook lijsten van horecagelegenheden zijn vermoedelijk wel te maken, en van bedrijven, maar hoeveel werk is dat? Hoe compleet zijn ze? Van banken in Nederland is vrij simpel een lijst te maken, evenals van teksten die bekende ransomware virussen op het scherm schijven, evenals de namen van bekende virussen. Het aantal talen waar men in de aangiftes me te nmaken heeft zal niet van de orde van alle talen in de wereld zijn, maar een beperkt aantal. Zo'n lijst is gemakkelijk te maken. Zulke lijsten zijn ook wel te maken voor bestaande smartphone merken. Om per merk ook nog de voorkomende typen vast te leggen is wat meer werk. Een lijst voor bestaande functies hoeft misschien niet zo heel lang te zijn, omdat de aangever, voorzover hij met een bedrijf te maken heeft, maar een beperkt aantal functies heeft. Men zal niet een schoonmaker van het bedrijf naar de politie sturen om een cybercrime bij dat bedrijf te melden.

Tot slot van deze bijlage nog enkele opmerkingen.

Opmerking Ook de op de collectie placeholders kan men semantische relaties definiëren. Zo zijn een <bank>, een <horecagelegenheid> en een <telecombedrijf> allemaal speciale gevallen (hyponiemen) van <bedrijf> (hyperoniem). Het zou kunnen zijn dat de verwijzing naar een persoon (aangeduid met een naam in een tekst) de ene keer wordt vervangen door de placeholder <naam> en de andere keer door,zeg, <persoon>. Dan is er feitelijk sprake van synonymie. Een <functie> kan men beschouwen als een deel (meroniem) van <bedrijf> (holoniem), dat in de regel uit werknemers bestaat die ieder een bepaalde functie vervullen. □

Opmerking Bij het gebruik van een SNAn is men gedwongen bij te houden welke placeholders in gebruik zijn. Dit voorkomt wildgroei. Ook moeten niet te veel placeholders worden geïntroduceerd die synoniem zijn van een bepaalde placeholder, zodat het overzicht niet verloren gaat. □

Opmerking De keuze van de naam van een placeholder is niet altijd simpel. De vraag is de mate van detail die in de naam naar voren komt. Stel in een aangifte wordt de naam van een virus genoemd. Stel (zoals in dit stuk) dat te identificerend voor de case wordt geacht. Men kan de naam vervangen door <software> of <programma>. Dat is aan de veilige kant. Maar misschien ook wel te veilig. Informatiever is <virus>, <virus software>, <malware> of, indien van toepassing <ransomware>. Dat zou de classificatie van het desbetreffende misdrijf kunnen vereenvoudigen. □

[41)] Zie (5) waar deze suggestie wordt onderzocht. Deze master thesis is onafhankelijk van het onderhavige stuk tot stand gekomen. Deze scriptie is onder de aandacht van de auteur dezes gebracht door Quinten Meertens, bij het reviewen van een vergevorderd concept van het onderhavige stuk. De auteur heeft derhalve geen gebruik kunnen maken van deze scriptie. De geïnteresseerde lezer heeft die mogelijkheid echter wel.

Opmerking Wederom inspireerde mij (7) tot een idee voor het classifceren van cybercrime. Op pagina 5 staat de vraag: '*To what degree can we have both data privacy and the benefit of data mining?*' Toen ik dit las realiseerde ik me dat een SNcy in principe toegepast kan worden op de niet beveiligde data. Dat wil zeggen de volautomatische stap. Immers geen CBS-er hoeft deze data te zien als deze stap wordt uitgevoerd. En dat de data meer detail hebben dan de meeste trefwoorden is een (waarschijnlijk) ondergeschikt probleem. Het is de interactieve stap waarbij onthullingsgevaar dreigt. Immers dan krijgen de classificatie-experts de data onder ogen. Dat zou impliceren dat alleen deze data geanonimiseerd zouden moeten worden. Ook in het geval experts cases willen inspecteren op mogelijk nieuwe trefwoorden en sleutelwoorden zouden die cases eveneens eerst geanonimiseerd moeten worden, voor zover dat niet al gebeurd is voor de interactieve classificatie van cases die niet volautomatisch geclassificeerd konden worden. Als inderdaad de meerderheid van de cases volautomatisch kan worden geclassificeerd impliceert dat dat, strict genomen, slechts een relatief klein deel van de data geanonimiseerd zou hoeven te worden, namelijk dat deel dat interactief moet worden geclassificeerd. Maar of het handig is om dat te doen voor inspectie is de vraag. □

