BUYER GROUP

AI BEELDHERKENNING MET DRONES IN DE OPENBARE RUIMTE

MARKTVISIE EN INKOOPSTRATEGIE

JANUARI 2024

Een Buyer Group is een samenwerking van publieke opdrachtgevers die een gedeelde marktvisie voor een bepaalde product-categorie ontwikkelen en vervolgens deze in komende jaren implementeren in hun inkooppraktijk. De inhoud van deze marktvisie is op basis van inzichten van deelnemers van de Buyer Group en mede op basis van informatie uit een marktconsultatie. De visie is bedoeld voor lezers als handreiking om verantwoorde digitale innovaties te ontwikkelen en in te kopen.

De Buyer Group AI beeldherkenning met drones is een initiatief van de Nederlandse AI Coalitie in samenwerking met PIANOo Expertisecentrum Aanbesteden[1]. De Buyer Group wordt mogelijk gemaakt door ministerie van Binnenlandse Zaken en Koninkrijksrelaties (Directoraat-generaal Digitalisering en Overheidsorganisatie).

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

NL AI Coalitie

PIANOo EXPERTISECENTRUM AANBESTEDEN

Deelnemende overheden van deze Buyer Goup (willekeurige volgorde)**:**

- Gemeente Breda
- Rijkswaterstaat (RWS)
- Nederlandse voedsel- en warenautoriteit (NVWA)
- ProRail
- Waterschapshuis
- Politie
- Provincie Zuid-Holland
- Waterschap Drents Overijsselse Delta
- Douane
- Gemeente Amsterdam
- Kadaster

Nederlandse Voedsel- en Warenautoriteit
Ministerie van Landbouw, Natuur en Voedselkwaliteit

Douane
Ministerie van Financiën

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

POLITIE

hetWaterschapshuis

provincie Zuid-Holland

kadaster

ProRail

Drents Overijsselse Delta

Gemeente Amsterdam

Gemeente Breda

[1] Deze publicatie is een resultaat van de Buyer Group, onder begeleiding van Joris Krüse en Rolf Zeldenrust (PIANOo). Wilt u meer weten over alle andere Buyer Groups die er bestaan en benieuwd wat de deelnemers van Buyer Groups afgelopen jaar bereikt hebben? U kunt erover lezen via: Public Impact Report 2021.

INHOUDSOPGAVE

VOORWOORD

"Momenteel staat AI volop in de belangstelling. Maar zoals dit prachtige resultaat van zo'n 2 jaar werk laat zien, komt er veel kijken bij de inzet van AI in de praktijk. De Buyer Group haakt in op deze digitale transitie, waarbij nieuwe manieren om data te verzamelen (in dit geval beeldmateriaal via drones) in combinatie met AI-technologie de technische aanjager is van een nieuwe manier van werken. Wat daarbij belangrijk is gebleken, is dat de Buyer Group niet specifiek technisch van aard is. De Buyer Group maakt duidelijk dat het bij de inzet van AI-technologie, naast techniek, bijvoorbeeld ook om thema's als ethiek en publieke acceptatie gaat.

Met deze marktvisie geven de deelnemende overheden een duidelijk signaal af aan ondernemers. De deelnemende overheden binnen deze groep laten ermee zien hoe ze deze digitale innovaties op een verantwoorde manier willen toepassen. Door de door hen geformuleerde uitgangspunten bij toekomstige projecten te gebruiken, kunnen bedrijven daarop gaan anticiperen. Zo dagen deze overheden het bedrijfsleven uit om met een aanbod te komen dat past bij huidige én toekomstige ambities.

Vanuit het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) zien we een enthousiaste groep koplopers die ervaringen en kennis bundelen en aangeven welke specifieke onderwerpen zij relevant vinden op het vlak van AI beeldherkenning met behulp van drones. Deze concretisering van een gecompliceerd thema en het ontsluiten van informatie willen we vanuit het ministerie van BZK ook komende periode ondersteunen, door de Buyer Group te continueren als leernetwerk. Zo zorgen we gezamenlijk dat deze technologieën op verantwoorde en doeltreffende wijze worden ingezet door de (digitale) overheid."

Elja Daae
Beleidscoördinator AI en Algoritmen, Ministerie BZK
Voorzitter Werkgroep Publieke Diensten, Nederlandse AI Coalitie

TER ILLUSTRATIE

AI-technologie[2] inzetten om beeldmateriaal – dat verkregen is door drones – tot waardevolle informatie te verwerken: daar draait het om in dit visiedocument. Deze digitale innovaties bieden namelijk steeds meer mogelijkheden om maatschappelijke uitdagingen het hoofd te bieden. Te denken valt aan het monitoren van biodiversiteit in een bepaald gebied, of de inspectie en onderhoud van infrastructuur, maar ook bijvoorbeeld aan het opsporen van illegale visfuiken.

Voorbeeld van een gebruikssituatie: het opsporen van visfuiken

De NVWA (Nederlandse Voedsel- en Warenautoriteit) zet beeldherkenning en drones in om illegale visserij op te sporen. De drone vliegt autonoom een vooraf bepaalde route waarbij foto's worden gemaakt van het wateroppervlak. Aan de hand van een algoritme worden deze beelden gecontroleerd op fuiken. Als er dan bijvoorbeeld verdachte deining in het water wordt waargenomen gaat de inspecteur naar de specifieke plaats om een inspectie uit te voeren.

› *Benieuwd? Bekijk het filmpje online*

[2] De afkorting AI staat voor 'Artificial Intelligence', ofwel Kunstmatige intelligentie.

Wat doet een Buyer Group?

De Buyer Group AI beeldherkenning met drones brengt deelnemende overheden samen om kennis te vergroten en ervaringen te delen over gebruikssituaties met AI beeldherkenning en drones[3]. Daarbij wil de Buyer Group komen tot een gezamenlijke visie (uitgangspunten) om ambities voor toekomstige aanbestedingen te bepalen. In deze groep bespreken overheden welke huidige en toekomstige wensen er spelen, brengen we de behoeftes in kaart, met daarbij aandacht voor randvoorwaarden en mogelijkheden uit de praktijk. De deelnemers van de Buyer Group bepalen de thema's van de marktvisie én streven na om het vervolgens te implementeren bij nieuwe projecten.

De hoofdlijnen

De overkoepelende ambitie bij de Buyer Group 'AI beeldherkenning met drones' ligt op verantwoord en toekomstbestendig digitaal innoveren met AI beeldherkenningstechnologie met drones.
Om deze ambitie te realiseren ziet de Buyer Group de volgende prioriteiten:

- Borgen van kwaliteit
- Cybersecurity
- Delen van data, AI en informatie
- Ethiek en publieke acceptatie

Belangrijk om te vermelden is dat de ontwikkelingen op het vlak van AI en drones momenteel rap gaan. Wanneer overheden ermee aan de slag gaan, is het advies om zo goed mogelijk op de hoogte te zijn van de laatste stand van zaken bij deze technologieën. Zo is het immers mogelijk dat in komende jaren nieuwe tools[4] gaan opkomen op bovenstaande vier thema's. Het betekent daarnaast ook dat het document een beschrijving geeft van de huidige opvattingen (2023), in komende perioden kunnen onderdelen veranderen of worden geconcretiseerd. Bent u enthousiast over deze Buyer Group, wilt u van gedachten wisselen of verbeteringen aandragen, of op de hoogte blijven? Neem dan contact op via buyergroups@pianoo.nl.

We moedigen aanbestedende diensten aan om de visie uit dit document te gebruiken en om ons feedback te geven via de Buyer Group.

Marktvisie en inkoopstrategie

De Buyer Group beoogt met dit visiedocument inzicht te geven in de thematiek en richting aan te brengen. Deze marktvisie kan onder andere gebruikt worden om houvast te bieden voorafgaand, tijdens en na afronding van aanbestedingen. Dit mede dankzij de concrete en praktische tips en tools voor aanbestedende diensten en marktpartijen.

Verder is ons doel de markt te informeren over de thema's en aandachtspunten van de deelnemende overheden van deze Buyer Group. Omdat de diverse overheden zich langs een soortgelijk perspectief (uitgesplitst in thema's) tot deze digitale innovaties willen wenden, wordt het voor bedrijfsleven interessant om te verdiepen in de ambities en aandachtspunten. Dat maakt het voor ondernemers ook eenvoudiger om vanuit de zaken waarop dit document zich concentreert vervolgens op aanbestedingen in te schrijven.

[3] Vergelijkbaar aan drones zijn ook andere hulpmiddelen mogelijk, zoals vaste camera's, camera in helicopter, camera op trein, rijdende en varende objecten, et cetera.

[4] Bijvoorbeeld om uitlegbaarheid van algoritmen te vereenvoudigen.

Leeswijzer

- In hoofdstuk 1 volgt beknopt de aanleiding en voorbeelden van toepassingen. Daarnaast schetsen we context en ontwikkelingen op het vlak van AI beeldherkenning en van drones.
- Hoofdstuk 2 staat stil bij de visie van de Buyer Group en de uitgangspunten per thema.
- Hoofdstuk 3 verdiept vervolgens de strategie per thema: hoe te komen tot het toekomstbeeld en praktische handvatten daarbij.
- De bijlagen bevatten een afkortingenlijst, een referentielijst en een bijlage met beknopte uitleg over de diverse categorieën algoritmen. Afsluitend een overzicht van de leden van de Buyer Group en gesprekspartners van deelnemende overheden die hebben bijgedragen.

Tot slot verwijzen we voor de volledigheid naar het marktconsultatie-verslag (2022) die mede ten grondslag lag aan bepaalde uitwerkingen in dit visiedocument.
Door een openbare oproep via TenderNed voor het raadplegen van de markt, stuurden 16 bedrijven inhoudelijke reacties toe op de specifieke vragen en waren betrokken bij de consultatiebijeenkomsten die daarop volgden.

Wij willen alle betrokkenen bedanken die vrijwillig hun waardevolle inzichten hebben verstrekt, waarmee ze een belangrijke bijdrage hebben geleverd.

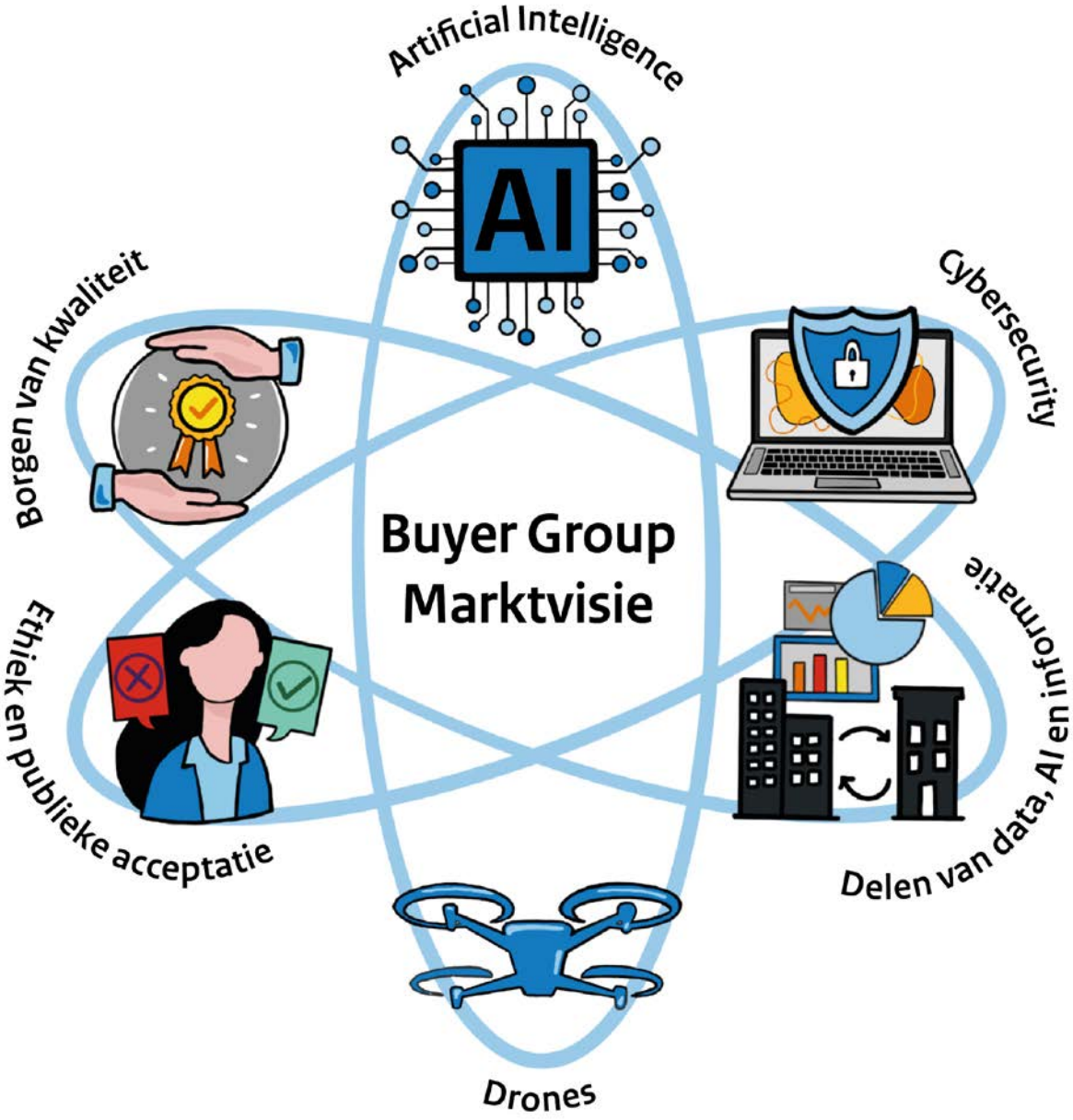
Voor wie is dit document bedoeld?
Voor projectmanagers en strategisch inkoopadviseurs die met overheidsopdrachten op het vlak van AI beeldherkenning met drones aan de slag gaan. Verder is dit document te hanteren als naslagwerk (om in beeld te krijgen wat belangrijke aandachtspunten zijn) wanneer overheden interesse hebben in de inhoud maar nog niet eraan toe zijn om de strategie zelf toe te passen. Hoe meer publieke opdrachtgevers aan de hand van soortgelijke optiek handelen, des te groter de gezamenlijke impact tot verantwoorde digitale innovatie.

Wat bedoelen we met 'marktvisie'?
Wij zien dit als uitgangspunten waarbij de deelnemende overheden uit de Buyer Group gezamenlijk hebben bepaald wat ze relevant vinden in dit werkveld en welke strategische richting ze voor zich zien. Deze marktvisie vormt een leidraad voor overheden bij het nemen van beslissingen en het bepalen van een passende koers in hun projecten/aanbestedingen.

› *Essentieel om te benadrukken: het kan per gebruikssituatie (use-case) verschillen in welke mate thema's relevant zijn*[5]

Wat bevat dit document niet?
Het is geen trendrapport of een verzameling van voorspellingen over de toekomstige ontwikkelingen binnen de markt. Het is in plaats daarvan bedoeld als een hulpmiddel om de huidige prioriteiten en zienswijze van deelnemers van de Buyer Group te begrijpen en toe te passen.

[5] Ter illustratie; bij een gebruikssituatie voor inspectie en onderhoud van publieke (kritieke) infrastructuur zal waarschijnlijk het thema cyber security meer van belang zijn dan bij het voorbeeld over het opsporen van visfuiken (pagina 4).


Artificial Intelligence
AI
Cybersecurity
Delen van data, AI en informatie
Drones
Ethiek en publieke acceptatie
Borgen van kwaliteit
Buyer Group
Marktvisie

1 INLEIDING

1.1 Doel van de visie

Het doel is om te achterhalen hoe kunstmatig intelligente technologie (AI) voor beeldherkenning met toepassing van drones verantwoord te benutten zijn: welke thema's en aspecten zijn voor overheden relevant om te doorgronden wanneer ze hiermee samen met marktpartijen aan de slag willen gaan?

Met de marktvisie laten de deelnemende overheden zien wat de opgave is. De marktvisie moet zorgen voor meer consistentie in de ambitie van overheden en een helder beeld van de toekomst bij projecten op het snijvlak van AI beeldherkenning met drones, voor zowel publieke organisaties als bedrijven.

1.2 Voorbeelden van gebruikssituaties

Het inwinnen van informatie uit beeldmateriaal helpt bij maatschappelijke uitdagingen en om publieke dienstverlening te verbeteren. Slimme digitale drone oplossingen kunnen nieuwe inzichten opleveren voor verschillende vraagstukken. Toepassingen zijn bijvoorbeeld het observeren van een gebied, zoals bij calamiteiten (brandweer, politie), of bij inspectie en onderhoud van objecten (zoals gebouwen).

Daarbij zijn drones een waardevol hulpmiddel voor het verzamelen van gegevens op veel verschillende gebieden. Een drone kan op voor mensen moeilijk te bereiken plekken komen en kan snel en efficiënt hoogwaardige gegevens vastleggen.

