FOX IT
part of nccgroup

CLASSIFICATIE
COMMERCIAL RESTRICTED
MINBZ

Onderzoek Forrest City

Rapportage

Onderwerp	Technische ondersteuning bij het redigeren van een Wob-publicatie
Datum	13 november 2019
Referentie	PR-190091
Opdrachtgever	Ministerie van Buitenlandse Zaken
Auteur(s)	[redacted]
Versie	1.0
Status	Definitief
Pagina's	21

FOR A MORE SECURE SOCIETY

DOCUMENTCLASSIFICATIE

Dit document is geclassificeerd als COMMERCIAL.RESTRICTED.MINBZ. De informatie die in dit document en bijbehorende bijlagen gepubliceerd is, is alleen bedoeld voor de geadresseerde(n). Het gebruik van het document door een andere partij dan de geadresseerde(n) is niet toegestaan, tenzij deze partij hiertoe expliciet geautoriseerd is door een geadresseerde. De informatie in dit document is COMMERCIAL.RESTRICTED.MINBZ. van aard en valt onder de bepalingen van een geheimhoudingsverklaring of -plicht.

Indien u het voorliggende document foutief heeft ontvangen en/of geen toestemming heeft tot inzage van het document, verzoekt Fox-IT u om het document direct te sluiten en te retourneren aan Fox-IT.

Enig misbruik van dit document of de informatie in het document is niet toegestaan. Fox-IT aanvaardt geen aansprakelijkheid voor enig ongeautoriseerd gebruik of misbruik van voorliggend document door een derde partij of schade ontstaan door de inhoud van het document.

Fox-IT B.V.
Olof Palmestraat 6
2616 LM Delft
Postbus 638
2600 AP Delft
Nederland

T +31 (0)15 284 79 99
F +31 (0)15 284 79 90
fox@fox-it.com
www.fox-it.com

Copyright © 2019 Fox-IT B.V.
Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enigerlei wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of op enige andere manier, zonder voorafgaande schriftelijke toestemming van Fox-IT B.V.

Handelsmerk
Fox-IT en het logo van Fox-IT zijn handelsmerken van Fox-IT B.V.
Alle andere in dit document opgenomen handelsmerken zijn eigendom van de genoemde organisaties.

Managementsamenvatting

Het ministerie van Buitenlandse Zaken (hierna: Opdrachtgever) heeft het afgelopen jaar twee officiële publicaties gedaan op grond van de Wet openbaarheid van bestuur (hierna: Wob) over steun aan gewapende groepen in Syrië. Het betreft een Wob-publicatie in november 2018 en een Wob-publicatie in juni 2019, o.a. over het Nederlandse non-lethal assistence (NLA)-programma. Fox-IT is gevraagd technisch advies te geven ten behoeve van de herbeoordeling van de NLA-Wob-publicatie door Opdrachtgever. Ten behoeve van de herbeoordeling is door Opdrachtgever een (beoordelings)team samengesteld bestaande uit medewerkers van Opdrachtgever en Pels Rijcken (landsadvocaat) voor de juridische kwalificatie en beoordeling en Fox-IT voor de technische ondersteuning.

Aan het begin van het project heeft Fox-IT, samen met de rest van het beoordelingsteam, diverse herleidbaarheidsrisico's geïdentificeerd in de Wob-publicatie van juni 2019. Deze risico's zijn door Fox-IT verder onderbouwd met behulp van OSINT-onderzoeken. De geïdentificeerde risico's hebben geleid tot diverse aanbevelingen van Fox-IT om zodoende de herleidbaarheidsrisico's te kunnen mitigeren. De aanbevelingen die Fox-IT heeft gedaan op basis van de geïdentificeerde risico's zijn als volgt samen te vatten:

4.1 Afbeeldingen in het geheel lakken.
4.2 Namen, logo's en andere identificerende vernoemingen lakken.
4.3 Gerelateerde organisaties en groepen afschermen. Onder afschermen wordt, naast lakken, ook verstaan dat gezorgd wordt dat informatie niet herleidbaar is naar deze groepen en organisaties.
4.4 Tijdsbepalingen en locatiebepalingen lakken.
4.5 Onderscheidende beschrijvingen van gebeurtenissen lakken.

Bovenstaande aanbevelingen zijn door de juristen binnen het beoordelingsteam in overweging genomen en gebruikt voor het opstellen van een reeks beoordelingslijnen. Aan de hand van deze beoordelingslijnen heeft Opdrachtgever de NLA-documenten uit de Wob-publicatie juni 2019 nogmaals beoordeeld.

Het is van belang te vermelden dat de resultaten uit de OSINT-onderzoeken voortkomen uit een afgekaderde opdracht, alsmede een momentopname zijn. Gezien de afkadering in de tijd is er door Opdrachtgever voor gekozen onderzoek te doen naar een beperkte selectie van teksten en afbeeldingen in de NLA-documenten. Niet elke in potentie risicovolle tekst of afbeelding kon uiteindelijk door Fox-IT onderzocht worden of binnen de gestelde tijd herleid worden naar vertrouwelijke informatie. Dit neemt echter niet weg dat het risico op herleidbaarheid wel van toepassing is op dergelijke tekst of afbeelding, aangezien een andere onderzoeker met meer tijd, middelen, bronnen of op een ander moment de informatie mogelijk wel kan herleiden.

Naast de handmatige bestudering van de NLA-documenten is besloten een aanvullende specifieke controle te doen op aanwezigheid van vertrouwelijke namen. Dit is gedaan door de NLA-documenten van juni 2019 doorzoekbaar te maken en vervolgens te doorzoeken op steekwoorden. De steekwoorden zijn afgeleid van de vertrouwelijke namen van groepen en organisaties. Dit heeft geresulteerd in één geïdentificeerde vertrouwelijke naam, die vervolgens door het beoordelingsteam is aangemerkt om te lakken.
Het steekwoordenonderzoek is beperkt door de kwaliteit van de ingescande documenten en alle mogelijke variaties op de groepsnamen die waarschijnlijk niet gedekt zijn door de steekwoorden.