D Placeholders in de geselecteerde cybercrime cases

Voorafgaand aan het analyseren van de aangiftes heeft de auteur eerst de geselecteerde aangiftes geanonimiseerd, omdat de oorspronkelijke politiedata privacy-gevoelig zijn. Deze bijlage biedt een overzicht van de placeholders die de auteur heeft gebruikt bij het anonimiseren van de geselecteerde cases. De keuze is bepaald door het feit dat de auteur een extreme mate van anonimisering heeft toegepast, waarbij getracht is alle informatie die gebruikt zou kunnen worden om personen te herkennen, direct of indirect, weg te halen. Hiermee is niet gezegd dat deze beveiligingsstrategie zonder meer zou moeten worden overgenomen, inclusief de hieruit voortvloeiende placeholders, voor soortgelijke exercities (bij onderzoek en productie). De lijst met placeholders pretendeert niet volledig te zijn; ze is immers slechts gebaseerd op een beperkt aantal cybercrime cases. Ze is vooral bedoeld als inspiratiebron.

In het hieronder gegeven overzicht worden alleen de placeholders genoemd, niet de waarden die ze vervangen. Ze worden ook niet per aangifte genoemd maar voor alle aangiftes met betrekking tot cybercrime. De meeste placeholders spreken voor zich. In de context van de cases waar ze gebruikt zijn, is hun betekenis eenvoudiger te begrijpen.

De placeholders zijn met behulp van Notepad++ uit het tussenrapport (in LaTeX) 'gehaald', waar al deze woorden in waren gemarkeerd. Zie Tabel D.1.

<aantal>	<accent>	<activiteit>	<adres>
<advertentienummer>	<advertentietekst>	<afdeling>	<app>
<bank>	<bankinfo>	<bankpasnummer>	<bankrekeningnummer>
<bedrag>	<bedrijf>	<bedrijfsactiviteit>	<bedrijfstype>
<bericht>	<bestandsnaam>	<bestandstype>	<betaalfaciliteit>
<betaalsite>	<betaalsysteem>	<blad>	<branche>
<brief>	<code>	<communicatiemedium>	<computerprogramma>
<contact>	<datum>	<device>	<emailadres>
<encryptiesoftware>	<feest>	<filetekst>	<fraudeurs>
<functie>	<geboortedatum>	<geldautomaat>	<gemeente>
<gokken>	<instelling>	<instellingstype>	<internetprovider>
<internetwinkel>	<jaar>	<kalmeringsmiddel>	<kenmerk>
<kwalificatie>	<land>	<landcode>	<leeftijd>
<locatie>	<maand>	<mededeling>	<melding>
<merk>	<middelen>	<naam>	<nummer>
<omschrijving>	<opdracht>	<pasnummer>	<percentage>
<periode>	<personalia>	<personeelslid>	<persoon>
<plaats>	<postbedrijf>	<product>	<provider>
<rekeningnummer>	<reserveringsnummer>	<slaapmiddel>	<software>
<specificatie>	<stichting>	<straat>	<systeem>
<taal>	<tekst>	<telecombedrijf>	<telefoonmerk>
<telefoonnummer>	<telefoonprovider>	<tijd>	<tool>
<type>	<valuta>	<virusscanner>	<voucher>
<wachtwoord>	<webbrowser>	<weblink>	<website>
<weekdag>	<werkplek>	<werkruimte>	<winkel>
<zoekmachine>			

Tabel D.1 Placeholders gebruikt in het geanonimiseerde bronmateriaal dat gebruikt is voor de analyse.