Voor we een aantal gebruikssituaties op een rij zetten, benadrukken we dat onderstaande geen complete lijst is maar ter inspiratie dient. Verder kan de status van onderstaande voorbeelden verschillen: soms gaat het om een pilot, in andere gevallen is het al jaren praktijk. Ook de reikwijdte van de projecten verschillen: soms gaat het om grote hoeveelheden data en geavanceerde algoritmes, maar er zijn ook relatief eenvoudige/kleinschalige toepassingen. Het kan gaan om:

Scannen en observeren

Het scannen/observeren van een gebied, om informatie te verkrijgen en inzicht te hebben in de ontwikkelingen daarin. Bijvoorbeeld:

- het opmeten van gebieden (stedelijk of landbouwpercelen)
- het herkennen van landschapselementen
- het monitoren van biodiversiteit in een bepaald gebied
- het vastleggen van overstromingsgebieden
- het opsporen en/of analyseren van objecten, zoals detectie van ziektebeelden van ziektebeelden van gewassen of bomen
- het in kaart brengen van vervuiling, zwerfvuil en dumping
- het overzicht hebben bij een (calamiteiten)situatie en surveillance
- het detecteren van drenkelingen op zee of vermiste personen

Inspectie en onderhoud

Voor inspectie en onderhoud van objecten, zoals:

- nauwkeuriger onderhoud van dijken
- veiligere inspectie van bruggen en wegen
- (voorspellend) onderhoud van gebouwen
- controleren van gebouwen en verbouwingen (uitbouw, dakopbouw)
- het opsporen van illegale visfuiken, plantages

Aandachtspunt: wie is de opdrachtgever/opdrachtnemer?
Doorgaans zijn overheden opdrachtgever en marktpartijen opdrachtnemer, maar afhankelijk van de activiteiten/ werkzaamheden van een gebruikssituatie kan dit verschillen. Een overheidsorganisatie kan ook een gedeelte van het proces zelf uitvoeren (bijvoorbeeld zelf drones besturen). In dat geval kan de overheidsorganisatie voor die (deel)activiteiten dan ook als opdrachtnemer worden beschouwd. Met als gevolg dat daar bepaalde taken en aandachtspunten bij horen (zie verder in dit document per thema).

1.3 Context en ontwikkelingen

Dit hoofdstuk licht beknopt toe welke processtappen en instrumenten er zijn om van het verkrijgen van beeldmateriaal tot waardevolle informatie te komen. Daarna volgt de context van recente relevante wetgeving in dit werkveld en enkele ontwikkelingen ter achtergrondinformatie.

1.3.1 Over remote sensing en drones

Remote sensing gaat over het proces van het verzamelen en waarnemen van informatie over een object, gebied of fenomeen zonder direct fysiek contact te maken. Bij remote sensing worden sensoren gebruikt om te kunnen waarnemen vanaf een bepaalde afstand. Drones zijn een onderdeel daarin en zo zijn er ook instrumenten als satellieten, vliegtuigen, of sensoren op de grond. Drones worden hierbij steeds populairder vanwege hun vermogen om beelden met een hoge resolutie vast te leggen tegen lagere kosten en meer flexibiliteit[6].

Datasets gegenereerd vanuit de verschillende remote sensing instrumenten worden veelal gecombineerd, vergeleken, verrijkt of gebruikt bij metingen ter plaatse. Drones kunnen een breed scala aan data verzamelen; hoge resolutie images en video's maar ook andere soorten sensordata/-metingen zoals hyperspectraal opnames (o.a. warmtebeelden), liDAR-data (laser), en gas- en luchtkwaliteitsmetingen.

Bovenstaande remote sensing instrumenten ('op afstand observeren en beelden verkrijgen') omvatten een aantal functionele stappen om tot informatie te komen:

- *Instrumenten*: Er zijn verschillende soorten instrumenten die worden gebruikt bij remote sensing, zoals hierboven beschreven.
- *Communicatie*: Nadat de instrumenten de data hebben verzameld, moeten deze data worden verzonden naar computers of cloud. Dit wordt gedaan door middel van communicatieverbindingen.
- *Data*: Zodra de data zijn verzameld en overgedragen, worden deze data opgeslagen en verwerkt. De data die zijn verzameld door de instrumenten worden vaak in ruwe vorm ontvangen en moeten worden verwerkt om nuttige informatie op te leveren. Dataverwerking kan activiteiten omvatten zoals filteren, het corrigeren van eventuele ruis, en het omzetten van de data in bruikbare bestandsindelingen.
- *Informatie*: Deze informatiefase omvat het extraheren van zinvolle informatie uit de verwerkte data. Informatie-extractie kan een reeks technieken omvatten, waaronder beeldclassificatie, kenmerkextractie of bepaalde AI-analyses over een dataset.
- *Systemen*: De laatste fase is systeemintegratie. Dit omvat het integreren van de communicatie, data-, en informatiestromen in een systeem dat nuttige inzichten en analyses kan opleveren.

[6] Flexibiliteit in termen van 'waar' en 'wanneer' gegevens worden verzameld.

1.3.2 Over AI en algoritmen

Momenteel is er in Nederland geen algemeen geldige definitie van AI die consistent wordt gebruikt door alle belanghebbenden. In dit document gebruiken we vandaar de omschrijving van AI van de Europese Commissie, die is opgenomen in het Nederlandse Strategisch Actieplan AI[7]:

› **Artificiële Intelligentie (AI):** *AI verwijst naar systemen die intelligent gedrag vertonen door hun omgeving te analyseren en – met een zekere mate van zelfstandigheid – actie ondernemen om specifieke doelen te bereiken.*

Algoritmen zijn een onderdeel van AI. Er bestaan verschillende definities van wat onder een algoritme wordt verstaan. In deze marktvisie hanteren we een definitie voor algoritme die in lijn is met de 'Richtlijnen voor het toepassen van algoritmen door overheden'[8].

› **Algoritme:** *Een formule of stapsgewijze procedure, dat wordt uitgevoerd middels een computer, om een probleem op te lossen, een vraag te beantwoorden, een voorspelling te doen, een beslissing te nemen of die te ondersteunen.*

Een algoritme is niet meer dan een verzameling instructies die computers gebruiken om data te verwerken. Dat kan van relatief eenvoudig tot heel complex. In ICT-taal is het een instructie of een werkwijze, ofwel een stukje code, om een probleem om te lossen. Algoritmes helpen om op een snellere manier informatie te verwerken en om ingewikkelde keuzes te maken. Zie Bijlage 1 voor een overzicht van de diverse categorieën algoritmen die in te zetten zijn[9].

Aan de hand van data die door algoritme worden gebruikt, wordt in verschillende stappen toegewerkt naar het beoogde eindresultaat, zoals het herkennen van beelden.

Processtappen om met data-gedreven algoritmen tot resultaat te komen

De dataset, het algoritme, en het model zijn nauw met elkaar verbonden:

- Dataset is informatie die is verzameld, verwerkt en geanalyseerd om de ontwikkeling van het algoritme en het model te trainen.
- Een model is een vereenvoudigde representatie van een systeem of proces is die te gebruiken is om tot een resultaat te komen (zoals voorspellingen doen of conclusies trekken).

Volgordelijk ziet het er als volgt uit:
Dataset > algoritme > model > eindresultaat

[7] Zie Kamerstukken II 2018/19, 26643, nr. 640, pagina 9.

[8] Richtlijnen voor het toepassen van algoritmen door overheden en publieksvoorlichting over data-analyses. | Richtlijn | Rijksoverheid.nl

[9] Het overzicht uit Bijlage 1 komt uit de 'Quickscan AI in publieke dienstverlening, van TNO i.o.v. BZK, 2021: Quickscan AI in publieke dienstverlening II | Rapport | Rijksoverheid.nl

Een dataset wordt in een algoritme gestopt om een algoritme te trainen[10] en dat levert een model op. Dat model is daardoor alleen *bruikbaar* voor data die lijkt op de dataset waarmee het getraind is. Let wel; we zeggen hier nadrukkelijk bruikbaar. Het is uiteraard technisch gezien mogelijk om data die niet lijkt op de originele dataset in het model stoppen, maar de output (resultaat) van het model is dan in mindere mate (tot niet) valide.

Wat hierboven te zien is, is dat het proces begint met een dataset. Er is dus data nodig om überhaupt een model te kunnen maken. Dit kan problemen geven. Data kan niet beschikbaar zijn omdat we uitzonderlijke situaties willen detecteren waar weinig tot geen data beschikbaar voor is.

› *Voorbeeld: Als tijdens het inwinnen van beeldmateriaal een andere weersomstandigheid of invalshoek betreft dan waarop het model is gebaseerd, kan dit tot andere (mindere) uitkomsten leiden. Het is dus van belang om de specificaties van de trainingsdata te weten. Hoe beter (completer) het model met verschillende data is getraind, hoe beter de uitkomsten.*

Daarnaast: als de benodigde data onder de AVG valt dan is een ander probleem dat de data verkregen is voor een bepaald doel waardoor het niet zo maar voor trainingsdoeleinden mag worden gebruikt.

1.3.3 Wetgeving

Wetgeving op dronegebied

Door het kabinet zijn in 2019 ambities en uitdagingen benoemd voor de komende jaren[11]:

- borgen van de veiligheid (in de lucht, op de grond en privacy);
- benutten van de maatschappelijke toepassingen;
- benutten van de economische kansen voor Nederland.

In aanvulling daarop is in april 2023 een actualisatie van het Actieplan van het ministerie van Infrastructuur en Waterstaat naar de Tweede Kamer gestuurd.[12] Dat is een doorvertaling van de Luchtvaartnota[13]. De Luchtvaartnota benoemt specifiek de volgende onderwerpen als aandachtspunten voor de ontwikkeling van drones in Nederland:

1. veiligheid van drones;
2. beveiliging van data die verkregen is door vliegen met drones;
3. nieuw verkeersmanagementsysteem voor drones (U-space);
4. herindeling van het Nederlandse luchtruim (inclusief ruimte voor drones voor personen- en goederenvervoer);
5. ruimte voor nieuwe (duurzame) technologie.

Daarnaast heeft de Europese Commissie in november 2022 haar ‘dronestrategie 2.0’ aangenomen, met een visie op de verdere ontwikkeling van de Europese dronemarkt[14]. Voor ze verder gaat met de invoering van innovatieve technologie, wil de Commissie een maatschappelijk draagvlak voor drones garanderen. Burgers maken

[10] Trainen is het proces waarbij data in algoritmen wordt ingevoerd om zo het algoritme patronen en relaties in de data te laten leren.

[11] Bron: Drones in het publieke domein van beleid naar uitvoering (ministerie I&W, 02-2019).

[12] Kamerbrief bij Actieplan Programma Onbemande Luchtvaart 2023-2025 | Kamerstuk | Rijksoverheid.nl

[13] Ministerie van Infrastructuur en Waterstaat (2022). Luchtvaartnota 2020-2050.

[14] Bron: Naar een grootschalige Europese dronemarkt (europa.eu)

zich bij drones zorgen over lawaai, veiligheid en privacy. Daarom wordt in de strategie aan nationale, regionale en lokale besturen gevraagd om dronediensten af te stemmen op de behoeften van burgers.

AVG en doelbinding

De Algemene Verordening Gegevensbescherming (kortweg AVG) heeft relevante implicaties voor het gebruik van drones, vanwege het potentieel om persoonsgegevens te verzamelen en verwerken tijdens vluchten. Drones kunnen camera's en sensoren bevatten die beelden en andere gegevens van individuen vastleggen, zoals gezichten, locaties en gedragingen. Hierdoor valt de inzet van drones onder de reikwijdte van de AVG.

Houd rekening met de privacy principes van de AVG bij het inzetten van drones. Zo dient u als organisatie transparant te zijn over het doel en de aard van de gegevensverzameling, en toestemming verkrijgen van betrokkenen wanneer persoonsgegevens worden verwerkt. Daarnaast moeten er passende technische en organisatorische maatregelen worden genomen om de gegevens te beschermen en ervoor zorgen dat de bewaartermijnen in overeenstemming zijn met de AVG-voorschriften.

Doelbinding in het kader van de AVG (Algemene Verordening Gegevensbescherming) gaat over het principe dat persoonsgegevens alleen worden verzameld voor specifieke, legitieme en duidelijk omschreven doeleinden. Dit betekent dat organisaties die persoons-gegevens verwerken, de gegevens alleen mogen gebruiken voor het doel waarvoor ze zijn verzameld en geen verdere verwerking mogen uitvoeren die niet verenigbaar is met dat oorspronkelijke doel.

De toekomstige Europese AI verordening

De Europese Commissie bevordert de ontwikkeling van verantwoord gebruik van AI. Hiervoor heeft het een voorstel voor een Europese AI verordening opgesteld.

! *Op dit moment ligt de definitieve tekst van de AI Act nog niet vast. Zowel de Raad van de EU als het Europees Parlement hebben amendementen. De definitieve 'AI Act' treedt waarschijnlijk halverwege 2024 (of 2025) in werking. Daarna krijgen organisaties 2 jaar de tijd om de nieuwe wet te implementeren.*

Over de AI Act en 'hoog risico' AI-systemen[15]

De AI Act richt zich vooral op AI-systemen met een hoog risico. Een AI-systeem krijgt het stempel 'hoog risico' als het valt onder bepaalde 'toepassingen' of 'categorieën'. Toepassingen op het vlak van AI beeldherkenning met drones vallen *over het algemeen* binnen deze classificering[16]. De AI Act vereist dat hoog-risico AI-systemen voldoen aan een aantal nieuwe verplichtingen, om ervoor te zorgen dat ze veilig en transparant zijn en geen onaanvaardbare risico's voor mensen opleveren. Er is onderscheid in twee soorten 'hoog risico':

- Lijst 1) AI toepassingen met een hoog risico waarvoor *self assessment* verplicht is;
- Lijst 2) AI toepassingen met een hoog risico die door een externe instantie op conformiteit getoetst moeten worden.

[15] Bronnen: Autoriteit Persoonsgegevens Inzet Artificial Intelligence Act (maart 2022), Presentatie PelsRijcken over Contracteren van AI (november 2022), en Kennisnet (juni 2023).

[16] Zie hiertoe artikel 6 van (huidige concept) AI Act.

Wanneer een algoritme of AI dat door een overheid wordt ingekocht mogelijk als 'hoog risico' zal kwalificeren, is advies in dat geval reeds nu afspraken te maken met de leverancier waarin wordt voorgesorteerd op de AI Act. Daarbij kan worden gedacht aan zaken als een systeem voor risicobeheer, kwaliteitscriteria voor data en databeheer, technische documentatie, registratie van logs, transparantie en informatieverstrekking aan gebruikers/overheidsorganisatie, menselijk toezicht, en mogelijk uitvoeren conformiteitsbeoordeling.

De gebruiker/overheidsorganisatie hebben ook verplichting, zoals AI-systemen gebruiken in overeenstemming met de gebruiksaanwijzing, zorgen dat de inputdata relevant en voldoende representatief is voor het beoogde doel, menselijk toezicht uitoefenen op het AI-systeem, logbestanden bewaren, personen informeren over wie besluiten worden gemaakt met behulp van AI, en een Fundamental Rights Impact Assessment (FRIA) uitvoeren (dit komt naast de verplichting van een DPIA wanneer persoonsgegevens worden verwerkt).

Binnen de verschillende thema's in de marktvisie van de Buyer Group worden er aspecten over bovenstaande opsomming belicht, zie daartoe hoofdstuk 3.

1.3.4 Enkele ontwikkelingen

De volgende opsomming en toelichting op ontwikkelingen dienen ter inspiratie en achtergrondinformatie, om een beeld te geven wat er onder andere op dit vlak plaatsvindt en wordt ondernomen.

Drone-as-a-service (DaaS) en drone in a box

We zien op dit moment nieuwe business modellen in ontwikkeling; zoals Drone-as-a-Service (DaaS). Een dergelijke service geeft toegang tot drones en het verkrijgen van beeldmateriaal, zonder zelf hardware en software aan te schaffen en te onderhouden. DaaS-providers bieden doorgaans een scala aan drone gerelateerde services, waaronder het vastleggen, verwerken en analyseren van gegevens, evenals droneverhuur, training van piloten en naleving van regelgeving.

Een andere ontwikkeling is 'Drone in a box', dat verwijst naar een soort systeem dat bestaat uit een drone én een grondstation dat dient als oplaad- en dockingstation voor de drone. Het concept is qua omvang te vergelijken met een verhuisdoos, waaruit de drone autonoom kan opstijgen en landen en het wordt opgeladen wanneer deze niet in gebruik is.

Initiatieven en samenwerkingen

In de afgelopen jaren zien we verschillende pilots en demonstratie-projecten met drones uitgevoerd door kennisinstituten, marktpartijen en overheden. Dit heeft geleid tot diverse innovatiecentra en kennisclusters, waarvan we enkele initiatieven benoemen:

- *Drone2go*: Drone2Go is een innovatief samenwerkingsproject van Rijkswaterstaat met de politie, brandweer, ILT Aerosensing en de Nederlandse Voedsel- en Waren Autoriteit. Het project Drone2Go is bedoeld om de ontwikkeling van autonome drones te stimuleren en werkt toe naar een landelijk dekkend netwerk van autonome drones. Dit doen ze samen met de markt en kennisinstellingen.