Tenslotte, heeft Fox-IT, met het oog op herleidbaarheid, op de door Opdrachtgever herbeoordeelde documenten een laatste analyse uitgevoerd. Uit deze analyse volgden enkele ongelakte teksten die door Fox-IT als risicovol zijn aangemerkt. De desbetreffende risicovolle teksten bleken allemaal gerelateerd te zijn aan de eerder geïdentificeerde risico's zoals beschreven in hoofdstuk 4 van dit rapport. Het betrof hier voornamelijk datums, tijden, locaties en beschrijvingen van gebeurtenissen die in de context een indirect herleidbaarheidsrisico opleverden.

Opdrachtgever heeft de risicovolle teksten in overweging genomen en, met inachtneming van de Wob-uitzonderingsgronden, op een aantal van deze teksten additionele lakhandelingen verricht.
Daarnaast heeft Opdrachtgever geoordeeld dat de risicovolle teksten geen aanleiding gaven tot het aanpassen van de reeds toegepaste beoordelingslijnen.

Inhoudsopgave

1	**Inleiding**	**6**
1.1	Situatieschets	6
1.2	Doelstellingen	6
1.3	Leeswijzer	7
2	**Opzet en werkwijze**	**8**
2.1	Het beoordelingsproces	8
2.2	IT-omgeving	9
2.3	Herleidbaarheid	9
2.3.1	Bronnen	10
2.3.2	Voorbeelden van herleidbaarheid	10
2.4	OSINT-onderzoek	11
2.4.1	Beperkingen van het OSINT-onderzoek	11
2.5	Documenten doorzoeken op steekwoorden	12
2.5.1	Beperkingen van het steekwoordenonderzoek	12
3	**Bevindingen**	**14**
3.1	OSINT-onderzoek	14
3.2	Steekwoordenonderzoek	14
4	**Risico's en aanbevelingen**	**15**
4.1	Afbeeldingen	15
4.2	Namen, logo's en andere identificerende vernoemingen	15
4.3	Gerelateerde organisaties en groepen	16
4.4	Tijds- en locatiebepalingen van gebeurtenissen	16
4.5	Onderscheidende beschrijvingen van gebeurtenissen	17
4.6	NLA-documenten op archiefweb.eu	18
Appendix A		**19**
A.1	Verklarende woordenlijst	19
Appendix B Resultaten uit onderzoek		**20**

1 Inleiding

Van 18 september 2019 tot 1 november 2019 heeft Fox-IT in opdracht van het ministerie van Buitenlandse Zaken het project Forrest City uitgevoerd. Dit document dient als eindrapportage voor dat project.

1.1 Situatieschets

Op 18 juli 2019 heeft een gesprek plaatsgevonden tussen het ministerie van Buitenlandse Zaken (hierna te noemen: Opdrachtgever) en Fox-IT B.V. (hierna te noemen: Fox-IT).

Tijdens dit gesprek heeft Opdrachtgever de volgende situatie geschetst:
Opdrachtgever heeft het afgelopen jaar twee officiële publicaties gedaan op grond van de Wet openbaarheid van bestuur (hierna: Wob) over steun aan gewapende groepen in Syrië. Het betreft een Wob-publicatie in november 2018 en een Wob-publicatie in juni 2019, o.a. over het Nederlandse non-lethal assistence (NLA)-programma.

In beide publicaties stond informatie die niet was weggelakt die wel weggelakt had moeten worden alvorens over te gaan tot publicatie, waaronder staatsgeheime en vertrouwelijke informatie. Beide publicaties zijn van www.rijksoverheid.nl verwijderd.

De volgende informatie dient beschermd te worden bij de Wob-publicatie:
- De namen en locaties van de gewapende groepen gesteund tijdens het NLA-programma evenals alle tot hen herleidbare informatie. Deze informatie is gerubriceerd als Staatsgeheim GEHEIM (Stg. G.).
- De namen van de uitvoerders wiens diensten gebruikt zijn om de groepen van goederen te voorzien. Deze informatie is gerubriceerd als Departementaal VERTROUWELIJK (Dep. V.).

Fox-IT is gevraagd technisch advies te geven ten behoeve van de herbeoordeling van de NLA-Wob-publicatie door Opdrachtgever. Ten behoeve van de herbeoordeling is door Opdrachtgever een (beoordelings)team samengesteld bestaande uit medewerkers van Opdrachtgever en Pels Rijcken (landsadvocaat) voor de juridische kwalificatie en beoordeling en Fox-IT voor de technische ondersteuning.

1.2 Doelstellingen

Opdrachtgever vraagt Fox-IT technisch advies te geven ten behoeve van de tweede herpublicatie van de betreffende documenten. Voor de tweede herpublicatie zijn door de Opdrachtgever de volgende doelen gesteld:
1. Beoordeling van- en extern advies op de herpublicatie van documenten die in juni 2019 heeft plaatsgevonden. Naar aanleiding van het extern advies, zal door het ministerie een tweede herpublicatie van documenten plaatsvinden op www.rijksoverheid.nl.
2. Startpunt voor de beoordeling is de geredigeerde versie van documenten die in juni 2019 is gepubliceerd. Die documenten dienen opnieuw beoordeeld te worden om te bezien waar informatie niet is weggelakt die wel weggelakt had moeten worden.

3. Het extern advies op de tweede herpublicatie dient nadrukkelijk betrekking te hebben op de volgende informatie:
    a. namen van Syrische groepen;
    b. logo's en vlaggen van Syrische groepen;
    c. informatie op basis waarvan valt te herleiden welke Syrische groepen steun kregen;
    d. beeldmateriaal/foto's op basis waarvan informatie over Syrische groepen te herleiden is;
    e. namen van bedrijven die de Nederlandse steun hebben uitgevoerd;
    f. inconsequenties in het weglakken van informatie;
    g. andere dan de hierboven genoemde punten die tijdens de beoordeling van documenten geconstateerd worden (zoals lessons learned of risico's die nog niet zijn onderkend).
4. Fox-IT zal daarbij ook de rol van tegenlezer op zich nemen door in de stukken actief op zoek te gaan naar gaten en herleidbaarheid, aan de hand van open bronnenonderzoek met behulp van ICT-ondersteuning (OSINT-onderzoek).
5. Uitgangspunt daarbij is dat onderzoekers van Fox-IT daarbij in teamverband werken met medewerkers van Opdrachtgever en met 2 á 3 externe advocaten/Wob-specialisten. Resultaten van de beoordeling zullen zoveel mogelijk direct worden verwerkt en uiteindelijk in een gezamenlijke eindrapportage worden vastgelegd.