E Kernbegrippen

Begrippen die voor dit stuk van belang zijn worden hier toegelicht. Regelmatig is Wikipedia gebruikt hierbij, vanwege de gemakkelijke toegankelijkheid. Verklaringen zijn soms in het Engels, omdat ze zijn ontleend aan de Engelstalige versie van Wikipedia. De verklaringen uit Wikipedia zijn niet altijd volledig of letterlijk overgenomen, maar indien nodig aangepast aan de behoeften in dit stuk. Bronnen zijn steeds vermeld.

Aangifte 1. Een formele procedure bij de politie om een misdrijf te melden, ook wel aangeduid als 'proces-verbaal'. 'Aangifte' is hier dus op te vatten als synoniem van 'proces verbaal'. 2. Het relaas van een aangever over misdrijf dat hem is overkomen. Hier is 'aangifte' een onderdeel van een proces-verbaal

Computervredebreuk Ongeoorloofd toegang verschaffen tot een computersysteem.

C-words In een semantisch netwerk zijn dit de woorden waar formele concepten dat het SN gebruikt om categorieën te omschrijven. Het SN heft als doel om teksten te linken aan één van deze categorieën op basis van D-words die als trefwoorden in teksten voorkomen. Het begrip speelt een centrale rol in (10).

Cybercrime Criminaliteit met ICT als middel en doelwit.

DDoS aanval DDoS = Distributed Denial of Service. [Zie: website aanval]

D-words In een Semantisch Netwerk zijn dat de trefwoorden die in teksten voorkomen en die karakteristiek zijn voor de categorieën die gebruikt worden om teksten te labellen. Deze kunnen een groot aantal vormen hebben, die echte qua betekenis hetzelfde zijn. Equivalentieklassen van dit soort woorden zijn C-words. Het begrip speelt een centrale rol in (10).

Enkelvoudig sleutelwoord [Zie: Sleutelwoord]

Enkelvoudig trefwoord [Zie: Trefwoord]

Fraude met behulp van computers Valsheid in geschrifte met betrekking tot computerdata.

Gedigitaliseerde criminaliteit Gedigitaliseerde criminaliteit bestaat uit strafbare feiten waarbij gebruik wordt gemaakt van een ICT middel. Cybercrime daarentegen omvat strafbare feiten die worden gepleegd via een ICT middel én die gericht zijn op een ICT middel. Bij gedigitaliseerde criminaliteit kan men denken aan het gebruik van sociale media als ontmoetingsplaats, het darkweb als handelsplaats en het gebruik van bitcoins voor witwassen. In de praktijk is het onderscheid tussen cybercrime en gedigitaliseerde criminaliteit niet zo strikt.

Hacking Ongeoorloofd computerdata verwijderen of aanpassen.

Helpdeskfraude zich voordoen als een medewerker van de helpdesk van een softwarebedrijf (vaak Microsoft) en zo toegang krijgen tot een computer van iemand en zijn/haar bankgegevens.

Holoniem [Zie: Meroniem]

Homoniem Twee woorden zijn elkaars homoniemen als ze op dezelfde manier worden uitgesproken en geschreven, maar verschillende betekenissen hebben. Voorbeelden van dergelijke woordparen in het Nederlands zijn 'bank', dat zowel zitmeubel als geldinstelling kan betekenen, en 'schop', dat zowel schep als trap met de voet kan betekenen. De beide betekenissen van bank zijn overigens van dezelfde oorsprong, maar schop als schep komt van scheppen, en als trap met de voet van schuiven. [Bron: https://nl.wikipedia.org/wiki/Homoniem] We zijn in dit stuk niet erg geïnteresseeerd in woorden die dezelfde klank hebben maar met verschillende betekenissen [bijvoorbeeld plee/play, card/cart, ree/ray, pas/pass] maar vooral in geschreven homoniemen, zoals bank