- *Drone Netwerk Gemeenten*: Een groep gemeenten[17] hebben het initiatief genomen om hun samenwerking op het gebied van drones te bundelen en nodigen andere gemeenten uit om zich aan te sluiten. In hun Manifest (2022) zijn drie doelen geformuleerd: het vergroten van bewustzijn onder ambtenaren en bestuurders, het onderzoeken van de kennisbehoefte van gemeenten, en het creëren van een centraal aanspreekpunt waar vragen en informatiestromen bij elkaar komen.
- *NLR drone center*: Het Nationaal Lucht- en Ruimtevaart-laboratorium (NLR) heeft eind 2015 het NRTC (Netherlands RPAS Test Centre) opgezet. Hier worden testen en evaluaties van prototypes en sensortoepassingen uitgevoerd, demonstraties gefaciliteerd, vluchtinspecties uitgevoerd en praktijktrainingen en technische keuringen gegeven. Het NRTC beschikt over een eigen luchtruim met ruimere bevoegdheden, om bijvoorbeeld te mogen vliegen met prototypes die nog niet aan alle eisen voldoen. Het NRTC is gevestigd op de testfaciliteit van NLR in Flevoland.
- *Unmanned valley*: Op een voormalig marinevliegkamp ligt dit fieldlab voor sensorgerelateerde technologieën en toepassingen. Het is een plek voor startups, scale-ups, gevestigde bedrijven, kennisinstellingen en overheden om drones en andere sensor-based innovaties te onderzoeken, ontwikkelen en testen.
- *Space53*: Deze stichting bundelt overheden, kennisinstellingen, hulpverleners en bedrijven tot drone-innovatiecluster en versterkt het ecosysteem door het creëren van de randvoorwaarden voor succesvolle ontwikkeling en toepassing van onbemande systemen.

1.4 Vooraf enkele randvoorwaarden en onderliggende overtuigingen

Wanneer er gesprekken zijn over AI beeldherkenningstechnologie en drones – zeker in de context van overheden – komen regelmatig een aantal onderliggende overtuigingen naar voren die (op dit moment) als belangrijk worden bevonden.
Op basis van ervaringen van deelnemers van de Buyer Group komen we tot de volgende punten:

- Zorg voor inzicht in wat de AI-technologie alsook de drone uitvoert en communiceer dit. Wees daarbij helder in hoe die technologie werkt en tot resultaat komt. Bijvoorbeeld hoe algoritmen bepaalde beelden/situaties herkent, of op basis van welke werkwijze er tot resultaat is gekomen (zoals wat de vliegroute van drone is). Per gebruikssituatie en per doelgroep verschilt het in welke mate die helderheid gewenst is[18].
- Laat gebruikers op de eerste plaats komen. Van belang is dat de technologieën als hulpmiddel worden gezien, waarbij de mens centraal staat in het toepassen ervan. Dat de technologie gericht is op het versterken van menselijke capaciteiten (bijvoorbeeld bij het herkennen van haarscheurtjes in bruggen), waarbij er een menselijke stap of validatie onderdeel is.
- Werknemers die de technologieën inzetten bij hun werkzaamheden, horen ook te begrijpen hoe het 'onder de motorkap' werkt. Dit pleit er voor om ook interne medewerkers voldoende op te leiden, als een publieke organisatie met deze digitale innovaties aan de slag wil.
- Ga op een veilige manier met de data om.

[17] De huidige initiatiefnemers zijn: Amsterdam, Apeldoorn, Den Haag, Enschede, Heerlen, HLT-Samen, Molenlanden en Rotterdam.

[18] De complexiteit van automatische verwerking van drone-gegenereerde beeldmateriaal kan per situatie variëren; het is elke keer maatwerk in welke zin helderheid gewenst is per doelgroep. Zie hoofdstuk 1.2 voor enkele voorbeelden van gebruikssituaties.

- Vorm vanaf de allereerste fase van het traject een kundig projectteam met verschillende specialisaties. Denk onder andere aan: Chief Information Security Officer of Chief Information Officer, data scientist, databeheerder, domeinexpert/materiedeskundige, functionaris gegevensbescherming, jurist, inkoopadviseur, en een communicatieadviseur die kan meedenken met adviseur ethiek.

Daarnaast merkt de Buyer Group op dat tijdens gesprekken en in (nieuws)artikelen/reportages over AI en drones, regelmatig de mogelijke risico's de boventoon voeren die de nieuwe technologieën met zich mee brengen. Daardoor kan er een terughoudendheid zijn om met deze digitale innovaties aan de slag te gaan en erover te communiceren. Des te meer reden voor het inzetten op verantwoord gebruik van deze technologieën, zoals de Buyer Group met deze marktvisie voor ogen heeft.

2 VISIE VAN DE BUYER GROUP

Waar wij voor staan

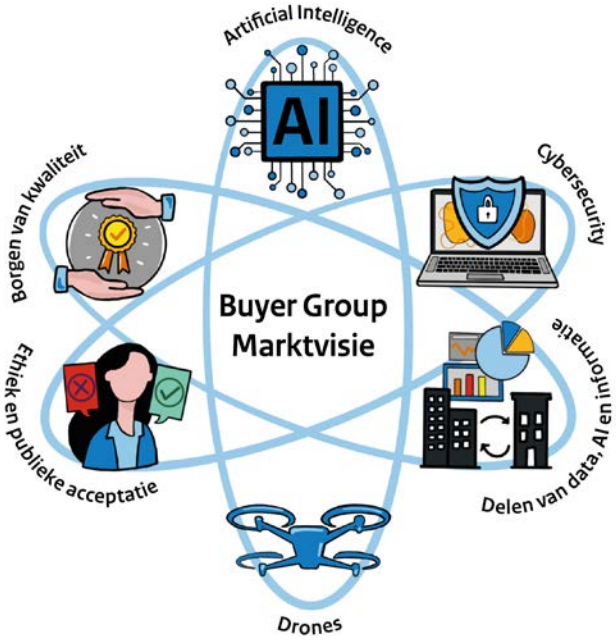
Bij publieke organisaties spelen diverse vraagstukken waar meerwaarde te halen is uit informatie via beeldherkenning en specifiek door middel van drones.

› *Deze Buyer Group wil de innovatieve technologie op een verantwoorde manier toepassen en inzetten voor een betere kwaliteit van de publieke dienstverlening en efficiëntere uitvoering van de publieke taken.*

Waar wij voor gaan

De kennis en ervaring met betrekking tot AI en drones is volop in ontwikkeling. We geloven in de kracht van deze digitale technologieën om publieke taken te verbeteren en we willen er op verantwoorde manier mee innoveren. We kunnen overheden laten zien dat het automatisch verwerken van beeldmateriaal dat verkregen is door remote sensing, zoals met drones, veel potentie heeft[19].

We beogen dat de mogelijkheden die drones bieden om meer, frequentere en nieuwe waarnemingen te verkrijgen, wordt benut en we er digitaal mee innoveren. Op die manieren kunnen we digitale technologieën inzetten om waardevolle nieuwe producten en diensten te (laten) ontwikkelen voor publieke taken. Opdat we de toegevoegde waarde van AI-beeldherkenningstechnologie en drone-technologie ten volle benutten op een verantwoorde manier.



De marktvisie van de Buyer Group is opgebouwd uit vier thema's:

- Borgen van Kwaliteit
- Cybersecurity
- Delen van data, AI en informatie
- Ethiek en publieke acceptatie

Daaronder vallen een aantal uitgangspunten die we willen bereiken:

[19] Remote sensing is het van een afstand observeren en beelden maken. Dat kan grote oppervlakten bestrijken zoals vanuit een satelliet, of kleinere oppervlakten of objecten met een drone.

Borgen van kwaliteit

- Het toepassen van een meer eenduidige aanpak in de levenscyclus van projecten door de overheid om de kwaliteit te waarborgen.
- Het betrekken van gebruikers als essentieel onderdeel van het proces bij het gebruik van AI om de kwaliteit te verbeteren.
- Het faciliteren van de ontwikkeling en implementatie van algoritmen door het hanteren van open standaarden.
- Het periodiek evalueren en verbeteren van de kwaliteit van projecten om te zorgen voor een blijvend hoog niveau van kwaliteit en prestaties.

Cybersecurity

- Het vergroten van het bewustzijn rondom cybersecurity door middel van o.a. educatie en voorlichting.
- Het stimuleren van een proactieve rol van zowel opdrachtgevers als opdrachtnemers in het waarborgen van cybersecurity.
- Het implementeren van gestandaardiseerde beveiligingsvoorwaarden, afhankelijk van de gebruikssituatie, voor opdrachtnemers van overheidsinstanties.
- Het regelmatig updaten en evalueren van de cybersecurity maatregelen om te zorgen voor een blijvend hoog niveau van bescherming tegen cyberdreigingen.

Delen van data, AI en informatie

- We onderschrijven het principe van "één keer verzamelen, meerdere keren gebruiken", binnen de mogelijkheden die doelbinding biedt (hierin is AVG bepalend).
- De overheid wil meer openheid over wat zij doet. De visie van het kabinet is: ‘openbaar tenzij’. Met als uitgangspunt dat overheidsinformatie openbaar gedeeld wordt, conform de Wet hergebruik overheidsinformatie (Who).
- Het gemakkelijk toegankelijk beschikbaar stellen van data, AI en informatie komt een meer datagedreven en innovatieve samenleving ten goede.

Ethiek en publieke acceptatie

- Het hanteren van het ethische perspectief als basishouding bij de opzet en uitvoering van AI-projecten, in lijn met de beleidslijn van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.
- Het waarborgen van transparantie en betrouwbare AI.
- Het betrekken van het publiek tijdens (de ontwikkeling van) AI beeldherkenning met drone projecten.
- Het opstellen en uitvoeren van een communicatiestrategie gericht op het verbeteren van de beeldvorming en het vertrouwen rondom AI beeldherkenning met drone projecten.




BORGEN VAN KWALITEIT

STRATEGIE PER THEMA: HOE ER TE KOMEN?

3 STRATEGIE PER THEMA: HOE ER TE KOMEN?

3.1 Het borgen van kwaliteit

Wat is onze ambitie

Wij willen een eenduidige aanpak in het borgen van kwaliteit bij projecten met AI beeldherkenningstechnologie door de overheid. Hierin staat de levenscyclus van een algoritme centraal. Daarbij is van belang om gebruikers te betrekken, open standaarden te hanteren en periodiek te evalueren om voor een hoog niveau van kwaliteit en prestaties te zorgen.

Levenscyclus van een algoritme

Een duidelijk beeld van de levenscyclus van een algoritme zorgt er voor dat het algoritme op een gestructureerde manier wordt ontwikkeld en dat het voldoet aan de noodzakelijke prestatienormen en -vereisten.

De levenscyclus is een iteratief proces en bestaat uit een viertal stadia. Deze zijn op hoofdlijnen op de volgende pagina weergegeven en beknopt toegelicht.

Er is een aantal manieren waarop *dieper* inzicht te krijgen is in levenscyclus, zoals met Explainable AI (XAI) machine learning technieken die helpen om inzicht te geven in welke informatie een model gebruikt om voorspellingen te verklaren.
Verder is een goed CI/CD (Continuous Integration/Continuous Deployment) proces een belangrijk element, zoals dat ook bij andere software trajecten is.

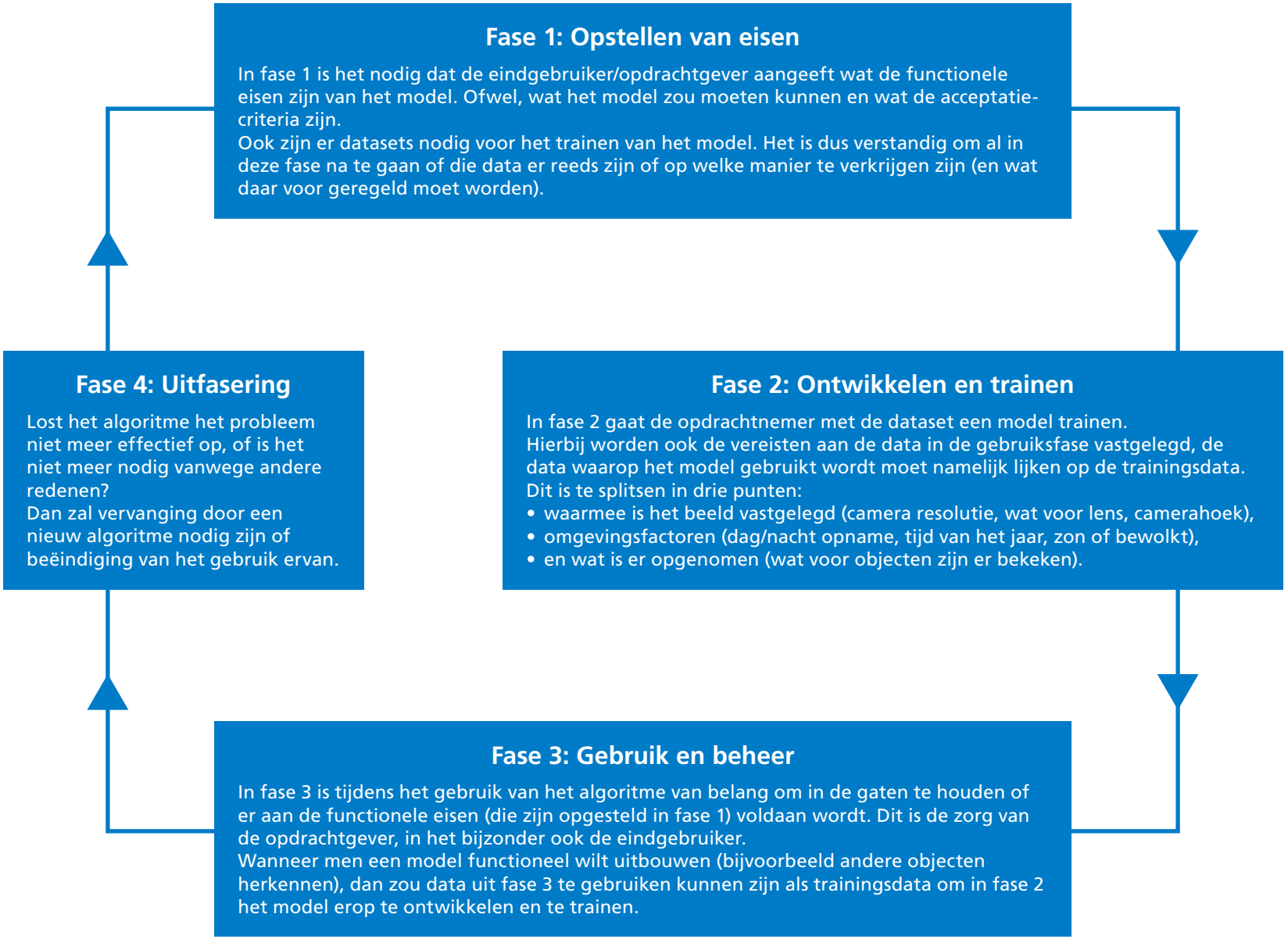
Gebruikers

Tijdens de levenscyclus is het van belang om na te denken over de rol en type van de gebruikers(groepen): dit in relatie tot de nauwkeurigheid, het gebruik van het informatieproduct en gedurende de ontwikkeling van een AI-algoritme.
Om te voorkomen dat de werking van een algoritme of de kwaliteit van data vanzelfsprekend wordt, is het nodig om de 'menselijke' stap of validatie (al is het maar steekproefsgewijs) altijd een onderdeel te laten zijn van het gebruik van data en algoritmes. Zodat er na verloop van tijd- niet blind gevaren wordt op de geproduceerde resultaten.
Houd daarom ook in het interface ontwerp van een softwaresysteem/ toepassing rekening met de mensgerichte interactie, ten behoeve van de beoogde gebruiker.

Open standaarden

Een open standaard heeft betrekking op de specificatie van de taal die computers onderling spreken. Een standaard is een afspraak die is vastgelegd in een specificatiedocument. Om gegevens uit te wisselen moeten ICT-systemen dezelfde standaard hanteren[20]. Het gebruik van open standaarden biedt in de levenscyclus dat verschillende algoritmen op een consistente en toegankelijke manier te ontwikkelen en gebruiken zijn. Dit is relevant wanneer algoritmen worden gebruikt in systemen die moeten samenwerken of data uitwisselen. Anders gezegd, open (data) standaarden zorgen er voor dat verschillende algoritmen en AI-systemen met elkaar kunnen communiceren en functioneren met elkaar. Zie ook hoofdstuk 3.3 voor meer toelichting.