1.3 Leeswijzer

Wanneer in dit rapport gesproken wordt over NLA-documenten, dan wordt daarmee gerefereerd aan de set van documenten als onderdeel van de betreffende NLA-Wob-publicatie in juni 2019.

De term 'gesteunde groep' verwijst naar één van de Syrische oppositiegroepen die gesteund zijn in het NLA-programma en daarom als Staatsgeheim GEHEIM zijn gerubriceerd.

Wanneer in dit rapport wordt gesproken over de vertrouwelijke informatie, dan wordt daarmee gerefereerd naar de gerubriceerde informatie die beschermd dient te worden bij de Wob-publicatie zoals beschreven in de situatieschets.

Dit hoofdstuk beschrijft de achtergrondinformatie en doelstellingen die ten grondslag liggen aan het uitgevoerde project. Hoofdstuk 2 beschrijft de opzet en werkwijze door Fox-IT. In hoofdstuk 3 worden in algemene bewoordingen de bevindingen van het onderzoek beschreven. Hoofdstuk 4 beschrijft de door Fox-IT geïdentificeerde risico's van herleidbaarheid en aanbevelingen tot mitigatie.

Appendix A bevat een verklarende woordenlijst ter verduidelijking van technische termen in dit rapport.

Appendix B bevat de resultaten uit het OSINT-onderzoek, de steekwoorden en resultaten uit het steekwoordenonderzoek. Deze bijlage is gerubriceerd als Staatsgeheim GEHEIM en is daarom niet opgenomen in dit rapport. De bijlage is opgeslagen en gedeeld in een, daartoe geschikte, beveiligde omgeving.

2 Opzet en werkwijze

Dit hoofdstuk beschrijft de opzet van het project en de werkwijze van Fox-IT. Het beperkt zich tot de activiteiten uitgevoerd door Fox-IT. De opzet van het omvattende Wob-herbeoordelingsproject wordt in een omvattende rapportage (opgesteld door Opdrachtgever) besproken.

2.1 Het beoordelingsproces

Ten behoeve van de herbeoordeling van het Wob-verzoek, heeft Opdrachtgever een beoordelingsteam samengesteld, bestaande uit:

- Een projectleider uit de organisatie van Opdrachtgever
- Twee juridische medewerkers uit de organisatie van Opdrachtgever
- Diverse inhoudelijke deskundigen uit de organisatie van Opdrachtgever
- Twee advocaten van Pels Rijcken (landsadvocaat)
- Twee onderzoekers van Fox-IT

Fox-IT heeft gedurende het beoordelingsproces voor een groot deel gefunctioneerd als deskundige op het vlak van OSINT-technieken en herleidbaarheid. In deze rol heeft Fox-IT deelgenomen aan overleggen en advies gegeven op het vlak van herleidbaarheid. Daarnaast heeft Fox-IT zelfstandig OSINT-onderzoeken en steekwoordenonderzoeken uitgevoerd.

Aan het begin van het project heeft Fox-IT, samen met de rest van het beoordelingsteam, diverse herleidbaarheidsrisico's geïdentificeerd in de Wob-publicatie van juni 2019. Deze risico's zijn door Fox-IT verder onderbouwd met behulp van OSINT-onderzoeken. De geïdentificeerde risico's hebben geleid tot diverse aanbevelingen van Fox-IT om zodoende de herleidbaarheidsrisico's te kunnen mitigeren.

Deze aanbevelingen zijn door de juristen binnen het beoordelingsteam in overweging genomen en gebruikt voor het opstellen van een reeks beoordelingslijnen. Aan de hand van deze beoordelingslijnen heeft Opdrachtgever de NLA-documenten uit de Wob-publicatie juni 2019 nogmaals beoordeeld.

Fox-IT heeft, met het oog op herleidbaarheid, op de door Opdrachtgever herbeoordeelde documenten een extra controle uitgevoerd. Uit deze controle volgden enkele ongelakte teksten die door Fox-IT als risicovol zijn aangemerkt. De desbetreffende risicovolle teksten bleken allemaal gerelateerd te zijn aan de eerder geidentificeerde risico's zoals beschreven in hoofdstuk 4 van dit rapport. Het betrof hier voornamelijk datums, tijden, locaties en beschrijvingen van gebeurtenissen die in de context een indirect herleidbaarheidsrisico opleverden.

Opdrachtgever heeft de risicovolle teksten in overweging genomen en, met inachtneming van de Wob-uitzonderingsgronden, op een aantal van deze teksten additionele lakhandelingen verricht.
Daarnaast heeft Opdrachtgever geoordeeld dat de risicovolle teksten geen aanleiding gaven tot het aanpassen van de reeds toegepaste beoordelingslijnen.

2.2 IT-omgeving

Fox-IT heeft dit onderzoek verricht op locatie van de Opdrachtgever. Ten behoeve van het project is een afgesloten projectruimte ingericht met een kluis waarin vertrouwelijk materiaal werd opgeborgen. Bij deze kluis werd een logboek bijgehouden waarin is bijgehouden wie, wanneer, welk materiaal uit de kluis heeft meegenomen uit de projectruimte. Fox-IT heeft in overleg met Opdrachtgever een IT-omgeving ingericht met IT-middelen die uitsluitend voor dit onderzoek zijn gebruikt.

Deze omgeving was als volgt opgebouwd:

Stg-omgeving
Een apart, losgekoppelde omgeving was ingericht voor het behandelen van staatsgeheime informatie. In deze omgeving zijn bijvoorbeeld notities bijgehouden en de NLA-documenten doorzoekbaar gemaakt, zodat de documenten daarbinnen doorzocht konden worden. Deze omgeving is tot Stg-omgeving benoemd en als zodanig goedgekeurd door Opdrachtgever.
De Stg-omgeving bestond uit drie laptops die onderling verbonden waren met een router. Deze router en laptops waren niet verbonden met het internet en/of andere netwerken. Informatie van- en naar deze omgeving werd overgebracht via een versleutelde USB-stick.