(geldinstelling, zitmeubel, grondbank, Doggersbank, etc), pas (pinpas, paspoort, toegangspas, doorgang in bergen, etc), hoofd (functie, lichaamsdeel, etc.), beurs (veiling, tentoonstelling, portemonnee). Vergelijk met Synoniem. [zie aldaar]

Hyperoniem [Zie: Hyponiem]

Hyponiem Een begrip A is een hyponiem van een begrip B als de betekenis van A volledig wordt gedekt door B met een doorgaans ruimere betekenis. Het begrip B is een hyperoniem van A. [bron: https://nl.wikipedia.org/wiki/Hyponiem]

ICT Informatie- en communicatietechnologie.

Identiteitsfraude Via list en bedrog, of gestolen, identiteitsgegevens van een persoon gebruiken voor oplichting van andere slachtoffers, om zo buiten beeld te blijven.

Machine Learning The study of computer algorithms that improve automatically through experience and by the use of data. It is seen as a part of artificial intelligence. Machine learning algorithms build a model based on sample data, known as 'training data', in order to make predictions or decisions without being explicitly programmed to do so. [bron: https://en.wikipedia.org/wiki/Machine_learning]

Malware Elke software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen. Het woord is een samentrekking van het Engelse malicious software (kwaadaardige software, soms schadelijke software). Malware veronderstelt kwade opzet. Software waarmee geen kwaad wordt beoogd, valt hier dus niet onder.[bron: https://nl.wikipedia.org/wiki/Malware]

Melder Iemand die als slachtoffer van een misdrijf, daarvan melding maakt bij de politie, die als gevolg daarvan een proces-verbaal opmaakt. Ook aangeduid als AAB, AAN of AG (afkortng voor 'aangever' of 'aanbrenger').

Meroniem Het woord dat het 'deel' benoemt, noemt men een meroniem van het 'geheel'. 'Klink' is hier dus een meroniem van 'deur'. De omgekeerde relatie 'geheel-deel' is holonymie. Het woord dat het geheel benoemt ('deur') is dan een holoniem van het deel ('klink'). [Bron: https://nl.wikipedia.org/wiki/Meronymie]

MLA = Machine Learning Application.

Microsoft support scam [Zie: Helpdeskfraude]

ML = Machine Learning [Zie aldaar]

Ontologie Het product van een poging een uitputtend en strikt conceptueel schema te formuleren over een bepaald domein. Een ontologie is typisch een datastructuur die alle relevante entiteiten en hun onderlinge relaties en regels binnen dat domein bevat, zoals bij een domeinontologie het geval is. Op het terrein van de kunstmatige intelligentie wordt het begrip ontologie gebruikt als aanduiding voor een door computers interpreteerbare beschrijving van de werkelijkheid (kennisrepresentatie). [bron: https://nl.wikipedia.org/wiki/Ontologie_(informatica)]

Ontology learning The automatic or semi-automatic creation of ontologies, including extracting the corresponding domain's terms and the relationships between the concepts that these terms represent from a corpus of natural language text, and encoding them with an ontology language for easy retrieval. As building ontologies manually is extremely labor-intensive and time-consuming, there is great motivation to automate the process.[bron: https://en.wikipedia.org/wiki/Ontology_learning] Ook aangeduid als: ontology extraction, ontology generation, ontology acquisition.

Phishing Methode waarbij via misleiding persoonlijke gegevens worden ontfutseld bij, of stiekem gekopieerd van, iemand, bijvoorbeeld inloggegevens voor bankaccount, met de bedoeling hier geld van te stelen.