[20] Zie voor verdere uitleg over kenmerken van 'open standaarden' de informatie van Forum Standaardisatie: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/open-standaarden/


Fase 1: Opstellen van eisen
In fase 1 is het nodig dat de eindgebruiker/opdrachtgever aangeeft wat de functionele eisen zijn van het model. Ofwel, wat het model zou moeten kunnen en wat de acceptatie-criteria zijn.
Ook zijn er datasets nodig voor het trainen van het model. Het is dus verstandig om al in deze fase na te gaan of die data er reeds zijn of op welke manier te verkrijgen zijn (en wat daar voor geregeld moet worden).
Fase 2: Ontwikkelen en trainen
In fase 2 gaat de opdrachtnemer met de dataset een model trainen.
Hierbij worden ook de vereisten aan de data in de gebruiksfase vastgelegd, de data waarop het model gebruikt wordt moet namelijk lijken op de trainingsdata.
Dit is te splitsen in drie punten:
• waarmee is het beeld vastgelegd (camera resolutie, wat voor lens, camerahoek),
• omgevingsfactoren (dag/nacht opname, tijd van het jaar, zon of bewolkt),
• en wat is er opgenomen (wat voor objecten zijn er bekeken).
Fase 3: Gebruik en beheer
In fase 3 is tijdens het gebruik van het algoritme van belang om in de gaten te houden of er aan de functionele eisen (die zijn opgesteld in fase 1) voldaan wordt. Dit is de zorg van de opdrachtgever, in het bijzonder ook de eindgebruiker.
Wanneer men een model functioneel wilt uitbouwen (bijvoorbeeld andere objecten herkennen), dan zou data uit fase 3 te gebruiken kunnen zijn als trainingsdata om in fase 2 het model erop te ontwikkelen en te trainen.
Fase 4: Uitfasering
Lost het algoritme het probleem niet meer effectief op, of is het niet meer nodig vanwege andere redenen?
Dan zal vervanging door een nieuw algoritme nodig zijn of beëindiging van het gebruik ervan.

Praktische invulling van de ambities

Om grip te krijgen op de ambities ziet de Buyer Group de volgende werkzaamheden terugkomen bij projecten op het vlak van AI beeldherkenning met drones. Daarbij lichten we processtappen per fase van de levenscyclus toe:

Werkzaamheden in Fase 1

› *Bepalen van het doel en het opstellen van eisen:*
Overweeg allereerst of de inzet van een algoritme zinvol is. Beschrijf samen met de gebruikers het probleem dat het algoritme/AI-systeem moet oplossen, waarvoor toepassing van AI beeldherkenning met drones nodig is. Richt verder als opdrachtgever een kundig projectteam in[21]: dat team bespreekt en benoemt de vereisten en voorwaarden waaraan moet worden voldaan om de algoritmen correct te laten functioneren. Daarbij kan het bijvoorbeeld gaan om de beschikbaarheid van bepaalde data of bronnen, of eventuele beperkingen voor het algoritme.

Let op: Het is aan de overheidsorganisatie om na te gaan welke van de beschreven werkzaamheden door interne medewerkers in het projectteam te realiseren zijn en bij welke activiteiten externe expertise voor nodig is. Dit kan elke keer afhangen van het specifieke product/dienst die wordt ingekocht, de specifieke gebruikssituatie en de kennis en ervaring die intern beschikbaar is.

De keuze van het AI-algoritme hangt af van de specifieke beeldherkenningstaak die wordt uitgevoerd. Er zijn verschillende vormen en soorten waarbij beeldherkenning algoritmen en AI-oplossingen kunnen worden ingezet in modellen om informatieproducten te ontwikkelen. Zoals bijvoorbeeld: Neurale netwerken, Support Vector Machines, Decision Trees, Random Forests, Deep Belief Networks, Generative Adversarial Networks. Het is daarom van belang om de juiste kennis en kunde aan tafel te hebben bij het opzetten van de beoogde levenscyclus.

Werkzaamheden in Fase 2

› *Het ontwerpen, ontwikkelen, trainen en testen van het algoritme:*
De opdrachtnemer zet het algoritme op en traint met behulp van een reeks gegevens en bronnen. Dit kan het schrijven van code inhouden om het algoritme te implementeren en de benodigde datastructuren of variabelen te configureren. Wees als opdrachtgever bewust van de diverse keuzes in de methodiek[22] die hierbij een rol kunnen spelen. In ideale situatie testen opdrachtnemer in samenspraak met opdrachtgever het algoritme vervolgens met behulp van een reeks testcases om de kwaliteit en prestaties te evalueren.

- Houd als opdrachtgever zeggenschap over de levenscyclus van een algoritme: wees ‘in control’ en kies bij voorkeur voor de AI-metriek die het meest eenvoudig is.
- Laat een (intern) inhoudelijk deskundige/materiedeskundige de kwaliteit verifiëren.

[21] Zie hoofdstuk 1.4 voor voorbeelden van specialisaties.

[22] Zie Bijlage 1 voor een overzicht van de diverse categorieën algoritmen die in te zetten zijn.

Werkzaamheden in Fase 3

› *Het gebruiken en in beheer nemen van een algoritme:*
Het is belangrijk dat opdrachtnemer het algoritme blijft testen om ervoor te zorgen dat het blijft presteren zoals verwacht en om mogelijke problemen te identificeren.

Train en werk het model tijdens de levensduur periodiek bij, om te voorkomen dat er een bepaalde bias wordt ontwikkeld waardoor modellen mogelijk niet meer nauwkeurig zijn ('concept drift'). Hierbij hoort periodieke validatie, op basis van nieuw materiaal. Het is van belang dat er goed gedocumenteerd wordt, zoals hoe data verzameld wordt en hoe geannoteerd. Om zo de samenstelling en kwaliteit van de data te controleren die wordt gebruikt om de modellen te trainen, en ook de uitkomsten van de modellen voor verscheidene subgroepen.

Als het algoritme niet naar verwachting presteert of als de eisen/voorwaarden van het probleem veranderen, kan het nodig zijn om het algoritme aan te passen om de prestaties te verbeteren of om het aan te passen aan de nieuwe omstandigheden. Dit kan het wijzigen van de code inhouden of het bijwerken van de gegevens die worden gebruikt om het algoritme te trainen. Het beheer van algoritmen en 'feedbackloops' zijn in deze fase een belangrijke activiteit, want op die manier is voortdurende monitoring en verbetering van het systeem te realiseren.

Laat de ontwikkeling van het algoritme gefaseerd gaan, waarbij de opdrachtnemer op hoofdlijnen belicht hoe de fases van de ontwikkeling ondervangen zijn. Zorg er voor dat de publieke opdrachtgever de mogelijkheid heeft terug te kunnen naar de vorige fases (go/no-go moment).

Werkzaamheden in Fase 4

› *Het algoritme uit faseren:*
Wanneer een algoritme een probleem niet meer effectief oplost, of niet meer nodig is vanwege andere redenen, neemt opdrachtgever met projectteam de beslissing hoe verder te gaan (nieuw algoritme of beëindiging van het gebruik). Overleg met dit ook met relevante betrokkenen en houdt daarbij rekening met de kosten en baten van het blijven gebruiken van het algoritme ten opzichte van vervanging ervan.

Aandachtspunten voor de samenwerking en eisen aan opdrachtnemer

- Bespreek wie op welk moment verantwoordelijk is:
  - Uit de marktconsultatie kwam naar voren dat partijen het logisch vinden en verwachten dat opdrachtgever de norm/prestatiecriteria (ondergrens van nauwkeurigheid) stelt waaraan het resultaat moet worden voldaan. Alsook dat opdrachtgever de uiteindelijke beslissing neemt of de uitkomsten van het model voldoende zijn om mee te handelen evenals op welke wijze het wordt ingezet (eventueel bij gevoelige gebruikssituaties er menselijke controle bij inbouwt).
  - Tegelijkertijd is de opdrachtnemer verantwoordelijk om duidelijk over te brengen wat haalbaar is en te informeren over de mogelijke afwijkingen. De verantwoordelijkheid voor het valideren van processtappen in de ontwikkelfase ligt doorgaans bij de opdrachtnemer. Immers het valideren van de algoritmen behoort onderdeel te zijn van het verificatie en validatieproces dat een opdrachtnemer doorloopt, om ervoor ter zorgen dat het algoritme voldoet aan de specificaties en vereisten van de opdrachtgever.

  - In de ideale situatie is dit een samenspel, zodat opdrachtnemer samen met opdrachtgever bekijkt welke data nodig is voor een goede validatie door een aantal representatieve gebruikssituaties te definiëren.
- Het (juridisch) borgen van de kwaliteit kan door KPI's[23] vast te leggen waaraan het algoritme dient te presteren. De afwegingen die in het ontwikkelproces worden gemaakt, dienen door het team vastgelegd te worden in een logboek. Daarbij moet de kanttekening worden geplaatst dat een (AI) model een benadering is van de werkelijkheid, en deze zal nooit 100% accuraat, volledig of nauwkeurig zijn.
- Zorg tijdens de looptijd van het contract voor onderhoud en ondersteuning om kwaliteit te borgen: algoritmen en datasets kunnen doorlopend onderhoud en ondersteuning nodig hebben om ervoor te zorgen dat ze goed blijven functioneren en voldoen aan de behoeften van de organisatie. Een toekomstbestendig contract kan bepalingen bevatten die de verantwoordelijkheden van de partijen bij het bieden van dergelijk onderhoud en ondersteuning schetsen.
- Overheden zijn verplicht om, bij aanschaf van ICT-producten of ICT-diensten van € 50.000,- of meer, te vragen naar relevante standaarden die zijn voorgeschreven op de 'Pas toe of leg uit'-lijst.
- De nauwkeurigheid en bewaking van een AI-systeem wordt bepaald aan de hand van acceptatiecriteria voor zowel de data-input, evenals voor het bepalen van het prestatievermogen van de output die het model produceert[24]. Dit kan daarnaast overwegingen omvatten zoals labelnauwkeurigheid, datakwaliteit en relevantie voor de betreffende taak. Bedenk hierbij dat elke toepassing maatwerk vereist.
- Onthoud dat het laten bouwen en het gebruik van een informatieproduct met AI-component een proces van productontwikkeling bevat waarbij naast technische mogelijkheden ook het 'Human design' een aspect is. Anders gezegd: technisch kan iets te ontwikkelen zijn maar blijft het product ook op de werkvloer werkbaar (voor bijvoorbeeld een controleur of inspecteur).
- Zorg dat een 'menselijke' stap of validatie, al is het maar steekproefsgewijs, altijd (ook in de jaren erna) onderdeel blijft van het gebruik van data en algoritmes. Grijp op tijd in als er twijfel is.
- Blijf ervan bewust dat materiedeskundigheid geborgd blijft, iemand met de juiste expertise/opleiding die uitkomsten van een AI model kan beoordelen. Deze persoon kan ofwel aan opdrachtgeverskant danwel aan de opdrachtnemerskant zitten.
- Opdrachtnemer dient periodiek de data te valideren, op basis van nieuw materiaal.
- Veranderingen in de technologie of industrie: het gebied van kunstmatige intelligentie (AI) en datawetenschap evolueert voortdurend en het is waarschijnlijk dat er in de loop van de tijd nieuwe technologieën en best practices zullen ontstaan.
  - Opdrachtnemer stelt de opdrachtgever op de hoogte wanneer nieuwe technische ontwikkelingen opkomen die relevant zijn voor de gebruikssituatie.
  - De opdrachtnemer handelt alle opdrachten af en verricht alle werkzaamheden conform de *stand der techniek* ten tijde van de opdrachtverlening.
- Neem in het contract bepalingen op die updates of wijzigingen mogelijk maken als dat nodig is. Via zogenoemde herzieningsclausules kunt u voorkomen dat een wezenlijke wijziging van de oorspronkelijke opdracht en heraanbestedingsplicht ontstaat.

[23] Wat het gewenste resultaat is en wat de ondergrens van de nauwkeurigheid van het algoritme mag zijn.

[24] Zie voor verdere uitleg over acceptatiecriteria, pagina 10 van AI Impact Assessment | Rapport | Rijksoverheid.nl

- Datalevering:
  - Doorgaans ontvangt de opdrachtgever de trainingsgegevens en het model of alleen de resultaten van het model. Als de opdrachtgever de trainingsgegevens en het model ontvangt, is meestal het model te gebruiken om voorspellingen te doen over nieuwe gegevens. Ook maakt dit het omschakelen tussen AI partijen eenvoudiger.
  - Zorg ervoor dat de data die ten grondslag ligt aan de training van het AI-model onder diverse omstandigheden is 'opgenomen'. Waarbij de eindgebruiker ten tijde van training daarbij betrokken is, zodat het model zo volledig/robuust mogelijk wordt getraind.
  - Net als bij andere IT-projecten, denk bij het inkopen van software met AI/algoritmen na over de vraag: hoe staan we ervoor als de overeenkomst afloopt?[25]

Graag wijzen we op de 'Modelbepalingen voor gemeenten voor verantwoord gebruik van Algoritmische toepassingen', die in opdracht van gemeente Amsterdam en verschillende samenwerkingspartners in Nederland zijn ontwikkeld met subsidie van het Ministerie van BZK.
De modelbepalingen zijn vrij te gebruiken en is op de website inclusief een toelichtingsdocument beschikbaar gesteld.

De modelbepalingen bieden een standaard set van mogelijke contractvoorwaarden die te hanteren zijn. Waaronder ook over de kwaliteit van de algoritmische toepassingen, zie ter inspiratie artikel 4 daaruit:

"4.1. Opdrachtnemer verklaart dat de Algoritmische toepassing is ontwikkeld en functioneert op een wijze die in overeenstemming is met wet- en regelgeving.
4.2. Opdrachtnemer verklaart dat de Algoritmische toepassing volgens een gemotiveerde aanpak is ontwikkeld.
4.3. Opdrachtnemer verklaart dat de Algoritmische toepassing nauwkeurig en correct functioneert.
4.4. Opdrachtnemer verklaart dat de Algoritmische toepassing geschikt is voor het Beoogde gebruik."

In navolging heeft ook de Europese Commissie een (uitgebreidere) vervolgversie beschikbaar gesteld: een set voor AI-toepassingen met hoog-risicoprofiel en een set voor AI-toepassingen met laag-risicoprofiel. Deze zijn zo opgesteld dat ze als bijlage kunnen worden toegevoegd aan een contract waarin reeds andere onderwerpen (zoals intellectueel eigendom, acceptatie, betalingen of aansprakelijkheid) al zijn vastgelegd.

[25] Zie hoofdstuk 3.3. over het delen van data, met meer aandachtspunten en verwijzing naar ARBIT/GIBIT.




CYBERSECURITY

STRATEGIE PER THEMA: HOE ER TE KOMEN?

STRATEGIE PER THEMA: HOE ER TE KOMEN?

3.2 Cybersecurity

Wat is onze ambitie

Cybersecurity met betrekking tot AI-beeldherkenning met drones beslaat een keten. Bij acties in deze keten (zie ook hoofdstuk 1.3.1) is het van belang om na te gaan of dat dit op een digitaal veilige manier gebeurt. Het gaat daarbij met name om:

- Cybersecurity ten aanzien van communicatie tussen systemen en tussen drones en computer.
- Cybersecurity van de opslag van de data. Zoals ervoor zorgen dat er voor regelmatige back-ups van de data is om te kunnen herstellen in geval van een cyberaanval of een andere storing.
- Cybersecurity bij de bewerking en verwerking van data. Te denken valt aan enkel toegang tot (bepaalde) data door geautoriseerde gebruikers. En afhankelijk van de gevoeligheid van de gebruikssituatie, een versleuteling van data om te beschermen tegen onbevoegde toegang.

Wij willen binnen deze keten een proactieve rol van zowel opdrachtgevers als opdrachtnemers in het waarborgen van cybersecurity stimuleren. De Buyer Group wil het bewustzijn rondom cybersecurity daarom vergroten en ziet een belangrijke rol voor educatie en voorlichting. Om te zorgen voor een blijvend hoog niveau van bescherming tegen cyberdreigingen zien we het belang van het regelmatig updaten en evalueren van securitymaatregelen en het implementeren van gestandaardiseerde beveiligingsvoorwaarden, (afhankelijk van de gebruikssituatie) voor opdrachtnemers van overheidsinstanties.

3.2.1 Verantwoording bij opdrachtnemer en opdrachtgever

Voor effectieve risicoanalyse van functionele, technische en organisatorische eisen is het essentieel dat de opdrachtgever (overheid) meedenkt en meewerkt met de opdrachtnemer. Het inschatten van risico's zijn een belangrijk onderdeel van informatiebeveiliging. Dit zijn niet alleen risico's van de opdrachtnemer, maar ook de risico's vanuit het gezichtspunt van de opdrachtgever, en waar tevens de opdrachtgever ook het beste zicht op heeft. Opdrachtgevers dienen een inventarisatie te hebben gedaan voor de aanbesteding over welk niveau van informatiebeveiliging van toepassing is. Daarbij is van belang dat opdrachtgever bij risicoanalyse de materiedeskundige personen betrekt.