OSINT-omgeving
Ten behoeve van OSINT-onderzoek is door Fox-IT een tweede omgeving ingericht. Deze omgeving werd uitsluitend gebruikt voor het uitvoeren van onderzoek op internet. Deze omgeving is de OSINT-omgeving genoemd.
De OSINT-omgeving bestond uit een netwerk van twee laptops die met het internet verbonden waren via een WLAN-4G router. Fox-IT heeft gebruik gemaakt van een Vodafone SIM kaart voor de 4G connectie naar het internet. Het Vodafone IP-adres (of IP-adressen) waarvan gebruik is gemaakt, is niet zondermeer herleidbaar naar Fox-IT en/of Opdrachtgever. Opdrachtgever heeft geoordeeld dat deze werkwijze als voldoende anoniem is beschouwd voor dit onderdeel van het project.

Gedurende het onderzoek was de IT-apparatuur ten alle tijden opgesloten in een kluis of onder toezicht van het beoordelingsteam. De gegevensdragers van de laptops waren gedurende het onderzoek versleuteld door middel van Microsoft Bitlocker en zijn na afloop van het onderzoek overgedragen aan Opdrachtgever ter vernietiging.

2.3 Herleidbaarheid

De vertrouwelijke informatie die door Opdrachtgever beschermd dient te worden, betreft specifiek de namen en locaties van de gesteunde groeperingen (zodoende als Staatsgeheim GEHEIM gerubriceerd) alsook de betrokken uitvoerders (Departementaal VERTROUWELIJK gerubriceerd). De NLA-documenten zijn allemaal gerelateerd aan deze gesteunde groepen en de uitvoerders en geven dus, in meer of mindere mate, iets weg over voor bedoelde vertrouwelijke informatie. De hoeveelheid informatie die weggegeven wordt, is bepalend voor het risico van bekendwording van deze informatie. De mate waarin de informatie leidt tot de bekendwording van de te beschermen informatie, wordt de herleidbaarheid genoemd.

2.3.1 Bronnen

Door informatie uit externe bronnen te combineren met de informatie uit de NLA-documenten kan de laatste informatie in sommige gevallen herleid worden naar te beschermen vertrouwelijke informatie. Fox-IT maakt hierbij onderscheid tussen de volgende externe bronnen:

Open bronnen. Dit betreft informatiebronnen, online of offline, die voor iedereen toegankelijk zijn. Bekende voorbeelden van open bronnen zijn: Google Search, Facebook en Twitter. Open bronnen kunnen soms ook enkel tegen betaling beschikbaar zijn. Indien een ieder tegen betaling toegang kan krijgen, dient dit ook beschouwd te worden als open bron.

Gesloten bronnen. Dit betreft informatiebronnen, online of offline, die slechts beschikbaar zijn voor een beperkte groep mensen. Hierbij valt de denken aan internetfora die hun gebruikers screenen voor gebruik, eigen databases en databases die slechts beschikbaar zijn voor specifieke personen of instanties.

Menselijke bronnen. Dit betreffen personen die één op één informatie delen. Dit kan gebeuren doordat ze bevraagd worden om informatie te delen of omdat ze zelf op zoek gaan om informatie te delen. Een commandant van een groep die informatie deelt met een onderzoeker over het NLA-programma is een voorbeeld van een menselijke bron.

2.3.2 Voorbeelden van herleidbaarheid

Hieronder zal het concept herleidbaarheid geïllustreerd worden aan de hand van een drietal fictieve voorbeelden.

Voorbeeld 1. Directe herleidbaarheid.
Het document bevat de naam van een gesteunde groepering. Dit zegt direct om welke groepering het gaat. De naam is daarom direct herleidbaar naar vertrouwelijke informatie.

Voorbeeld 2. Indirecte enkelvoudige herleidbaarheid.
Een document bevat de passage[1] "Commandant al-hamid is hoofd van groepering <gelakt>". De passage vermeld niet welke groepering het hier betreft. Echter, een onderzoeker kan via Google zoeken op "rebel group al-hamid" en zo achterhalen welke groepering deze commandant leidt. Deze passage is daarom indirect herleidbaar naar vertrouwelijke informatie.

Voorbeeld 3. Indirecte samengestelde herleidbaarheid.
Gegeven de passage "In december 2017 is <gelakt> samengegaan met een andere groep in het noorden" en even later de passage "De stad waarin de nieuw gevormde groep <gelakt> actief is, heeft ongeveer 150.000 inwoners". De verschillende elementen zijn los niet met voldoende zekerheid herleidbaar. Echter, een onderzoeker zal door middel van verschillende bronnen, zoals genoemd in 2.3.1 kunnen achterhalen op welke groepen in december 2017 zijn samengegaan en vervolgens vaststellen welke van deze groepen hun hoofdkwartier in een stad met ongeveer 150.000 inwoners heeft. Deze informatie is samen indirect herleidbaar naar vertrouwelijke informatie.

[1] Deze passage, als ook de passage in Voorbeeld 3, is fictief en slechts bedoeld als voorbeeld. Indien enige gelijkenissen bestaan met bestaande groepen, dan berust dat op toeval en bestaat er geen relatie tussen de passage en de betreffende groep.

2.4 OSINT-onderzoek

Open Source INTelligence is informatie afkomstig uit open bronnen die gebruikt wordt in de context van een onderzoek. OSINT-onderzoek is onderzoek op basis van dergelijke informatie.

Fox-IT heeft onderzoek verricht naar herleidbaarheid van informatie in diverse NLA-documenten. Het doel van dit onderzoek was drieledig:

- Het identificeren van herleidbaarheidsrisico's in de NLA-documenten van juni 2019.
- Het vinden van voorbeelden van herleidbaarheid naar vertrouwelijke informatie ter onderbouwing van de aanbevelingen.
- Het toetsen van de nieuwe beoordelingslijnen.