Placeholder Een algemene aanduiding die een tekstfragment vervangt om het identificatierisico

te verkleinen. Heel algemeen zou men één placeholder kunnen gebruiken om al deze cases af te dekken, en die <missing> te noemen. Daarmee wordt echter de begrijpelijkheid van een tekst verstoord. Om die reden zijn er meer specifieke placeholders gebruikt die aangeven wat voor soort informatie ze afdekken. Zo worden gebruikt <naam>, <adres>, <plaats>, <bedrijf>, etc. Placeholders zijn van de vorm '<tekst>'.

Proces-verbaal Een schriftelijke weergave waarin iemand (vaak een ambtenaar) verslag uitbrengt van in zijn of haar aanwezigheid geconstateerde feiten en omstandigheden, zijn of haar verrichtingen en de persoonsgegevens van betrokkenen en getuigen. Een proces-verbaal is daarmee een bewijs van wat die persoon heeft gezien en geconstateerd. In een proces-verbaal worden zowel aangiftes van overtredingen als overtredingen vastgesteld en eventueel de naam van een verdachte en diens verklaring. Bij aangifte is er een verklaring van het slachtoffer. [bron: `https://nl.wikipedia.org/wiki/Proces-verbaal`]

Ransomware Malware die een computer en/of gegevens die erop staan blokkeert en vervolgens van de gebruiker geld vraagt om de computer weer te 'bevrijden' middels een tegen betaling verstrekte code. Betalen blijkt echter niet (altijd) tot ontsluiting van de besmet geraakte computer te leiden, zo waarschuwt de Nederlandse overheid. En zelfs wanneer na betaling de code succesvol wordt gebruikt blijft de software op de computer staan en kan deze enkele maanden later opnieuw het systeem blokkeren en om nog meer geld vragen. [bron: `https://nl.wikipedia.org/wiki/Ransomware`]

Samengesteld sleutelwoord [Zie: Sleutelwoord]

Samengesteld trefwoord [Zie: Trefwoord]

Semantisch netwerk Een netwerk dat semantische relaties tussen begrippen weergeeft. Dit wordt vaak gebruikt als een vorm van kennisweergave. Het netwerk kan een gerichte of een simpele graaf zijn. De graaf bestaat uit knopen, die de begrippen voorstellen, en zijden [die semantische relaties tussen de begrippen symbaliseren]. [bron: `https://nl.wikipedia.org/wiki/Semantisch_netwerk`]

Semantische relatie Een relatie van het type hyponymie/hyperonymie, meronomie/holonymie, synonymie, etc. Het is dus en relatie die gebaseerd is op de betekenis van begrippen. Door dit soort relaties te definiëren op de D- en C-woorden definieert men een semantisch netwerk. [Zie: Semantisch Netwerk]

Sleutelwoord Een trefwoord dat aanduidt dat een misdrijf een cybercrime betreft, en dat eventueel specificeert welk type cybercrime. Een sleutelwoord kan uit één woord bestaan (enkelvoudig sleutelwoord) of uit meerdere woorden (samengesteld sleutelwoord).[42)]

SN = Semantisch Netwerk. [Zie aldaar]

SNAn een Semantisch Netwerk om de politiedata met betrekking tot aangiftes van slachtoffers te anonimiseren.

SNCy een semantisch netwerk voor cybercrime.