3.2.2 Bewust en bekwaam

Het is van belang dat gebruikers bewust zijn dat hun gedrag een zeer belangrijke schakel is in het veilig houden van de gebruikte IT-systemen. Het gaat erom dat men doorkrijgt wat de risico's zijn op het gebied van cybersecurity, dit vergt een bepaalde kennis en oordeel van een situatie. De Buyer Group deelnemers vinden het daarom een randvoorwaarde dat de betrokkenen die werken met beeldherkenning/drones zich realiseren welke beveiligingsrisico's gepaard gaan met deze technologieën. Dit geldt voor zowel eigen medewerkers alsook aan de kant van de opdrachtnemer. Om dit te bewerkstelligen is gerichte interne kennisdeling, opleiding en communicatie nodig.

- Zo kunt u gebruikersessies organiseren rond het thema informatiebeveiliging.
- Ten aanzien van bekwaamwording is (basis) kennisopbouw nodig. Alle betrokkenen bij het project moeten op de hoogte

zijn van de regels en procedures en deze ook doorleven[26]. Het is van belang om deze kennis te onderhouden, afhankelijk van de rollen en functies van de medewerker, aangezien de wereld rondom cybersecurity aan verandering onderhevig is. Voor de kennisopbouw en het onderhouden ervan bestaan diverse middelen. Zoals e-learnings, het inzetten van een ethische hacker, en ransomware-simulaties (waarbij een gebruiker echt het gevoel heeft en schrikt omdat het lijkt dat er op dat moment gehackt wordt).
- Verder is het belangrijk dat organisaties lid zijn van de gebruikersgroepen op de diverse fora, zodat er kennis is van nieuwe bedreigingen.
- Een andere aanbeveling is om periodieke (contract)management overleggen te beleggen waarin informatiebeveiliging een vast thema is op de agenda. Hier kunnen gewenste veranderingen op het gebied van informatiebeveiligingsnormen besproken worden.

3.2.3 Standaardisatie

Voor een effectieve en efficiënte samenwerking van IT-systemen is gelijkgestemde informatiebeveiliging van de automatisering essentieel.

Standaardisatie van beveiligingsvoorwaarden is hierbij een belangrijk onderdeel. Standaardisering in aangekochte diensten/producten vergemakkelijkt een onafhankelijke beoordeling/audit op het vlak van security. Zo kunnen risico's in kaart worden gebracht met analyses en inventarisatie van externe koppelvlakken. Hierbij kan een PDCA cyclus gehanteerd en ingericht worden op basis van beveiligingsrichtlijnen.

De PDCA (Plan-Do-Check-Act) is een beproefde methodiek voor het beheren van veranderingen en het verbeteren van processen.

Een PDCA is een continu proces dat periodiek wordt doorlopen om risico gestuurd processen te evalueren. In de context van informatiebeveiliging kan het worden gebruikt om de prestaties van het informatiebeveiligingsproces van een organisatie te meten en te verbeteren. Met periodieke scans kunnen (ernstige) kwetsbaarheden gemeld worden en direct opgepakt worden, indien nodig.
Te denken aan:
- Secure codereview,
- Configuratie reviews en Attack & Penetration testen,
- Assessments op (naleven van) procedures die opdrachtgever heeft om de informatiebeveiliging van de gebruikte componenten te waarborgen.

Praktische invulling van de ambities

Om grip te krijgen op deze ambities ziet de Buyer Group de volgende werkzaamheden terugkomen bij projecten op het vlak van AI-beeldherkenning met drones.

Het begint bij het gezamenlijk opstellen, met o.a. de interne ICT-afdeling, van een beleid ten aanzien van de benodigde competenties en functie-vereisten voor eigen medewerkers. Denk daarbij aan medewerkers die in hun dagelijkse praktijk de beeldherkenning en drones in hun werkzaamheden gebruiken, alsook de betrokkenen vanuit de IT afdeling (techneuten, netwerkspecialisten, automatisering adviseurs, cybersecurity adviseurs), contractmanagers, stafmedewerkers.

Betrek bij eerste interne opstartfase van een project (bij strategiefase voorafgaand aan het project/aanbesteding) de IT betrokkenen, zodat

[26] https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cybersecurity/

er gelijk vanaf het begin wordt nagedacht over informatiebeveiliging ('security by design' aanpak).

Ga bij het vaststellen van de informatiebeveiligingsvoorwaarden uit van de beveiligingsrichtlijnen die voor de gebruikssituatie relevant zijn, aangezien de bepalingen afhankelijk zijn van de situatie waarin de technologie van beeldherkenning en drones wordt toegepast (zoals vitale of niet-vitale infrastructuur). Voor een effectieve en efficiënte samenwerking van IT-systemen is gelijkgestemde informatiebeveiliging van de automatisering dan ook essentieel.

De ICO Wizard kan overheden erbij helpen om te komen tot die specifieke informatiebeveiligingseisen die nodig zijn voor hun gebruikssituatie.

Deelnemers van de Buyer Group hanteren de BIO (dit is de norm voor kantoorautomatisering) en de CSIR 3.4 (dit is meer een implementatie richtlijn voor industriële automatisering) bij het formuleren van beveiliging voorwaarden en deze helpen om je vraagspecificatie helder te krijgen. Hieruit vloeien voorwaarden voort die je vervolgens in het contract aan opdrachtnemer stelt.

Er zijn beveiligingsrichtlijnen die helpen bij het compleet krijgen van je vraagspecificaties omtrent cybersecurity, zo is er:

- De BIO (Baseline Informatiebeveiliging Overheid), dat gebaseerd is op het internationaal geldende normenkader NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002. De BIO is voor de overheid verplicht en schrijft het basisniveau voor informatiebeveiliging binnen de overheid voor. De BIO bevat generieke controls/beheersdoelen voor de IT/Kantooromgeving. De BIO biedt één normenkader voor de beveiliging van de Informatievoorziening (IV) van de overheid. De BIO richt zich op de beveiliging van de Kantoorautomatisering (KA) en is niet zonder meer geschikt voor de beveiliging van de Industriële Automatisering. Bij de BIO ligt de focus op de informatie en de vertrouwelijkheid van de automatisering. Terwijl bij industriële automatisering de focus ligt op de functies van het object of systeem/proces en de betrouwbaarheid daarvan. Voor de beveiliging van Industriële Automatisering zijn standaarden beschikbaar. De Europese standaard hiervoor is de IEC 62443.
- De CSIR 3.4 (Cybersecurity Implementatierichtlijn Objecten), deze is gebaseerd op IEC62443 en heeft relaties met de BIO. Het is een vertaalslag van de relevante controls/beheersdoelen uit de BIO en de NCSC Checklist beveiliging ICS/SCADA systemen, met aanvullingen uit de relevante delen van de IEC 62443 voor de beveiliging van Industriële Automatisering.

Wees als opdrachtgever ervan bewust dat het kan gebeuren dat startups en midden-en klein bedrijven (nog) geen volledige certificering hebben of verkrijgen. Bespreek vooraf met je interne IT/beveiligingsexpert op welke wijze jullie daarmee om gaan en neem dit op in de aanbestedingsdocumenten[27].
Afhankelijk van de gebruikssituatie kan het bijvoorbeeld voldoende zijn wanneer ondernemers met het leveren van periodieke

[27] Bij gebruik van keurmerken verplicht de Aanbestedingswet om ook altijd 'gelijkwaardig' te accepteren. Inschrijvers kunnen alle geschikte bewijsmiddelen gebruiken om aan te tonen dat zij voldoend aan 'gelijkwaardigheid'.

rapportages voldoende zekerheid kunnen bieden. Waarbij je als opdrachtgever vooraf duidelijk hoort aan te geven welke controles en het aanleveren van welke informatie daarin belangrijk zijn.

Door middel van bijvoorbeeld een ISO certificering laten organisaties aan overheidsopdrachtgevers zien dat ze hun informatiebeveiliging beheersen en de (verwerking van) gegevens van die opdrachtgevers goed hebben beveiligd. Door aan de certificering te voldoen, betekent het dat systemen en werkprocessen aantoonbaar zijn beveiligd tegen datalekken en externe dreigingen.

Vraag een SBOM[28] uit of stel een SBOM samen. Een SBOM is een soort 'materialenpaspoort', maar betreft dan de onderdelen van de software (of in geval van hardware, HBOM). Met het opstellen/uitvragen van dit document wordt verder bijgedragen aan een grotere softwaretransparantie. Een SBOM geeft inzicht in de samenstelling en functionaliteit van de systemen. Om de impact, kwetsbaarheden en risico's in de onderliggende softwarecomponenten en op het IT-landschap beter in te schatten. In een SBOM staan de exacte versies van alle software- en hardwarecomponenten die toegepast worden, zodat er gelijk een mededeling opkomt voor potentiële kwetsbaarheden bij een controle ten opzichte van Common Vulnerabilities and Exposures (CVE) lijst.

Kanttekening is dat een SBOM lijst niet een statische lijst is, het vergt updates wanneer er nieuwe (versies van) componenten worden gebruikt. De SBOM is niet een waterdichte oplossing, aangezien kwetsbaarheden die niet-publiek bekend zijn (zoals 'zero-day' kwetsbaarheden) door het toepassen van SBOMs niet geïdentificeerd zullen worden. Een ander punt om rekening mee te houden is de leesbaarheid van een SBOM. Hiervoor is van het belang om te weten voor welke doelgroep (expert of leek) en met welke doelstelling de SBOM geschreven wordt. Zo zal een expert meer gebaat zijn bij de inzichten van metadata en dergelijke om bijvoorbeeld een toets te kunnen doen op AVG compliancy. Terwijl een persoon die minder deskundig is op dit specifieke werkgebied meer gebaat is bij inzicht in brondata, model en trainingsdata. Iets wat meer inzicht en begrip geeft over de informatie uitkomsten en de herkomst van data.

Aandachtspunten voor de samenwerking en eisen aan opdrachtnemer

- Opdrachtnemer heeft voor eigen personeel een cybersecurity awareness programma.
- Opdrachtnemer voldoet aan de beveiligingseisen uit de richtlijnen die door opdrachtgever voor de gebruikssituatie wordt toegepast en blijft op de hoogte (bijvoorbeeld door gebruikersforum) van informatiebeveiliging in zijn software daartoe.
- Opdrachtnemer waarborgt de digitale veiligheid gedurende de gehele levensduur van het contract en houdt de software en systemen daarop up-to-date.
- Bespreek als opdrachtgever met eigen cybersecurity adviseur de mogelijkheden en nut om een SBOM te laten aanleveren door opdrachtnemer. Om daarmee als overheid inzicht te krijgen in de onderdelen van de software en om afspraken te maken met

[28] SBOM verwijst naar Software Bills of Materials.

opdrachtnemer om te melden ingeval van beveiligingsrisico's op de onderdelen, evenals wanneer er nieuwe (versies van) componenten worden gebruikt.

- Opdrachtnemer richt een PDCA cyclus in en stemt dit periodiek af met de (cybersecurity adviseur van) opdrachtgever.
- De wereld op het vlak van informatiebeveiliging verandert snel. Neem op in de aanbestedingsdocumenten dat opdrachtnemer (ook) oog houdt op de toekomstige ontwikkelingen op het vlak van informatiebeveiliging en samen met opdrachtgever ervoor zorgt dat dit veilig blijft in de toekomst:
  - Het gaat daarbij ook om de processen die bij de overheids-organisatie zijn ingebed. Zorg dat intern de processen goed belegd zijn qua cybersecurity en contractmanagement. Bijvoorbeeld dat de interne cybersecurity functionaris erop toeziet als een contract niet voldoet aan eisen of nieuwe ontwikkelingen zijn op dat vlak. Om toekomstige ontwikkelingen gedurende de looptijd te kunnen beheersen (LCM-borging).
  - Richt (in verband met de snel veranderende wereld inzake informatiebeveiliging) de interne organisatie zo in dat frequenter checks in het contractmanagement worden doorlopen. Een nieuwe ontwikkeling of toepassing (net als dreigingsbeeld of een ontdekt lek) zijn een trigger om opnieuw door het PDCA proces te gaan en maatregelen langs te lopen of eventuele aanvullende maatregelen op beveiligingsvlak nodig zijn.
  - Benoem bij de aanbesteding welke procesafspraken en protocollen[29], en organisatorische voorschriften[30] de overheids-organisatie gebruikt om de veiligheid van toepassingen en AI-systemen te waarborgen evenals de te nemen stappen bij incidenten. Dit is momenteel afhankelijk per overheidsorganisatie welke invulling eraan wordt gegeven. Raadpleeg daartoe de relevante interne expert in informatiebeveiliging en juridisch adviseur.
- Net als elk ander ICT contract, hoort het de rechten en plichten van de partijen in geval van geschillen te beschrijven. Een suggestie van de Buyer Group is om op te nemen dat eventueel de partijen mogelijke geschillen kunnen brengen naar bijvoorbeeld het SGOA (Stichting Geschillenoplossing Automatisering). Te denken valt aan bijvoorbeeld voortijdige bemiddeling, arbitrage of second opinion. Bij het SGOA zit specifieke expertise waardoor (momenteel) er sneller en inzichtelijker bepaalde conflictbemiddeling mogelijk is dan via de rechtelijke macht.
- Regel in het contract dat na afloop er gegevensvernietiging plaatsvindt, en/of eventuele gegevensoverdracht (voor bijvoorbeeld opvolgende marktpartij, als opdrachtgever dat wenst). Verlang als opdrachtgever dat ondernemer een schriftelijke verklaring aanlevert van het digitaal vernietigen, volgens de normen van de Archiefwet (dus ook van back-ups en veiligheidskopieën). Een verklaring biedt namelijk aanspraak en voorkomt dat gegevens niet hergebruikt worden op een andere manier.

[29] Te denken valt aan ITIL protocol (beschrijft o.a. hoe om te gaan met veranderingen), CSIR richtlijn, en BIO (geeft o.a. hoe de security organisatie in te richten).

[30] Zo heeft bijvoorbeeld ProRail op dit moment interne eisen dat persoonsgegevens zijn uitgesloten om bij datasets mee te modelleren op het vlak van AI tooling.




DELEN VAN DATA, AI EN INFORMATIE

STRATEGIE PER THEMA: HOE ER TE KOMEN?

STRATEGIE PER THEMA: HOE ER TE KOMEN?

3.3 Delen van data, AI en informatie

Wat is onze ambitie

We onderschrijven het principe van 'één keer verzamelen, meerdere keren gebruiken', binnen de mogelijkheden die doelbinding biedt[31]. Deze ambitie heeft tot doel het hergebruik van bestaande data te bevorderen alsook het streven om niet onafhankelijk van elkaar vergelijkbare algoritmen voor soortgelijke taken te laten ontwikkelen en implementeren. Daarnaast wil de overheid meer openheid over wat zij doet, met als uitgangspunt dat overheidsinformatie openbaar gedeeld wordt. Deze lijn volgt de Buyer Group in haar ambitie, namelijk 'openbaar tenzij'[32]. Waar mogelijk willen wij datasets, AI en informatie (centraal) beschikbaar kunnen stellen, aangezien het een meer datagedreven en innovatieve samenleving ten goede komt en (her)gebruik van data.

- Een consistente manier van verzamelen, opslaan en delen van data (over de gehele keten van beeldmateriaal tot informatie) staat hierin centraal, waarvoor goed gegevensbeheer nodig is.
- Verder heeft het delen van data met name waarde als het is van metadata om de gegevens te begrijpen en te interpreteren. De Buyer Group ziet een belangrijke rol voor open formaten en functionele beschrijvingen bij het vastleggen van de metadata.
- Tegelijkertijd draait het bij het beschikbaar stellen erom dat de gegevens gemakkelijk toegankelijk zijn. Ofwel: het bevorderen van de vindbaarheid en het kunnen begrijpen en gebruiken van data is nodig om de volle potentie van datadelen te (laten) benutten.

[31] Hierin is AVG bepalend, zie ook hoofdstuk 3.4.

[32] Conform de Wet hergebruik overheidsinformatie (Who).

3.3.1 Gegevensbeheer en toegang tot gegevens

Er liggen veel kansen om te werken met AI en datadelen, daarbij valt of staat alles met solide gegevensbeheer: het is nodig dat er op de juiste manier met data wordt omgegaan en de data(sets) kwalitatief goed in elkaar zitten. Met gegevensbeheer bedoelen wij hoe er met data wordt omgegaan (op bijvoorbeeld een platform/server). Gegevensbeheer is gericht op het operationele beheer van de data binnen een applicatie of specifieke context.

In het kader van gegevensbeheer zorgen open formaat standaarden ervoor dat data toegankelijk zijn en effectiever te gebruiken in een breed scala van contexten. Door met open formaat standaarden te werken, biedt het de mogelijkheid om data onafhankelijk van een applicatie en in meerdere type systemen te kunnen gebruiken. Dat verhoogt de toegevoegde waarde van de data. Dit in tegenstelling tot data die zijn opgeslagen of gedeeld met behulp van eigen/gesloten formaten; deze kunnen alleen worden geopend of gebruikt door specifieke tools of systemen (dat kan resulteren in afhankelijkheid daartoe).