Fox-IT heeft zelf actief in de NLA-documenten gezocht naar informatie die mogelijk herleidbaar is naar vertrouwelijke informatie. Daarnaast zijn met regelmaat passages geduid door andere leden van het beoordelingsteam die mogelijk herleidbaar zouden zijn. Als uitgangspunt zijn de NLA-documenten gebruikt uit de Wob-publicatie van juni 2019. De documenten zijn vervolgens aandachtig doorgenomen. Op basis van de informatie uit het document is vervolgens getoetst of de informatie via online open bronnen herleidbaar is naar vertrouwelijke informatie.

Fox-IT heeft voor haar onderzoek enkel gebruik gemaakt van online open bronnen. De volgende bronnen zijn onder andere (maar niet uitsluitend) gebruikt in het OSINT-onderzoek:

- Google zoekmachine
- Google translate
- Youtube
- Twitter
- Facebook
- Reverse image zoekmachine
- Liveuamap
- Reddit
- Websites waarnaar verwezen wordt via bovengenoemde bronnen

Het OSINT-onderzoek heeft geresulteerd in verschillende voorbeelden van indirecte herleidbaarheid en heeft inzicht gegeven in de kwetsbaarheden van de voorgaande werkwijze in het lakken. De resultaten worden besproken in hoofdstuk 3 en hoofdstuk 4.

2.4.1 Beperkingen van het OSINT-onderzoek

Om het OSINT-onderzoek af te kaderen is met Opdrachtgever besloten om ongeveer tien mandagen te besteden aan het onderzoeken op het internet. In deze tijd zijn een select aantal documenten onderzocht op herleidbaarheid en zijn zoekacties tot bepaalde diepte uitgelopen. Fox-IT acht het aannemelijk dat een onderzoek waarin meer tijd beschikbaar is voor OSINT-onderzoek meer documenten zal bestrijken en mogelijk meer resultaten zal opleveren.

Gedurende het onderzoek is door Fox-IT uitsluitend gebruik gemaakt van open bronnen op het internet. Fox-IT heeft geen zicht op gesloten bronnen die mogelijk beschikbaar zijn voor andere onderzoekers.

Tevens is reeds bekend, onder andere uit Trouw artikelen[2], dat bijvoorbeeld journalisten uitgebreid telefonisch contact hebben gezocht met Syrische groepen om informatie in te winnen. Dit is illustratief voor hoe menselijke bronnen gebruikt kunnen worden om informatie te verkrijgen over het NLA-programma. Deze informatie kan vervolgens gecombineerd worden met informatie uit de NLA-documenten voor bevestiging. Fox-IT heeft gedurende het onderzoek geen gebruik gemaakt van menselijke bronnen of gesloten bronnen om de herleidbaarheid te toetsen.

Een derde beperking van het OSINT-onderzoek ligt in het feit dat het een momentopname betreft. Het is mogelijk dat informatie die nu (nog) niet vindbaar is in open bronnen in de toekomst wel vindbaar gaat zijn. Dit kan zijn omdat de informatie later publiek gemaakt wordt, nieuwe pagina's doorzoekbaar zijn gemaakt of links naar de informatie zijn verschenen. Als iets gedurende dit OSINT-onderzoek onvindbaar is gebleken, kan daaruit niet afgeleid worden dat dit in de nabije toekomst onvindbaar zal blijven.

2.5 Documenten doorzoeken op steekwoorden

Naast de handmatige bestudering van de NLA-documenten is besloten een aanvullende specifieke controle te doen op aanwezigheid van vertrouwelijke namen. Dit is gedaan door de NLA-documenten van juni 2019 doorzoekbaar te maken en vervolgens te doorzoeken op steekwoorden.

De NLA-documenten zijn in de Stg-omgeving doorzoekbaar gemaakt door middel van de software Veritas eDiscovery[3]. De software heeft ingescande documenten voor het grootste deel omgezet[4] naar tekst door middel van optical character recognition (OCR). Vervolgens heeft de software de tekst geïndexeerd om het efficiënt doorzoekbaar te maken.

Fox-IT heeft van Opdrachtgever een lijst van namen ontvangen. Volgens Opdrachtgever is dit de volledige lijst van gerubriceerde namen van gesteunde groepen en de namen van de uitvoerders. Deze lijst is door Fox-IT omgezet naar een lijst van steekwoorden waarmee de NLA-documenten uit juni 2019 zijn doorzocht. Deze lijsten zijn zodoende als staatsgeheim gerubriceerd en daarom opgenomen in Bijlage B en niet opgenomen in dit rapport.

2.5.1 Beperkingen van het steekwoordenonderzoek

De kwaliteit van sommige ingescande documenten leverde een beperking op. De mate waarin de ingescande documenten via OCR correct omgezet worden naar tekst wordt voor een groot deel bepaald door de kwaliteit van de scans: voor slecht leesbare scans is de kans groot dat deze niet de juiste tekst opleveren. Sommige NLA-documenten zijn gedurende de voorgaande herbeoordelingen reeds meermaals ingescand waarbij de leesbaarheid van de tekst sterk achteruit is gegaan. Voor die documenten is de kans groot dat de teksten niet goed worden omgezet en daarom ook niet goed doorzocht kunnen worden[5].

---

[2] https://www.trouw.nl/nieuws/zo-kwam-verslaggever-ghassan-dahhan-in-contact-met-syrische-rebellenleiders~be77bb56/

[3] Veritas eDiscovery is een e-discovery platform dat gebruikt wordt om data doorzoekbaar te maken en met meerdere mensen te kunnen doorzoeken en reviewen.

[4] Een aanzienlijk deel van de documenten betrof ingescande documenten. Dit z jn feitelijk plaatjes waarin tekst afgebeeld is. Om dit doorzoekbaar te maken, zullen deze plaatjes eerst (terug) omgezet moeten worden naar tekst.

[5] Het is moeilijk te kwantificeren wat de foutmarge is voor de omzetting naar tekst. Hiervoor zou een vergelijking gemaakt moeten worden met de ongescande versies van de documenten (voor zover die besch kbaar z jn) en dat valt buiten de scope van dit project.

Een tweede beperking ligt in het feit dat namen van sommige groepen op veel verschillende manieren gespeld kunnen worden en dat dezelfde groepen onder verschillende namen hebben bestaan. De kans is aanzienlijk dat niet alle spellingsvormen of namen zijn opgenomen in de steekwoordenlijst. Fox-IT heeft getracht de steekwoordenlijst zo te maken dat mogelijk verschillende spellingen hiermee zo veel mogelijk afgevangen worden.