Supervised learning Is the machine learning task of learning a function that maps an input to an output based on example input-output pairs. It infers a function from labeled training data consisting of a set of training examples. In supervised learning, each example is a pair consisting of an input object (typically a vector) and a desired output value (also called the supervisory signal). A supervised learning algorithm analyzes the training data and produces an inferred function, which can be used for mapping new examples. An optimal scenario will allow for the algorithm to correctly determine the class labels for unseen instances. [bron:

[42)] Omdat het in dit stuk alleen over cybercrime gaat is met sleutelwoord impliciet begrepen dat het om cybercrime gaat. Maar dezelfde aanpak die hier bepleit wordt voor cybercrime zou voor andere misdrijven ook kunnen worden gebruikt. Om misverstanden te voorkomen zou men een prefix kunnen gebruiken dat aangeeft om welk soort misdrijf het gaat, bijvoorbeeld 'cy' voor çybercrime, en 'cyt' voor type cybercrime, etc. We zouden dan moeten spreken over cy-sleutelwoord, of cyt-sleutelwoord, etc. Maar dat is in dit stuk overbodig.

https://en.wikipedia.org/wiki/Supervised_learning]

Synoniem Een synoniem of evenwoord van een bepaald woord in een taal is een ander woord in dezelfde taal met min of meer dezelfde betekenis. Dit verschijnsel wordt synonymie genoemd. [bron: https://nl.wikipedia.org/wiki/Synoniem_(taalkunde)] In de context van dit stuk heeft het begrip een ruimere betekenis. Zo worden afkortingen of veel voorkomende verschrijvingen van een woord (bijvoorbeeld 'ransomeware' in plaats van 'ransomware') ook als synomiemen beschouwd. Of enkelvoud en meervoud van een zelfstandig naamwoord, of verschillende vervoegingen van een werkwoord.

Technical support scam [Zie: helpdeskfraude]

Toelichting Een aanvulling op een aangifte waarbij de verbalisant extra informatie geeft over het misdrijf in kwestie. Dat is vaak een interpretatie van het misdrijf. Of het betreft opmerkingen over vervolgacties van de politie. Of opmerkingen over soortgelijke misdrijven. Of het vermeldt door de aangever geleverd bewijsmateriaal, etc.

Training set In machine learning, a common task is the study and construction of algorithms that can learn from and make predictions on data. Such algorithms function by making data-driven predictions or decisions, through building a mathematical model from input data. [bron: https://en.wikipedia.org/wiki/Training,_validation,_and_test_sets]

Trefwoord In dit stuk: kenmerk dat cybercrime, of een bepaald type cybercrime, karakteriseren. Een trefwoord kan uit één woord bestaan (enkelvoudig trefwoord) of uit meerdere woorden (samengesteld trefwoord).[43)]

Unsupervised learning A type of algorithm that learns patterns from untagged data. The hope is that through mimicry, the machine is forced to build a compact internal representation of its world and then generate imaginative content. [Bron: https://en.wikipedia.org/wiki/Unsupervised_learning]

Verbalisant Een opsporingsambtenaar die een proces-verbaal opmaakt. Dit is meestal een politieambtenaar maar het kan ook een Buitengewoon opsporingsambtenaar (Boa) betreffen.

Website aanval Door een spervuur van e-mailtjes een computersysteem uitschakelen of onbruikbaar maken. Hiervoor wordt vaak een botnet gebruikt. Hier kan ook mee worden gedreigd en is dan een vorm van afpersing.

[43)] Omdat het in dit stuk alleen over cybercrime gaat is met trefwoord impliciet begrepen dat het om cybercrime gaat. Maar dezelfde aanpak die hier gekozen is voor cybercrime kan in principe ook voor andere misdrijven worden gebruikt. Om misverstanden te voorkomen zou men een prefix kunnen gebruiken dat aangeeft om welk soort misdrijf het gaat, bijvoorbeeld 'cy' voor çybercrime, en 'cyt' voor type cybercrime, etc. We zouden dan moeten spreken over cy-trefwoord, of cyt-trefwoord, etc. Maar dat is ditstuk niet nodig.

Colophon

Publisher
Statistics Netherlands
Henri Faasdreef 312, 2492 JP The Hague
www.cbs.nl

Prepress
Statistics Netherlands, Grafimedia

Design
Edenspiekermann

Information
Telephone +31 88 570 70 70, fax +31 70 337 59 94
Via contact form: www.cbs.nl/information