De Buyer Group is een voorstander van open formaat standaarden. Aangezien data erdoor makkelijker uitwisselbaar zijn en niet gebonden aan één software omgeving. Het gebruiken of het vereisen van open standaarden ziet de Buyer Group als een goede stap richting het integraal benutten van data over verschillende domeinen. Het kan

'data-waste'[33] verminderen doordat hergebruik makkelijker is. Bij domeinen waar een bepaalde volwassenheid optreedt zijn de open standaarden het meest effectief[34]. Bij innovatieve ontwikkelingen kunnen de voordelen minder sterk zijn, bijvoorbeeld als er nog geen (standaard) consensus is over de inhoud en interpretatie van data. Per gebruikssituatie ligt het dus aan de volwassenheid of een standaard (al) gewenst is, dit zal dus per geval moeten worden bekeken.

Afhankelijk van de toepassing en de gevoeligheid van de data, kan het passend zijn om ofwel data niet te delen dan wel op een beperkte/gecontroleerde manier te delen. Bijvoorbeeld door het gebruik van gegevensmaskering of andere technieken om gevoelige informatie te beschermen.

Het gebruik van data wordt beheerst door diverse wetten en voorschriften die specificeren waarvoor gegevens wel of niet mogen worden gebruikt, evenals voorwaarden waaronder gegevens met derden mogen worden gedeeld. Zoals:

- *Wet hergebruik van overheidsinformatie:* Een wet die tot doel heeft de beschikbaarheid en het hergebruik van de informatie van overheden te vergroten om transparantie, verantwoording, innovatie en economische groei te bevorderen. Het creëert een wettelijk kader dat hergebruik van deze informatie door het publiek en ondernemers mogelijk maakt.
- *Algemene Verordening Gegevensbescherming (AVG)*: zie toelichting bij hoofdstuk 1.3.3 en hoofdstuk 3.4.
- *De Europese AI Verordening:* zie toelichting bij hoofdstuk 1.3.3.

Wees met gebruiksvoorwaarden zo concreet mogelijk over het kunnen toepassen van de gegenereerde data en het (eventueel) kunnen delen ervan. Vervolgens kunnen gebruiksvoorwaarden duidelijkheid verschaffen over onder meer wie de eigenaar is van de data, hoe de data gebruikt kunnen worden en hoe eventuele geschillen tussen partijen worden afgehandeld.

3.3.2 Metadata en openheid met codes

Metadata is van vitaal belang bij gegevensbeheer en datadelen. Data heeft in het bijzonder waarde wanneer het is voorzien van **metadata**. Metadata beschrijft bijvoorbeeld welke informatie de dataset bevat, hoe het is verzameld, en hoe het kan worden gebruikt. Met deze aanvullende informatie is data te interpreteren. Bovendien kunnen metadata worden gebruikt om de nauwkeurigheid[35] en integriteit van de gegevens te waarborgen.

Wanneer overheden ervoor kiezen om algoritmen en codes te delen, biedt werken met open formaten een manier om anderen in staat te stellen de code te gebruiken en aan te passen. Algoritmen in een open formaat kunnen ook beschikbaar worden gesteld via open source, waarbij de broncode kan worden bekeken, gewijzigd en gebruikt. De belangrijkste voordelen van algoritmen in een open formaat zijn dat ze anderen in staat stellen om de nauwkeurigheid en eerlijkheid ervan te verifiëren, evenals eventuele vooroordelen te identificeren. Algoritmen in een open formaat kunnen door anderen worden gebruikt en aangepast voor nieuwe gebruiksscenario's of om aan specifieke behoeften te voldoen. Het is echter belangrijk op te merken dat het niet automatisch betekent dat de gegevens die

[33] Verzamelde data die ongebruikt blijft.

[34] Het is niet mogelijk een uitputtende lijst met open standaarden te maken aangezien het afhangt van het domein en de toepassing. Te denken valt aan bijvoorbeeld OGC-standaarden, op het vlak van geografische informatiesystemen (GIS) en locatiegebaseerde diensten.

[35] Het geeft inzicht in wanneer de data is geaggregeerd.

worden gebruikt om het algoritme te trainen en te testen, openbaar moeten zijn, aangezien deze gevoelig of privé kunnen zijn.

Door een algoritme te voorzien van een functionele beschrijving geeft het een beter begrip hoe het algoritme werkt, de beoogde resultaten en de beperkingen ervan[36]. Dit kan van belang zijn voor het beoordelen van de nauwkeurigheid, eerlijkheid en betrouwbaarheid en is essentieel voor het opbouwen van vertrouwen, transparantie en naleving in het gebruik. Het vereiste niveau van transparantie kan variëren, afhankelijk van de aard van het algoritme en de gebruikscontext. Het is van belang om de balans te vinden tussen transparantie en veiligheid en bescherming van gevoelige informatie. Transparant zijn over algoritmen zorgt ook voor meer publiek begrip en toezicht op de besluitvorming door de overheid (zie eveneens hoofdstuk 3.4 over ethiek).

Door het delen van ervaringen bij het ontwikkelen van algoritmen kunnen overheden van elkaar leren en hun processen verbeteren. Dit kan leiden tot meer hergebruik en samenwerking tussen verschillende overheidsinstanties en overheidsniveaus. Een manier om hier te komen is de ontwikkeling van een gezamenlijke roadmap voor het delen van gegevens.

3.3.3 Toegankelijke data beschikbaar stellen

Laagdrempeligheid/toegankelijkheid tot data is een belangrijk aspect om te zorgen dat gedeelde data wordt gebruikt. Wanneer gegevens tussen organisaties gemakkelijk te vinden en te openen zijn, is de kans groter dat deze worden (her)gebruikt. Dit creëert kansen voor nieuwe innovatieve informatieproducten.

Het gebruik van open standaarden voor gegevensopslag en -uitwisseling kunnen hierbij helpen om de toegankelijkheid te bevorderen, aangezien deze standaarden zijn ontworpen om breed te worden overgenomen en begrepen door veel verschillende systemen en platforms. Overheden kunnen hun data open en (publiekelijk) beschikbaar stellen via open data portalen.

Bij het delen van data gaat het niet alleen om de beschikbaarheid van data, maar ook om de kwaliteit van data. Het kan bij open of gedeelde data een uitdaging zijn om gegevens te (her)gebruiken wanneer de data onvolledig of van slechte kwaliteit zijn. Het verstrekken van nauwkeurige, actuele en hoogwaardige data maken de gegevens ook waardevoller voor meerdere opdrachtnemers. Dat bevordert op zijn beurt weer het gelijke speelveld. Zo wordt er een competitieve situatie gerealiseerd dat het makkelijk maakt voor nieuwe spelers om ook aan te kunnen bieden.

Gegevensbeheer en het beschikbaar maken van data geld kost. Maak van tevoren de balans op tussen de kosten en baten tijdens de opstartfase van het project. De kosten voor het opzetten en onderhouden van bijvoorbeeld een dataportaal kunnen fors zijn, afhankelijk van de complexiteit van het systeem en het aantal gebruikers dat er toegang toe zal hebben. Soms zijn overheden deels budget gefinancierd (o.a. Kadaster) en vragen daarom een vergoeding voor het verstrekken van gegevens om hun kosten te dekken. Deze vergoeding kan variëren afhankelijk van het type gegevens dat wordt verstrekt en het gevraagde bedrag.

[36] Een functionele beschrijving is een gedetailleerde beschrijving van de functionaliteiten en kenmerken van een systeem of proces, om bijvoorbeeld gebruikers en ontwikkelaars te helpen begrijpen hoe het werkt en wat het kan doen.

Praktische invulling van de ambities

Om grip te krijgen op deze ambities ziet de Buyer Group de volgende werkzaamheden terugkomen bij projecten op het vlak van AI-beeldherkenning met drones.

Ga tijdens de aanvangsfase[37] van een project uit van het gedachtegoed:

- ✔ 'Eén keer verzamelen, meerdere keren gebruiken' (binnen de mogelijkheden die doelbinding biedt[38])
- ✔ 'Openbaar, tenzij'

Zorg er voor dat de software die de overheid maakt of laat maken open source is, als mogelijk. Dit betekent dat de code toegankelijk en herbruikbaar zal zijn (zie hoofdstuk 3.3.2). Dat is de kern van de in 2020 geïntroduceerde beleidslijn 'Open, tenzij'. De 'tenzij' komt voort uit de weigeringsgronden van de Wet Open Overheid. Probeer dus met open source te werken wanneer het kan en overweeg daarbij de potentie van het uitwisselen van data of algoritmen met collega-overheden.

Het is lastig om in algemene zin voor projecten aan te geven hoe data en algoritmen te behandelen. Ga voor elk specifiek project hierover binnen de organisatie het gesprek aan:

- Overleg tijdens de aanvangsfase[39] of de organisatie het eigendom van de invoerdata, uitvoerdata en algoritmen wil (of moet) verkrijgen, of dat alleen het recht om ze te gebruiken voldoende is. De keuze hiertoe kan verschillen per organisatie en gebruikssituatie (ziet het bijvoorbeeld toe op kernprocessen).
- Voer vooraf een marktverkenning[40] uit om te ontdekken welke ontwikkelingen en oplossingen waardevol zijn voor de behoeften. Ook een marktconsultatie[41] kan helpen om (specifieke) zaken te verhelderen.
- Grofweg zijn er twee opties om als publieke opdrachtgever met de markt aan de slag te gaan: het aankopen van een reeds bestaand product/dienst[42] of het starten van een ontwikkeltraject om een werkbare oplossing te realiseren. In het bijzonder bij de laatste optie is het van belang de rollen en voorwaarden (mede t.a.v. data en algoritmen) van opdrachtgever en opdrachtnemer te bepalen[43]. Ga de dialoog erover aan met de markt.

[37] Bij de eerste strategiefase voorafgaand aan het project.

[38] Hierin is AVG bepalend, zie ook hoofdstuk 3.4.

[39] Bij de eerste strategiefase voorafgaand aan het project/aanbesteding.

[40] Stappenplan marktverkenning | PIANOo - Expertisecentrum Aanbesteden

[41] Stappenplan marktconsultatie | PIANOo - Expertisecentrum Aanbesteden

[42] Die geen aanzienlijk noodzakelijke aanpassing nodig heeft.

[43] Te denken valt bijvoorbeeld aan eigendom van de ontwikkeling (foreground IP) en de methodologie en kennis die tot de oplossing heeft geleid (background IP).

Neem contact met soortgelijke overheden op bij (nieuwe) mogelijkheden voor datadelen en de mogelijkheden om kosten te delen. Stel het contract vervolgens zo op dat hergebruik ook door de andere collega-overheden mogelijk is (binnen de mogelijkheden die doelbinding biedt[44]). Belangrijke punten die daarbij van belang zijn, is dat opdrachtgever eigenaar wordt van de data, evenals eisen om de interoperabiliteit te vergroten van de geleverde data.

Is het plan om met het project ook de data openbaar beschikbaar te stellen?

- Ga als projectteam na of de data die voor een bepaald doel zijn verzameld, ook daadwerkelijk voor een ander doel te gebruiken is danwel als open data mogen worden verspreid. Daarbij zijn diverse afwegingen, zoals de aard van de gegevens, potentiële risico's voor organisaties en veiligheidsaspecten zoals privacy en staatsveiligheid. Voer er een risicobeoordeling op uit. Denk daarbij ook aan de AVG, zie hoofdstuk 3.4.
- Ga na of het beschikbaar stellen van de data centraal in te regelen is bij bestaande initiatieven/portals. Doe hiertoe een verkenning. Let daarbij op mogelijke eisen ten aanzien van opslag, beheer en distributie. Zie ook studies over het delen van data, uitgevoerd door de Nederlandse AI Coalitie[45].

Stel verder van tevoren gebruiksvoorwaarden op als u met anderen data of algoritmen gaat delen die u verzamelt.

Aandachtspunten voor de samenwerking en eisen aan opdrachtnemer

- Eigendom-, auteurs- en databankrechten zijn belangrijke aspecten van data en van algoritmen, zodoende ook voor de uitwisseling ervan. Bespreek als opdrachtgever met een (interne of externe) jurist de diverse mogelijkheden in deze rechten. Bij het aangaan van contracten voor IT-producten en -diensten hanteren overheden doorgaans algemene voorwaarden, zoals de ARBIT[46] of GIBIT[47]. Ook voor grote en bijzondere IT-projecten kunnen deze worden gebruikt of daarvoor als uitgangspunt kunnen dienen.
- Ga als intern projectteam vooraf na waar de interoperabiliteit in te regelen of vergroten is, zie hoofdstuk 3.3.2. De Buyer Group ziet een belangrijke rol voor gegevensbeheer, open standaarden evenals functionele beschrijvingen bij het vastleggen van de metadata.
- Maak het contract omtrent standaarden zo eenvoudig mogelijk, om laagdrempeligheid na te streven. Wanneer ondernemers de specificaties gemakkelijk kunnen begrijpen, verkleint dat de kans op misverstanden die anders het hergebruik en de ontwikkeling van data(producten) kunnen belemmeren. Daarnaast bevordert het ook de toegankelijkheid van de aanbesteding voor (jonge) innovatieve ondernemers.
- Maak een keuze bij aanbesteding om open formaat standaarden toe te passen bij de data en voor het mogelijk kunnen delen van algoritmen, om interoperabiliteit te bevorderen (zie ook hoofdstuk 3.3.1 en 3.3.2).
  - De keuze voor open data hangt af van de gevoeligheid en vertrouwelijkheid van de gebruikte data.

[44] Hierin is AVG bepalend, zie ook hoofdstuk 3.4 over Ethiek en publieke acceptatie.

[45] Data Delen - Nederlandse AI Coalitie (nlaic.com)

[46] Algemene Rijksinkoopvoorwaarden bij IT-overeenkomsten.

[47] Gemeentelijke Inkoopvoorwaarden bij IT.

- Laat het doel, de logica en de werking van het algoritmen procedureel transparant maken: om zo de werking van het algoritme te begrijpen hoe deze data verwerkt en beslissingen neemt. Dit kan door het algoritme te voorzien van een functionele beschrijving dat inzicht biedt in de resultaten en de beperkingen ervan. Om zo te kunnen nagaan of de juiste maatregelen zijn genomen om de kwaliteit te waarborgen en risico's te beperken. Het bevordert op zijn beurt het vertrouwen in het AI-gebruik en kan relevant zijn bij het Algoritmeregister.
- Als de algoritmen en het AI-systeem specifiek voor opdrachtgever gemaakt worden, overweeg dan om niet alleen de uitkomst van het algoritme beschikbaar te stellen maar ook het algoritme zelf (afhankelijk van gevoeligheid van een use case).
- Opdrachtgever en -nemer horen voorwaarden van open-sourcelicentie te begrijpen en na te leven wanneer data en/of algoritmen gaan delen.
  - Onder een open-sourcelicentie is te regelen dat anderen het algoritme (onder bepaalde voorwaarden) mogen gebruiken, kopiëren en verspreiden. Dit is afhankelijk van het type licentie. Zo is het bijvoorbeeld mogelijk dat alle wijzigingen of verbeteringen aan het algoritme onder dezelfde open-sourcelicentie voor het publiek beschikbaar worden gesteld, of ook dat bijvoorbeeld de oorspronkelijke maker wordt vermeld.
  - Wanneer opdrachtgever van plan is de data als open data ter beschikking te stellen, kan worden gekeken naar de licentievoorwaarden zoals Creative Commons (CC BY 4.0).
- Overweeg, in het kader van kennisdeling, om bepaalde wederkerige voorwaarden op te nemen in de gebruiksovereenkomst wanneer opdrachtgever data beschikbaar stelt. Bijvoorbeeld:
  - Wanneer derden de data gebruiken voor hun eigen dienst/product, dat ze de overheidsorganisatie ervan op de hoogte stellen en hen toegang bieden tot de nieuwe gegenereerde relevante datasets om te gebruiken voor overheidsdoeleinden.
  - Onderzoeksinstellingen en bedrijven die data de gebruikt voor onderzoek- en ontwikkeling, dat de kennis en inzichten daaruit worden gedeeld met de overheidspartij die ze ervan op de hoogte stellen.




ETHIEK EN PUBLIEKE ACCEPTATIE

STRATEGIE PER THEMA: HOE ER TE KOMEN?

STRATEGIE PER THEMA: HOE ER TE KOMEN?

3.4 Ethiek en publieke acceptatie

Wat is onze ambitie

"Bezint eer gij begint", (onwenselijke) effecten van nieuwe technologie zijn soms moeilijk te overzien.

Daarom willen wij het ethische perspectief als basishouding bij de opzet en uitvoering van AI-beeldherkenning met drones hanteren, in lijn met de beleidslijn van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Daarbij willen we transparantie en betrouwbare AI waarborgen en zien we een belangrijke rol voor het betrekken van het publiek tijdens (ontwikkeling van) AI-beeldherkenning met drone projecten. Het opstellen en uitvoeren van een communicatiestrategie gericht op het verbeteren van de beeldvorming is hierin een onderdeel om het vertrouwen rondom AI-beeldherkenning met drone projecten te vergroten.

Met behulp van impact assessments zijn de risico's op deze onwenselijke effecten te verkleinen en te voorkomen. Hiervoor zijn diverse risicobeoordelingstools en methodes voorhanden waarmee overheden en ondernemers strategieën kunnen ontwikkelen om ethische risico's te beperken. Zoals monitoring van eerlijkheidsaspecten[48], alsook verklaarbaarheid en transparantiemechanismen[49].