Zoals besproken met Opdrachtgever, leiden bovenstaande beperkingen ertoe dat niet volledig op de technologie vertrouwd kan worden om alle manifestaties van namen te vinden. Daarom is besloten het steekwoordenonderzoek als een aanvullende controle in te zetten. Naast het steekwoordenonderzoek zijn de documenten meermaals handmatig door het beoordelingsteam bestudeerd op (onder andere) aanwezigheid van vertrouwelijke namen. Het risico dat vertrouwelijke namen door technische beperkingen gemist worden, is daarmee getracht te reduceren.

3 Bevindingen

3.1 OSINT-onderzoek

Fox-IT heeft onderzoek verricht naar herleidbaarheid van informatie in diverse NLA-documenten. De verschillende OSINT-onderzoeken en de hieruit vloeiende gedetailleerde resultaten bevatten staatsgeheime informatie en zijn daarom beschreven in bijlage B. Deze bijlage is opgesteld in de Stg-beveiligde omgeving bij Opdrachtgever en op locatie via een beveiligde omgeving met Opdrachtgever gedeeld.

Fox-IT heeft met de methodiek en daarbij horende beperkingen, zoals beschreven in hoofdstuk 2.4, een zestal voorbeelden gevonden die illustratief zijn voor de herleidbaarheidsrisico's in de gepubliceerde NLA-documenten van juni 2019.

Het is van belang te vermelden dat de resultaten uit de OSINT-onderzoeken voortkomen uit een afgekaderde opdracht, alsmede een momentopname zijn. Gezien de afkadering in de tijd is er door Opdrachtgever voor gekozen onderzoek te doen naar een beperkte selectie van teksten en afbeeldingen in de NLA-documenten. Niet elke in potentie risicovolle tekst of afbeelding kon uiteindelijk door Fox-IT onderzocht worden of binnen de gestelde tijd herleid worden naar vertrouwelijke informatie. Dit neemt echter niet weg dat het risico op herleidbaarheid wel van toepassing is op dergelijke tekst of afbeelding, aangezien een andere onderzoeker met meer tijd, middelen, bronnen of op een ander moment de informatie mogelijk wel kan herleiden.

3.2 Steekwoordenonderzoek

Fox-IT heeft een steekwoordenonderzoek uitgevoerd op de NLA-documenten van juni 2019. Daarbij zijn de resultaten handmatig beoordeeld. Dit heeft geresulteerd in één geïdentificeerde vertrouwelijke naam, die vervolgens door de juristen binnen het beoordelingsteam is aangemerkt om te lakken.

4 Risico's en aanbevelingen

Fox-IT heeft in de NLA-documenten van juni 2019 een aantal risico's voor herleidbaarheid geïdentificeerd. Deze risico's zijn onder te brengen in een aantal categorieën en worden in de volgende subhoofdstukken behandeld. Daarbij wordt tevens een advies uitgebracht voor het mitigeren van de herleidbaarheidsrisico's. Deze adviezen komen direct voort uit de geïdentificeerde risico's en zijn ter overweging voorgelegd aan Opdrachtgever. Fox-IT kan geen uitspraak doen over de vraag of de herleidbaarheidsrisico's en de daaraan gekoppelde (technische-) aanbevelingen overeenkomen met de (juridische-) mogelijkheden tot lakken welke Opdrachtgever toekomen op grond van de Wob.

4.1 Afbeeldingen

Fox-IT heeft vastgesteld dat in de NLA-documenten van juni 2019 diverse afbeeldingen zijn opgenomen en deels gelakt of helemaal niet gelakt zijn.
Afbeeldingen vormen op zichzelf een permanent risico op herleidbaarheid via verschillende OSINT-technieken. Met zogenaamde reverse-image zoekmachines kan snel worden gezocht op de aanwezigheid van een specifieke foto op het internet. Indien de afbeelding op een bepaald moment online is geplaatst, is de kans groot dat deze terug te vinden is via één van deze zoekmachines. De gepubliceerde afbeelding kan leiden naar meer informatie gerelateerd aan de afbeelding. De afbeeldingen worden in de NLA-documenten gerelateerd aan vertrouwelijke informatie (bijvoorbeeld de naam van een gesteunde groep waarvan de leider is afgebeeld) en het terugvinden van de afbeelding vormt daarmee een direct risico voor de vertrouwelijke informatie.

Fox-IT heeft steekproefsgewijs een aantal afbeeldingen opgezocht en daarbij met beperkte inspanning een match gevonden. Uit het gegeven dat door Fox-IT niet meer matches zijn gevonden, kan niet worden afgeleid dat niet langs andere wegen of met andere applicaties door een gemotiveerd en goed ingevoerde onderzoeker wel een match is te krijgen. Tevens bestaat de mogelijkheid op toekomstige plaatsing en/of bekend worden van (beeld)materiaal die daardoor op een later moment tot een match kan leiden.

Los van de herleidbaarheid door reverse-image zoekmachines, bevatten de afbeeldingen kernmerken die, zeker voor een geïnformeerde onderzoeker, directe of indirecte aanwijzingen kunnen opleveren voor namen van gesteunde groepen (bijvoorbeeld type uniformen, onderdelen van gebouwen, specifieke producten, etc).

Op basis van bovengenoemde risico's adviseert Fox-IT om in overweging te nemen alle afbeeldingen in volledigheid weg te lakken.

4.2 Namen, logo's en andere identificerende vernoemingen

Gedurende het onderzoek is gebleken dat de gelakte NLA-documenten van juni 2019 afbeeldingen bevatten waarop Arabische teksten te lezen zijn of vlaggen te zien zijn. Daarnaast is vastgesteld dat gebruik wordt gemaakt van pseudoniemen voor groepen.

Namen, logo's, vlaggen en andere identificerende vernoemingen geven informatie weg over de gesteunde groepen. Een (deel van) een naam of logo is vaak direct herleidbaar naar de gesteunde groep. Ook labels of codes die gebruikt worden als pseudoniem voor een groep vormen een risico. Een dergelijk pseudoniem zal weliswaar niet direct herleidbaar zijn, maar een onderzoeker zal gebeurtenissen over verschillende documenten kunnen koppelen aan dezelfde groep. Het pseudoniem hoeft dan slechts op één locatie herleidbaar te zijn, om voor de onderzoeker in alle documenten de groep te onthullen.

Op basis van bovengenoemde risico's adviseert Fox-IT om in overweging te nemen alle identificerende vernoemingen naar gesteunde groepen weg te lakken.

4.3 Gerelateerde organisaties en groepen

Naast de gesteunde groepen beschrijven de NLA-documenten een aantal gerelateerde organisaties, waaronder andere gewapende groepen, uitvoerders en M&E[6] organisaties. De gerelateerde organisaties zijn in meer of mindere mate weggelakt, maar zijn in sommige gevallen nog bij naam genoemd en in andere gevallen eenvoudig te herleiden.

Informatie over organisaties gerelateerd aan de gesteunde groepen is mogelijk herleidbaar tot de gesteunde groepen zelf. Deze herleidbaarheid kan liggen in de onderscheidenheid van de relatie. Bijvoorbeeld: 'groep A is voortgekomen uit groep B' of 'Uitvoerder X levert goederen aan de gesteunde groepen'. Open bronnen, maar vooral ook gesloten- en menselijke[7] bronnen kunnen vervolgens gebruikt worden om vanuit de gerelateerde organisaties door te rechercheren naar gesteunde groepen. Voor het voorkomen van herleidbaarheid via deze route is Opdrachtgever afhankelijk van de strikte geheimhouding door de organisaties en hoeveelheid informatie beschikbaar op internet die iets vertelt over de relatie. Het vernoemen van gerelateerde groepen en organisaties vormt daarom een herleidbaarheidsrisico voor de vertrouwelijke informatie.

Op basis van het bovengenoemde risico adviseert Fox-IT om in overweging te nemen de informatie die herleidbaar is naar gerelateerde organisaties weg te lakken.

4.4 Tijds- en locatiebepalingen van gebeurtenissen

Bij het beoordelen van de NLA-documenten van juni 2019 is vastgesteld dat veelvuldig datums en locaties genoemd worden. Voorbeelden zijn een datum van een email of een datum en locatie van een specifieke gebeurtenis.

Tijd- en locatiebepalingen geven doorgaans belangrijke informatie over waar en wanneer een beschreven gebeurtenis heeft plaatsgevonden. Wanneer een gebeurtenis voldoende onderscheidend is, zal de gebeurtenis herleidbaar zijn tot de namen van partijen betrokken bij een dergelijke gebeurtenis. We leven in een tijdperk waarin gebeurtenissen veelvuldig en bijna direct met datum en locatie worden

[6] Monitoring & Evaluation organisaties zijn ingezet door Opdrachtgever om het NLA-programma in Syrie te evalueren. Deze organisaties staan op locatie in contact met de verschillende betrokken organisaties en groepen.

[7] Het is bekend dat onderzoekers gebruik kunnen maken van menselijke bronnen voor inlichtingen. Dit is onder andere beschreven in een artikel over het NLA-programma van Trouw. https://www.trouw.nl/nieuws/hoe-al-qaida-aan-een-mobiele-bakkerij-uit-nederland-kwam~bf192ece/

vastgelegd op het internet. Hierbij valt te denken aan verslaglegging op een nieuws-site, een tweet op Twitter en een video op Youtube. Dit maakt het mogelijk om specifieke gebeurtenissen op basis van een beschrijving en locatie en/of tijd via open-bronnen terug te vinden. Een voorbeeld hiervan zijn schriftelijke verklaringen ondertekend door groepen die regelmatig op Twitter worden geplaatst. Een beschrijving hiervan in de documenten zou relatief makkelijk terugvindbaar zijn op Twitter.

Naast de open bronnen kunnen gesloten- en menselijke bronnen gebruikt worden om de gebeurtenissen te relateren aan vertrouwelijke informatie. Tijds- en locatiebepalingen die direct of indirect gerelateerd zijn aan de gesteunde groepen vormen daarom een herleidbaarheidsrisico.

Op basis van het bovengenoemde risico adviseert Fox-IT om in overweging te nemen vermeldingen van tijd en locatie te lakken.

4.5 Onderscheidende beschrijvingen van gebeurtenissen

Bij het beoordelen van de NLA-documenten van juni 2019 is vastgesteld dat veelvuldig specifieke gebeurtenissen worden beschreven. Hierbij valt te denk aan beschrijvingen van aanvallen op groepen, levering van goederen aan de groepen en organisaties van de groepen. Het detailniveau van de omschrijvingen varieert.

De beschreven gebeurtenissen zijn op enige wijze gerelateerd aan de gesteunde groepen (anders werden ze niet beschreven in de NLA-documenten). Een onderzoeker die een beschreven gebeurtenis kan terugvinden in open bronnen zal waarschijnlijk de betrokken groepen kunnen duiden. De sleutel ligt hier in de terugvindbaarheid van een gebeurtenis. De terugvindbaarheid wordt bepaald door een aantal zaken:

1. Specifieke informatie, zoals een locatie en een tijd. Echter, ook het aantal geleverde goederen in een levering, het leveren van een bijzonder goed en het aantal slachtoffers in een aanslag kunnen bijvoorbeeld een gebeurtenis specificeren.
2. Publiciteit rondom de gebeurtenis. Dit kan zijn in de vorm van een post op Facebook of een nieuwsartikel.
3. Frequentie van dergelijke gebeurtenissen binnen de periode en regio.

De aanslag op president Kennedy zal al vindbaar zijn met de informatie: moord op president, 20e eeuw, Noord-Amerika. Een luchtaanval op een hoofdkwartier van een gesteunde groep zal moeilijk vindbaar zijn op basis van het land en de eeuw. Echter, wanneer de dag en een stad meegegeven worden, is de kans al groter dat de luchtaanval vindbaar is op Twitter en andere social media sites. Hoe vaak een bepaalde (vergelijkbare) gebeurtenis plaatsvindt, is soms moeilijk op voorhand in te schatten.