Er is op dit vlak geen one-size-fits-all oplossing. Het is daarom van belang om de geschiktheid van elke tool of methode voor de specifieke gebruikssituatie en organisatie te evalueren.

Bias

Onbewuste vooringenomenheid in uitkomst van algoritme (een bias) kan weliswaar ontstaan in alle fasen van het ontwikkelproces, maar voornamelijk tijdens de trainingsfase. Door tijdens alle fasen een kritische houding aan te nemen kan het worden gesignaleerd. De focus ligt hierbij op de dataset, de architectuur en de aannames die hierbij zijn gemaakt. Meestal treedt bias op tijdens de trainingsfase. Daarom is extra aandacht nodig bij het samenstellen van een trainingsdataset. Een zo gevarieerd mogelijke dataset is van belang. Ook is het een manier om juist gebruik te maken van technieken waarbij gewerkt wordt met ongebalanceerde datasets, datasets met een mogelijke bias erin.

Communicatiestrategie

De Buyer Group vindt het belangrijk dat organisaties op een begrijpelijke wijze en op tijd communiceren naar stakeholders, inclusief de opties voor bezwaar en mogelijkheden voor contact voor vragen en informatie. Een communicatiestrategie hoort volgens de Buyer Group een vast onderdeel te zijn in de aanloop naar het gebruik van AI-systemen en drone technologie.

[48] Rekeninghouden met diversiteit in de populatie/gegevensbestand, ter voorkoming van afwijkingen voor specifieke personen, groepen of andere eenheden ontstaan.

[49] Er kan verantwoording worden afgelegd over de gevolgde procedures en de werking van het algoritme is te verklaren en uit te leggen.

Beschrijf in een strategie onder meer stapsgewijs hoe en wanneer organisaties informatie verstrekken over het gebruik van AI-systemen. Op welke wijze wordt gecommuniceerd hangt uiteraard af van voor welke doelgroep het is bedoeld. De werking van AI technologie (en brondata) begrijpelijk maken voor publiek kan bijvoorbeeld ook door visualisatie, verklarende afbeeldingen, of beschrijvingen van (simpele) voorbeelden. Verder verdient naleving (bezwaarprocedures) een plek in een dergelijk plan. Verbind daar vanzelfsprekend concrete acties aan, zodat er daadwerkelijk een (elektronisch) loket beschikbaar is die met eventuele bezwaren aan de slag gaat.

Regelgeving en handhaving

In Nederland heeft de overheid de bevoegdheid om wet- en regelgeving te handhaven met betrekking tot het ethisch gebruik van AI, waaronder die met betrekking tot gegevensbescherming, privacy en non-discriminatie. De centrale toezichthouders die verantwoordelijk zijn voor de handhaving van deze wet- en regelgeving is de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens is verantwoordelijk voor de handhaving van de Algemene Verordening Gegevensbescherming (AVG) en de Wet bescherming persoonsgegevens die het verzamelen, bewaren en gebruiken van persoonsgegevens regelen. De Autoriteit Persoonsgegevens kan boetes voor het overtreden van deze wetten.

De registratie van risicovolle algoritmen wordt naar alle waarschijnlijkheid in 2024/2025 wettelijk verplicht op basis van de Europese AI verordening. Begin als overheidsorganisatie met het vastleggen van algoritmen in het publieke Algoritmeregister[50]. Zorg als overheid ervoor dat de benodigde informatie[51] die nodig is voor het Algoritmeregister daarin terecht komt.

De Inspectie Leefomgeving en Transport (ILT) houdt toezicht op het naleven van wet- en regelgeving voor de luchtvaart en is verantwoordelijk voor het reguleren en handhaven van het gebruik van drones. Ze kunnen sancties opleggen aan personen of organisaties die droneregelgeving overtreden, zoals boetes of straffen voor het besturen van drones in beperkt luchtruim of het niet registreren van een drone. ILT heeft richtlijnen uitgevaardigd voor de veilige bediening van drones, waaronder regels over vlieghoogte, vliegen in de buurt van luchthavens en vliegen over bevolkte gebieden. Ze kunnen indien nodig ook het luchtruim in bepaalde gebieden afsluiten voor drones.

Lokale overheden hebben in Nederland ook de bevoegdheid om beperkingen op te leggen aan het gebruik van drones in hun rechtsgebied. Zo hebben sommige gemeenten het vliegen met drones in bepaalde gebieden, zoals parken of natuurgebieden, verboden om dieren in het wild te beschermen en de natuurlijke omgeving te behouden.

Praktische invulling van de ambities

Om grip te krijgen op deze ambities ziet de Buyer Group de volgende werkzaamheden terugkomen bij projecten op het vlak van AI-beeldherkenning met drones.

Voer een impact assessment uit ter voorbereiding op uw project, zo heeft bijvoorbeeld het Ministerie van Infrastructuur en Waterstaat

[50] Het Algoritmeregister van de Nederlandse overheid.

[51] Voor meer informatie: Algoritmes (pleio.nl)

ontwikkelde het AI Impact Assessment (AIIA)[52]. Een assessment helpt bij het nadenken over de diverse effecten van AI-systemen. Het AIIA combineert meerdere raamwerken, zoals AVG-wetgeving, NEN- en ISO-normen en de Europese AI Act. Het assessment helpt je rekening te houden met wat er mag en kan. Met het AIIA let je op de technische werking, op data en privacy en op risico's waar het AI-systeem toe leidt. Ten slotte ondersteunt het AIIA bij het afleggen van verantwoording, zowel binnen de organisatie als naar de samenleving.

Wees als publieke organisatie bewust van de impact die u maakt met drones op publiek. Het communiceren erover, op basis van een communicatiestrategie, is belangrijk voor acceptatie en mitigeren van potentiële weerstand. Wanneer niet helder uit te leggen is wat u gaat doen en waarom, dan is dat een belangrijk aandachtspunt: heroverweeg in dat geval om het niet te doen.

De werking van AI-technologie (en brondata) begrijpelijk maken voor publiek kan door visualisatie, geannoteerde beelden, of (simpele) praktijkcasus te beschrijven. Uitleggen hoe een model tot een uitkomst is gekomen is lastiger. Dit geldt al helemaal voor ingewikkeldere modellen, zoals neurale netwerken. In praktijk zal het zoeken zijn naar de balans tussen verklaarbaarheid en complexiteit. Advies daarbij is om modellen in eerste instantie klein en relatief eenvoudig te houden, zodat het te overzien is. Het is van belang om de brondata beschikbaar te houden en daarbij aan te geven welke data ervan is gebruikt om tot het model te komen, alsook welke codering van het model uit andere modellen komt (die op andere data is getraind).

Het vastleggen van algoritmen in een register kan nog best een klus zijn, afhankelijk van welke stappen er al bij uw organisatie hierin zijn gezet. Sommige organisaties hebben hun eigen register, anderen zijn aangesloten op het Nederlandse Algoritmeregister. Het vaststellen/bespreken welke algoritmen moeten worden opgenomen in een register, wie verantwoordelijk is, en het toegankelijk uitleggen ervan kan capaciteit vergen. Als er reeds werkwijzen bij uw overheidsorganisatie is ingeregeld, is het vanzelfsprekend dat de algoritmes uit uw project op consistente wijze toegankelijk worden gemaakt en benoem/verwerk die werkwijze van tevoren in de aanbesteding.

Een algoritmeregister is er om toegankelijk te zijn voor het publiek en heeft tot doel informatie te verschaffen over de algoritmen die worden gebruikt door overheden. Een algoritmeregister bevat informatie over het doel van het algoritme, de typen invoer- en uitvoergegevens, de programmeertaal waarin het algoritme is geïmplementeerd en alle andere relevante details. Het kan ook beschrijvingen of uitleg bevatten van hoe de algoritmen werken en waarvoor ze worden gebruikt.

Het is mogelijk om (op hoofdlijnen) de werking van algoritmen van AI-beeldherkenningstechnologie begrijpelijk te maken. Het inzicht geven kan op verschillende manieren worden gedaan, zoals over hoe het is opgebouwd, hoe het is getraind, hoe de parameters zijn gekozen, evenals waarom en hoe de uitkomst wordt gebruikt. Zie ook het hiernavolgende tekstkader dat toelichting geeft over hulpmiddelen.

Betrek op verschillende momenten in het proces stakeholders en laat ook zien wat er met deze input/co-creatie gebeurt. Feedbackloops zijn

[52] AI Impact Assessment | Rapport | Rijksoverheid.nl

van belang bij de ontwikkeling van AI, omdat ze een systeem in staat stellen om van fouten te leren, zich aan nieuwe situaties aan te passen en zijn prestaties voortdurend te verbeteren. Om AI-oplossingen af te stemmen op de behoeften van betrokkenen (zoals gebruikers en burgers) en publieke waarden[53] tastbaar te maken, zijn er verschillende soorten feedbackloops voor participatie te gebruiken:

- User feedback loops: Hierbij wordt input verzameld van gebruikers van AI-systemen over hun ervaring met de systemen en wordt die feedback gebruikt om aanpassingen en verbeteringen aan de plannen door te voeren. Dit kunnen enquêtes, interviews en bruikbaarheidstesten zijn.
- Stakeholder feedbackloops: Hierbij wordt overlegd met belanghebbenden, zoals maatschappelijke organisaties en experts, om hun standpunten over het gebruik van AI beeldherkenning met drones te verzamelen en ervoor te zorgen dat deze digitale oplossingen zijn afgestemd op hun behoeften en waarden.
- Feedbackloops voor burgers: deze omvatten het betrekken van burgers via openbare raadplegingen en door burgers geleide initiatieven om hun mening over het gebruik van AI te verzamelen en ervoor te zorgen dat AI-oplossingen zijn afgestemd op hun behoeften en waarden.

Weet dat er diverse hulpmiddelen zijn om aan de slag te gaan met ethiek bij AI en inzicht in algoritmen:

- Om de diverse visies op ethische kwesties met betrekking tot AI te verzamelen is betrokkenheid van belanghebbenden waardevol. Er zijn werkvormen voor om inzichten te verkrijgen van bijvoorbeeld burgers, werknemers en experts, zoals het gezamenlijk opstellen van een "customer journey"[54].
- Het opsporen van algoritmische vooroordelen (bias) zoals: Aequitas, FairTest en What-If-tool.
- Uitlegbaarheid en interpreteerbaarheid: Enkele voorbeelden zijn TCAV (Testing with Concept Activation Vectors), LIME, SHAP, Breakdown.
- Het monitoren van eerlijkheid: Voorbeelden zijn Fairness Flow, Fairlearn en AIF360.
- Privacy-effectbeoordeling, zoals datalekken of misbruik van persoonsgegevens. Enkele voorbeelden zijn DPIA, Richtlijnen Privacy Impact Assessment en PIA-Kit.

Zet het onderwerp ethiek (en eventuele risico's op dat vlak) standaard als bespreekpunt op de agenda bij (periodieke/jaarlijkse) contract-management overleggen tussen opdrachtgever-opdrachtnemer.

Wees als projectleider bewust van hoe er wordt gehandhaafd t.a.v. het ethisch gebruiken van AI en het gebruik van drones, en schakel met de betreffende inhoudsexperts die binnen de organisatie daarover gaan. Zoals met de AVG expert die binnen de organisatie werkt.

Wanneer het gaat om het gebruik van drones en het bijbehorende meldingsprotocol, is het van belang om rekening te houden met de data die door de drones worden verzameld en verwerkt. Deze data kunnen persoonlijke informatie bevatten, zoals beelden van personen of voertuigen op de grond. Door een DPIA uit te voeren voor het meldingsprotocol van drones, kunnen organisaties de risico's voor

[53] Zie bijvoorbeeld de zes 'Tada-waarden' uit het Tada Manifest; https://tada.city/

[54] Zie bijvoorbeeld https://ccn.waag.org

de privacy van individuen identificeren en beheersen, en ervoor zorgen dat het gebruik van drones in overeenstemming is met de privacywetgeving.

Een DPIA is een proces waarbij de mogelijke risico's voor de privacy van individuen worden geïdentificeerd en beoordeeld wanneer persoonlijke gegevens worden verwerkt. Het doel van een DPIA is om organisaties te helpen de risico's te begrijpen en maatregelen te nemen om deze risico's te beperken of te vermijden. De Europese AI Act en de DPIA (Data Protection Impact Assessment) zijn afzonderlijke wettelijke verplichtingen. Terwijl AI Act zich richt op het beoordelen van de naleving van risicovolle AI-systemen met specifieke vereisten, betreft DPIA het evalueren van mogelijke risico's van de verwerking van persoonsgegevens.

Voor AI-systemen met een hoog risico die persoonsgegevens verwerken, kunnen beide beoordelingen elkaar echter kruisen, waardoor de verantwoordingsplicht en risicobeperking worden verbeterd.

Aandachtspunten voor de samenwerking en eisen aan opdrachtnemer

- Om het effect van het inzetten van AI en beeldherkenning te overzien, laat intern (of extern) een impact assessment[55] uitvoeren: de resultaten en aandachtspunten zijn vervolgens te verwerken in het inkooptraject.
- Opdrachtnemer houdt in zijn werkzaamheden zich aan de daartoe geldende regelgeving, zoals de AVG. Wanneer een opdrachtnemer mogelijke risico's opmerkt, stelt het de opdrachtgever ervan op de hoogte.
- Maak als opdrachtgever een keus in welke partij vanuit AVG-perspectief verantwoordelijk is voor de brondata, wie deze beschikbaar houdt en voor hoelang. Net als bij elk ander ICT contract, regel indien relevant een verwerkersovereenkomst.
- Vraag als opdrachtgever naar een heldere uitleg door opdrachtnemer, met als doel om als publieke partij inzicht[56] te krijgen in de werking van de algoritmen en/of AI model alsook het datamanagement. Mogelijk kan de uitleg ook als input dienen voor het algoritmeregister.
  - Neem in overeenkomst bijvoorbeeld de voorwaarde op dat als overheidsorganisatie het verlangt, de leverancier zal assisteren bij het invullen van het Nederlandse Algoritmeregister.
  - Laat opdrachtnemer een beschrijving aanleveren ten aanzien van de hele keten. Op het niveau van: op deze locatie(s) zijn opnames gemaakt, de opnames gaan in dit model, dat herkent deze beelden, dit wordt vervolgens zo vastgelegd, om uiteindelijk tot deze uitkomst te komen.
  - Laat opdrachtnemer tekstueel toelichten welke data is gebruikt om tot het model te komen, alsook welke codering van het model uit andere modellen komt (die op andere data is getraind).
  - Maak in samenwerking een vertaling ervan voor het publiek. Het publiek is met name geïnteresseerd in welke soort data (welke kenmerken) erin gaat en wat er mee gedaan wordt. Het moet op een begrijpelijke/laagdrempelige wijze gedeeld kunnen worden.
- Geef bij de opdrachtnemer aan dat er belang wordt gehecht aan stakeholderfeedbackloops en hoe deze zijn ingericht. Bij het inzetten van AI en beeldherkenning in het publieke domein kan een participatiestrategie daartoe gewenst.

[55] AI Impact Assessment | Rapport | Rijksoverheid.nl

[56] In het geval er een SBOM voor de informatiebeveiliging (zie hoofdstuk 3.3.2) wordt uitgevraagd bij de aanbesteding, kan dat mogelijk als rode draad dienen tot overzicht.

- Bereid aan de start van het traject een communicatiestrategie voor. En rol deze uit gedurende de looptijd van het project, dit kan tijdens de ontwikkeling zijn alsook wanneer het in gebruik genomen is. Van belang zijn helder taalgebruik en een eventuele visuele toelichting. Zorg er daarnaast voor dat opdrachtnemer tijdens het inzetten van een drone op bepaalde wijze naar de omgeving communiceert dat er met een drone wordt gevlogen en voor welk doel[57].
- Regel een bezwaarprocedure in. De NvWA heeft bijvoorbeeld een (algemene) meldingsmogelijkheid ten aanzien van overlast van hun drones. Deze is door burgers en stakeholders online in te vullen[58].

[57] Zo regelt Politie dit bijvoorbeeld door ter plekke een aantal duidelijke grote informatieborden te plaatsen waarop wordt aangegeven dat er wordt gevlogen. Een ander voorbeeld is gemeente Den Haag, die bijvoorbeeld een webpagina erover heeft opgesteld: Den Haag - Proef met drone voor controleren van gebouwen

[58] Zie: https://www.nvwa.nl/over-de-nvwa/hoe-de-nvwa-werkt/drones-voor-de-bescherming-van-voedsel-dier-en-natuur

BIJLAGEN

1 – AI EN ALGORITMEN, EEN OVERZICHT VAN DE DIVERSE TYPEN
2 – BEGRIPPENLIJST
3 – BIBLIOGRAFIE
4 – DEELNERMERSLIJST VAN DE BUYER GROUP

BIJLAGE 1 – ALGORITMEN EN AI, EEN OVERZICHT VAN DIVERSE TYPEN

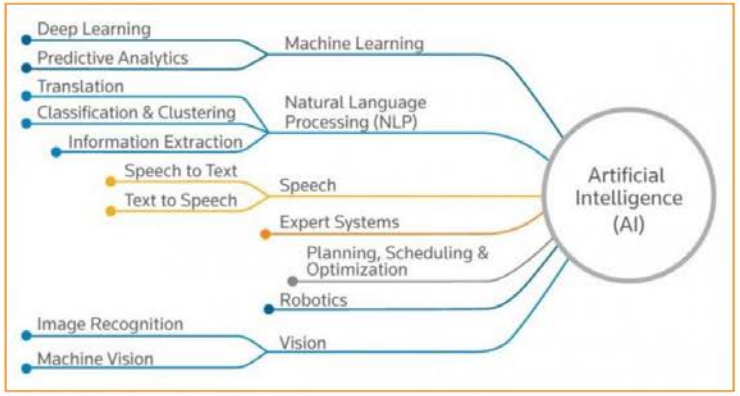
AI: EEN PARAPLUBEGRIP EN TYPEN MACHINE LEARNING

AI is een paraplubegrip waaronder veel verschillende technologieën vallen (zie figuur *AI technologieën*). Binnen AI wordt onderscheid gemaakt tussen:

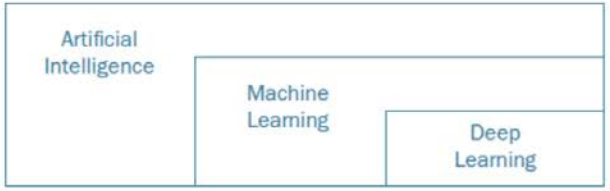
- **Regel-gebaseerde** algoritmen: mensen hebben regels opgesteld op basis waarvan het algoritme onderscheid maakt; en
- **Data-gedreven** algoritmen: het algoritme wordt getraind op basis van de invoer van data.

Er zijn veel typen data-gedreven algoritmen. Drie belangrijke categorieën zijn:

- **Supervised learning** (leren onder begeleiding en met behulp van menselijke interventie): betekent dat het algoritme gegevens als invoer krijgt en leert patronen te herkennen.
- **Unsupervised learning** (onbegeleid leren): leren zonder toezicht betekent dat het algoritme zelf categorieën creëert, zonder iets over de gegevens te weten.
- **Reinforcement learning** ('versterkingsleren'): betekent dat het algoritme op zoek gaat naar het meest optimale patroon zodat het de hoogst haalbare beloning kan ontvangen.



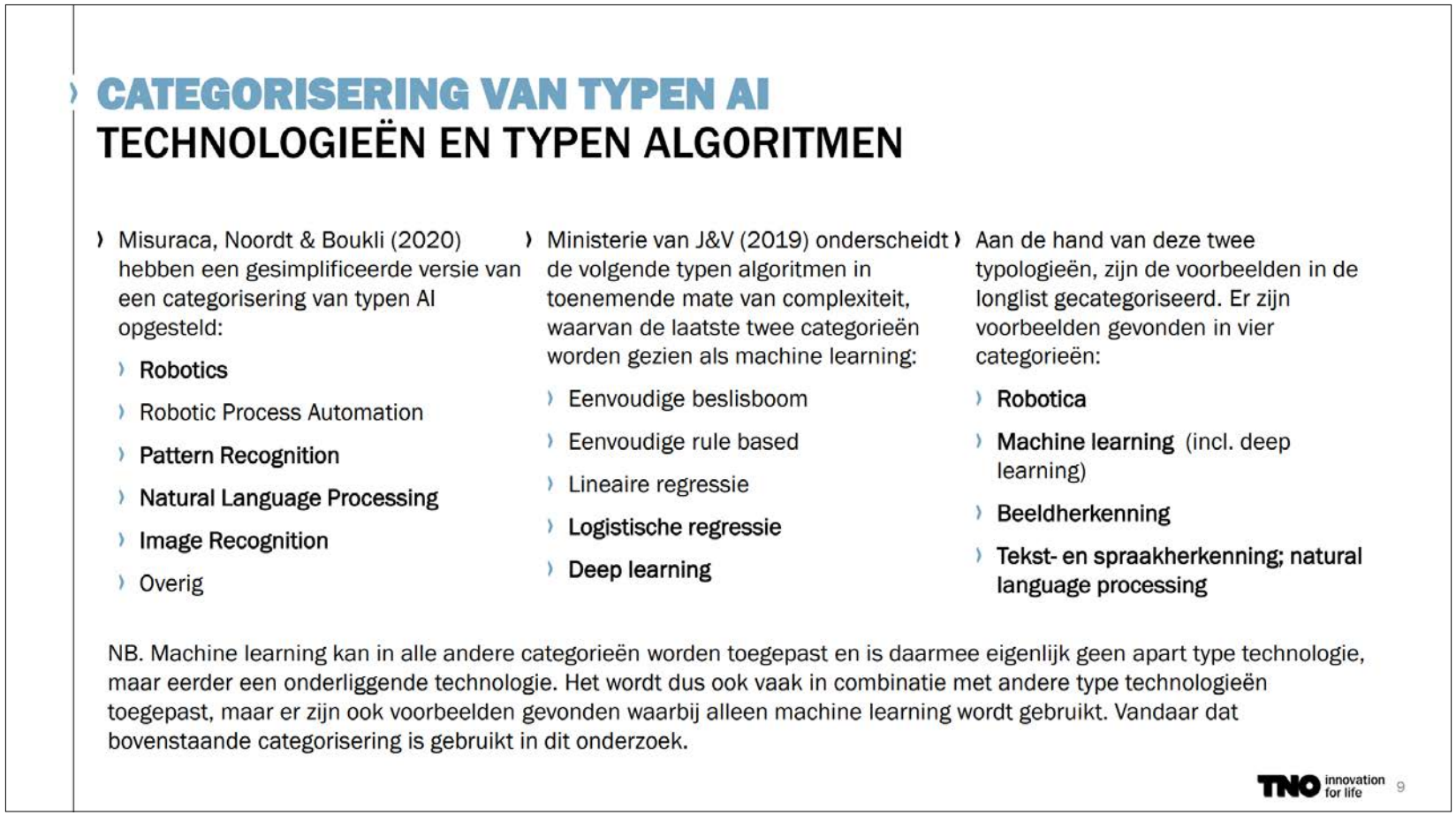
AI technologieën. Bron: Fong (2018)



Deep Learning als onderdeel van Machine Learning als onderdeel van AI. Bron: TNO (2018)

TNO innovation for life 8

Bron: Quickscan AI in publieke dienstverlening II, 2021, TNO (i.o.v. BZK)



Bron: Quickscan AI in publieke dienstverlening II, 2021, TNO (i.o.v. BZK)

BIJLAGE 2 – BEGRIPPENLIJST

De begrippen die hieronder in de lijst staan vermeld, worden in de hoofdtekst van dit rapport reeds nader toegelicht. Vandaar dat we hieronder de originele uitdrukking vermelden, maar geen verdere uitleg erover opnemen.

AVG	Algemene Verordening Gegevensbescherming
AI	Artificial Intelligence (ofwel; kunstmatige intelligentie)
AIIA	AI Impact Assessment
BIO	Baseline Informatiebeveiliging Overheid
CI/CD	Continuous Integration/Continuous Deployment
CSIR	CyberSecurity ImplementatieRichtlijn
CVE	Common Vulnerabilities and Exposures
DaaS	Drone as a service
DPIA	Data Protection Impact Assessment
HBOM	Hardware bill of materials
ICO	Inkoopeisen Cybersecurity Overheid
ICT	Informatie- en Communicatietechnologie
IEC	International Electrotechnical Commission
ILT	Inspectie Leefomgeving en Transport
IP	Internet Protocol
ISO	International Standardization Organization
IT	Information Technology
KPI	Kritieke Prestatie Indicatoren
LCM	Lifecycle Management
LiDAR	Light Detection And Ranging of Laser Imaging Detection And Ranging
NCSC	Nationaal Cybersecurity Centrum
NEN	Nederlandse Norm
NLAIC	Nederlandse AI Coalitie
NLR	Nationaal Lucht- en Ruimtevaartlaboratorium
NRTC	Netherlands Remotely Piloted Aircraft Systems Test Centre
NVWA	Nederlandse voedsel en waren autoriteit
PDCA	Plan Do Check Act
PDF	Portable Document Format
PIA	Privacy Impact Assessment
RPAS	Remotely Piloted Aircraft Systems
SBOM	Software Bill of Materials
SGOA	Stichting Geschillenoplossing Automatisering
TCAV	Testing with Concept Activation Vectors
U-space	Unmanned Aircraft System Traffic Management
Who	Wet hergebruik overheidsinformatie
XAI	Explainable AI

BIJLAGE 3 – BIBLIOGRAFIE

Actieplan Programma Onbemande Luchtvaart 2023-2025, kamerbrief
Ministerie van Infrastructuur en Waterstaat
https://www.rijksoverheid.nl/documenten/kamerstukken/2023/04/20/actieplan-programma-onbemande-luchtvaart-2023-2025

AI Impact Assessment – Het hulpmiddel voor een betrouwbaar AI-project
Ministerie van Infrastructuur en Waterstaat
https://www.rijksoverheid.nl/documenten/rapporten/2022/11/30/ai-impact-assessment-ministerie-van-infrastructuur-en-waterstaat

Algemene Rijksinkoopvoorwaarden bij IT-overeenkomsten Rijksoverheid
https://www.rijksoverheid.nl/onderwerpen/zakendoen-met-het-rijk/voorwaarden-voor-rijksopdrachten

Algoritmeregister en informatie over algoritmen
Nederlandse overheid
https://algoritmes.overheid.nl/nl
https://algoritmes.pleio.nl/

AI-whitepaper, een Europese benadering over kunstmatige intelligentie op basis van excellentie en vertrouwen
Europese Commissie
https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

AP Inzet Artificial Intelligence Act (maart 2022)
Autoriteit Persoonsgegevens
https://autoriteitpersoonsgegevens.nl/uploads/imported/ap_inzet_ai_act.pdf

Basismaatregelen cybersecurity
Nationaal Cybersecurity Centrum (NCSC)
https://www.ncsc.nl/onderwerpen/basismaatregelen

Beleid van de Nederlandse overheid voor het gebruik van open standaarden in haar ICT-systemen
https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/standaardisatie-en-architectuur/open-standaarden/

Bespreek digitale veiligheid met je IT-dienstverlener
Digital trust center, ministerie van Economische Zaken en Klimaat
https://www.digitaltrustcenter.nl/sites/default/files/2021-12/Praatplaat_digitale_veiligheid.pdf

Beslisboom Open Standaarden t.a.v. de 'Pas toe of leg uit'-lijst
Forum Standaardisatie
https://www.forumstandaardisatie.nl/beslisboom/beslisboom-open-standaarden

Brochure: AI-systemen, ontwikkel ze veilig
AIVD
https://www.aivd.nl/actueel/nieuws/2023/02/15/ai-systemen-ontwikkel-ze-veilig

Co-Creation Navigator
Waag
https://ccn.waag.org/

Digitale Overheid cybersecurity
https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cybersecurity/

Dronestrategie 2.0: Naar een grootschalige Europese dronemarkt
Europese Commissie
https://ec.europa.eu/commission/presscorner/detail/nl/ip_22_7076

Handreiking: Governance voor een verantwoorde toepassing van algoritmen
Berenschot
https://www.berenschot.nl/media/vf5fj1mw/handreiking_governance-voor-een-verantwoorde-toepassing-van-algoritmen.pdf

ICO-wizard (Inkoopeisen Cybersecurity Overheid)
Baseline Informatiebeveiliging Overheid (BIO)
https://www.bio-overheid.nl/ico-wizard/

ICT dossier van PIANOo Expertisecentrum Aanbesteden
https://www.pianoo.nl/nl/sectoren/ict

Kennisnet, toelichting op de AI Act (juni 2023)
https://www.kennisnet.nl/artikel/20477/de-ai-act-wat-kunnen-scholen-verwachten-van-deze-nieuwe-wet/

Modelbepalingen voor gemeenten voor verantwoord gebruik van Algoritmische toepassingen
Gemeente Amsterdam
Contractvoorwaarden voor algoritmen – Innovatie (amsterdam.nl)

Marktconsultatie rapportage (juli 2022)
Buyer Group AI beeldherkenning met drones
https://www.pianoo.nl/sites/default/files/media/documents/2022-09/marktconsultatie_bg_ai_beeldkrkenning_drones-juli2022.pdf

Nederlandse AI Coalitie Werkgroep Data Delen
https://nlaic.com/bouwstenen/data-delen/

Pels Rijcken – Contracteren van AI (presentatie door Jeroen Naves, november 2022)
https://www.pianoo.nl/nl/terugblik-cop-digitale-innovaties-hoe-koop-je-verstandig-algoritmische-toepassingen

Quickscan AI in publieke dienstverlening II
TNO i.o.v. BZK
Quickscan AI in publieke dienstverlening II | Rapport | Rijksoverheid.nl

Rapport: Aandacht voor algoritmes
Algemene Rekenkamer
https://www.rekenkamer.nl/publicaties/rapporten/2021/01/26/aandacht-voor-algoritmes

Rapport: Reference guide to federated and interoperable AI data spaces
Nederlandse AI Coalitie
https://nlaic.com/wp-content/uploads/2023/04/NL_AIC_Towards_a_federation_of_AI_data_spaces.pdf

Richtlijnen voor het toepassen van algoritmen door overheden en publieksvoorlichting over data-analyses
https://www.rijksoverheid.nl/documenten/richtlijnen/2021/09/24/richtlijnen-voor-het-toepassen-van-algoritmen-door-overheden-en-publieksvoorlichting-over-data-analyses

Software Bill of Materials (SBoM) en cybersecurity, onderzoeksresultaten
Nationaal Cybersecurity Centrum (NCSC)
https://www.ncsc.nl/onderzoek/onderzoeksresultaten/software-bill-of-materials-sbom-en-cyber-security-map

Tada Manifest, voor een verantwoorde digitale stad
https://tada.city/

Verantwoord vliegen Luchtvaart nota 2020-2050
Ministerie van Infrastructuur en Waterstaat
https://www.rijksoverheid.nl/documenten/rapporten/2020/11/20/bijlage-1-luchtvaartnota-2020-2050

Wet hergebruik van overheidsinformatie
https://wetten.overheid.nl/BWBR0036795/2016-10-01

BIJLAGE 4 – DEELNEMERSLIJST VAN DE BUYER GROUP

Lijst van personen die afgelopen jaren deelnamen aan deze Buyer Group als aanspreekpunt en die voornamelijk een bijdrage leverden:
(vermelding organisatie ten tijde van gesprek/deelname)

- Peter de Jong - Product manager maatwerk (Kadaster)
- Gerbrand Vestjens - Specialist Geo Data (Kadaster)
- Ariea Vermeulen – Coördinator programma drones (RWS)
- Marcel Vos - Expert Vastgoed en Infrastructuur (RWS)
- Rob Broekman - Pijlerhoofd Remote Sensing en Drones (NVWA (InnovatieLab)
- Okan Okkuscu - AI Specialist Innovatielab (NVWA (InnovatieLab)
- Klaas Jan Russcher – Robotica onderzoeker Politie (Nationaal Politielab AI)
- Darko Brodic – Project manager UAS (Douane)
- Marlies van der Goot - Adviseur geo-informatie (ProRail)
- Evelyn Uittenbogaard - Tendermanager AM & ICT (ProRail)
- Stoffel Bos - Information security officer (ProRail)
- Andrea Westendorp (ProRail, voorheen WDODelta)
- Coen Bergman - Strategisch adviseur & Team Lead bij directie Digitalisering en Innovatie (Gemeente Amsterdam)
- Hans Nouwens - Project manager Smart City (Gemeente Breda)
- Ivonne Jansen - Strategisch Adviseur Technology, Society and Ethics (Provincie Zuid-Holland)
- Jeroen Waanders – Adviseur innovatie (WDO Delta)
- Rob de Lange - Corporate Information Security Officer (Provincie Overijssel, voorheen WDODelta)
- Leonie de Wilde – Inkoopadviseur en Contractmanager (Waterschapshuis)
- Sanne Wijnhorst - Manager Inkoop (Waterschapshuis)

COLOFON

Deze publicatie is een resultaat van de Buyer Group en geschreven in samenwerking met de deelnemers, onder begeleiding van:

- Rolf Zeldenrust (senior adviseur innovatie en markt, PIANOo)
- Joris Krüse (innovatiestrateeg, Studio Kidman & Nicholson)

Bent u enthousiast over deze Buyer Group, wilt u van gedachten wisselen of verbeteringen aandragen, of op de hoogte blijven? Neem dan contact op via buyergroups@pianoo.nl.

Illustratie, ontwerp en productie
Studio Kidman & Nicholson (voorpagina gegenereerd met AI)
PIANOo
Xerox | Osage

PIANOo Expertisecentrum Aanbesteden
Rijksdienst voor Ondernemend Nederland
info@pianoo.nl | www.pianoo.nl