Rapportages of andersoortige documenten waarin uitgebreid geschreven wordt over specifieke gebeurtenissen vormen daarom een groter risico. Elk stukje informatie kan beschouwd worden als een puzzelstukje; met voldoende stukjes, kan de lezer de puzzel zelf invullen.

Op basis van bovengenoemde risico adviseert Fox-IT om in overweging te nemen beschrijvingen van specifieke gebeurtenissen of een reeks van gebeurtenissen te lakken of in ieder geval voldoende te ontdoen van specifieke kenmerken. Bij twijfel over de frequentie van vergelijkbare gebeurtenissen, adviseert Fox-IT om in de overweging uit te gaan van een lage frequentie en dus hogere onderscheidenheid van de gebeurtenis.

4.6 NLA-documenten op archiefweb.eu

Fox-IT heeft vastgesteld dat de NLA-documenten van november 2018 op 21 oktober 2019 nog beschikbaar waren op de officiële archiefwebsite van de rijksoverheid: rijksoverheid.webarchief.eu. Fox-IT heeft tevens in de twee bekende archiveringsdiensten gezocht: Google cache en web.archive.org. Op die locaties zijn de NLA-documenten niet teruggevonden.

De betreffende NLA-documenten op rijksoverheid.webarchief.eu bevatten vertrouwelijke informatie en informatie herleidbaar naar de vertrouwelijke informatie en zijn relatief eenvoudig te vinden voor een onderzoeker. De beschikbaarheid is daarom een aanzienlijk risico op onderkenning van deze vertrouwelijke informatie.

Op basis van bovengenoemde risico, adviseert Fox-IT Opdrachtgever om de beheerder van rijksoverheid.webarchief.eu te verzoeken de betreffende NLA-documenten te verwijderen.

Ten tijde van schrijven, op 13 november 2019, is door Fox-IT een controle gedaan op de aanwezigheid van deze documenten. Daarbij is vastgesteld dat het Wob besluit van november 2018 en de daarbijhorende bijlagen niet meer te downloaden zijn van rijksoverheid.archiefweb.eu.

Opgemaakt op 13 november 2019

Appendix A

A.1 Verklarende woordenlijst

Term	Uitleg
OCR	Optical character recognition. Technologie waarmee tekst uit een afbeelding wordt omgezet in bewerkbare tekst. Een voorbeeld hiervan is automatische kentekenplaatherkenning.
OSINT	Open Source INTelligence is informatie afkomstig uit open bronnen die gebruikt wordt in de context van een onderzoek. Voorbeelden van open bronnen zijn social media sites en internetfora.
Reverse-image zoekmachine	Reverse-image zoekmachines maken het mogelijk om afbeeldingen te vinden op het internet die gelijkenissen vertonen (of hetzelfde zijn) als de ingegeven afbeelding. Een gebruiker kan een afbeelding van een auto invoeren en de zoekmachines zal vertellen waar op internet dat plaatje of een variant daarvan voorkomt.
Stg (rubricering)	Rubriceringsklasse Staatsgeheim van bijzonder informatie volgens het Voorschrift Informatiebeveiliging voor Bijzondere Informatie (VIRBI). Stg rubricering wordt onderverdeeld in drie niveau's: Stg Zeer Geheim , Stg Geheim en Stg Confidentieel.

Appendix B Resultaten uit onderzoek

Deze bijlage bevat de resultaten uit het OSINT-onderzoek, de steekwoorden en de resultaten uit het steekwoordenonderzoek. Deze bijlage is gerubriceerd als Staatsgeheim GEHEIM en is daarom niet opgenomen in dit rapport. De bijlage is opgeslagen en gedeeld in een daartoe geschikte beveiligde omgeving. In opdracht van Opdrachtgever is onderstaand veralgemeniseerd overzicht met betrekking tot de inhoud van de bijlage opgenomen.

Tabel 1. Overzicht van resultaten uit het onderzoek

Nummer	Omschrijving	Herleidbaarheidsrisco
1	Informatie uit een passage was via social media Reddit en Twitter herleidbaar naar vertrouwel jke informatie door een beschrijving van een gebeurtenis en een datum en locatie.	4.4 en 4.5
2	Informatie uit een passage was via Google en Twitter herleidbaar naar vertrouwelijke informatie door een beschr jving van een gebeurtenis en een datum en locatie. Het was vervolgens te bevestigen door middel van een weergegeven afbeelding.	4.1, 4.4 en 4.5
3	Informatie uit een passage was via Google en Wikipedia herleidbaar naar vertrouwelijke informatie doordat specifieke aantallen genoemd werden in combinatie met een datum en een reeks gebeurtenissen.	4.4 en 4.5
4	Informatie uit een passage was via Twitter herleidbaar naar vertrouwelijke informatie door een beschrijving van een gebeurtenis en een datum en locatie.	4.4 en 4.5
5	Informatie uit een overzicht over een t jdsperiode was via Wikipedia en Google herleidbaar naar vertrouwel jke informatie door kenmerkende aantallen.	4.5
6	Een afbeelding uit een document was terugvindbaar op het internet.	4.1
7	Een document bevatte een vertrouwelijke naam.	4.2

Fox-IT

Fox-IT voorkomt, onderzoekt en beperkt de meest serieuze dreigingen door cyberaanvallen, datalekken of fraude met innovatieve oplossingen voor overheid, defensie, politie, vitale infrastructuur, banken en grote bedrijven wereldwijd. In zijn aanpak combineert het bedrijf slimme ideeën met technologie om hiermee innovatieve oplossingen te bieden die zorgen voor een veilige maatschappij. Fox-IT ontwikkelt producten en maatwerkoplossingen om de beveiliging van gevoelige overheidssystemen te garanderen, industriële netwerken te beschermen, online bankiersystemen te verdedigen en strikt vertrouwelijke data te beveiligen.

Bezoek onze website voor meer informatie over Fox-IT en onze partners.

CLASSIFICATIE
COMMERCIAL RESTRICTED
MINBZ

FOX IT
part of nccgroup

fox-it.com

Fox-IT
Olof Palmestraat 6, Delft
Postbus 638, 2600 AP Delft
Nederland

T +31 (0)15 284 7999
F +31 (0)15 284 7990
fox@fox-it.com