Biometrie in militaire operaties

Tegenstanders in missiegebieden bedienen zich graag van anonimiteit, waardoor het moeilijk kan zijn ze te vinden. Biometrie (vingerafdrukken, DNA, irisscan, gezichtsherkenning, stem) kan bij deze zoektocht een cruciale rol spelen doordat hiermee een onweerlegbaar verband kan worden gelegd tussen personen onderling, personen en incidenten, personen en wapens, en verschillende aangetroffen goederen. Inzet van biometrie tijdens missies kan een bijdrage leveren aan het operationeel effect, de veiligheid van het eigen personeel en de nationale veiligheid. Snel en met wetenschappelijke nauwkeurigheid kunnen uitspraken worden gedaan over de identiteit van personen. Een groot voordeel is het verminderen van collateral damage als gevolg van misidentificatie tijdens het targeting proces waardoor het draagvlak bij de lokale bevolking wordt verstevigd. Het hoge tempo heeft als voordeel dat we maximaal gebruik maken van het verrassingseffect. Ook de NAVO zet in op de ontwikkeling van biometrie.

Drs. J. van Kleef – luitenant-kolonel van de Koninklijke Marechaussee [*]

Met de toenemende globalisering en een steeds mobielere wereldbevolking is het voor tegenstanders (individuen en netwerken) eenvoudig om missiegebieden in- en uit te reizen. Iemand kan de ene maand bezig zijn met de productie en verspreiding van IED's in Afghanistan, zich de maand erop naar de Kaukasus begeven, om vervolgens te vertrekken naar het Midden-Oosten, Noord-Afrika of de Balkan. Militaire eenheden daarentegen gaan naar één missiegebied om daar te strijden tegen een specifieke (liefst herkenbare) tegenstander die zich, zodra hij het risico loopt zichtbaar te worden, kan verplaatsen naar een voor hem veilige plaats buiten het missiegebied of op kan gaan in de lokale bevolking. Verplaatsbaarheid over grenzen is het grote voordeel van de tegenstander ten opzichte van de eenheden in het missiegebied. Hierdoor wordt het vinden van de tegenstander bemoeilijkt. Biometrie kan bij deze zoektocht een cruciaal stuk van de puzzel leveren.

De NAVO heeft het gebruik van biometrie in militaire operaties om (mogelijke) tegenstanders te kunnen identificeren aangemerkt als leemte.[1] NAVO-landen passen wel biometrie toe (Nederland in de Task Force Uruzgan bijvoorbeeld), maar het gebruik is binnen de alliantie nog niet systematisch. Nederland

* Jeroen van Kleef is werkzaam bij het cluster Integrale Plannen & Advies van de staf Koninklijke Marechaussee. Hiervoor was hij verbonden aan het Defensie Expertisecentrum C-IED. Binnen het bureau Attack the Network was hij, samen met Elnt R. Breen (KMar), verantwoordelijk voor biometrie.

1 NATO Biometric Framework *Concept of Biometrics in Support of Operations* (MCM 0050-2012

heeft zich tijdens de NAVO-top van 2012 in Chicago bereid verklaard op te treden als *lead nation* op dit gebied, met als hoofdtaken het ontwikkelen en laten publiceren van doctrine, het incorporeren van biometrische capaciteiten in (NAVO)oefeningen en het ontwikkelen van (technische) standaarden.

Doelstelling en opbouw artikel

Het doel van dit artikel is tweeledig: het uiteenzetten van het belang van biometrie en hoe dit kan bijdragen aan militaire inzet, en het geven van bredere bekendheid aan de door Nederland geschreven NAVO-doctrine over het onderwerp. Eerst wordt het belang van biometrie uitgelegd. Het gaat daarbij om de effectiviteit van de operatie, de veiligheid van eigen troepen en nationale veiligheid. Vervolgens wordt nader ingegaan op het proces zoals beschreven in de doctrine en wordt stilgestaan bij keuzes en overwegingen in elke stap. De *Allied Intelligence Publication-15* (STANAG 6515) is daarbij de basis.

Het belang van biometrie

Situatie

Het vinden van de tegenstander (netwerk of individu) kan ernstig bemoeilijkt worden doordat hij bewust onzichtbaar wil zijn. Hij kan gebruik maken van veel en snelle verplaatsingen binnen en buiten een missiegebied, zich bedienen van aliassen, et cetera. Intelligence is lange tijd gefocust geweest op materieel, concentraties van eenheden en de omvang en capaciteiten van een reguliere tegenstander. Het is evident dat dit nog steeds belangrijk is en ook weer aan belang wint, maar de focus op het individu en de netwerken waarbinnen het

FOTO US ARMY, R. PORTER

Het registreren van personen in een biometrisch identificatiesysteem, zoals hier in de gevangenis van Khowst in Afghanistan, verscherpt de focus op individuen en de netwerken waarin zij zich bewegen

Biometrische kenmerken en modaliteiten

Een biometrisch kenmerk is een biologische en gedragsmatige karakteristiek van een individu waarvan onderscheidende, herhaaldelijke kenmerken kunnen worden vastgesteld waarmee de uniciteit van een persoon kan worden bepaald. Er zijn meerdere soorten biometrische kenmerken met elk specifieke voor- en nadelen voor toepassing in militaire operaties. De meest gebruikte modaliteiten zijn vingerafdruk, irisscan, gezichtsherkenning, stemherkenning en DNA. Daarnaast is er bijvoorbeeld toetsenbordaanslag (toepassing in cyberdomein) en hartslagritme, maar die laat ik in dit artikel buiten beschouwing.

De voor- en nadelen en mogelijke militaire toepassingen van de modaliteiten zijn:

- Vinger- en handafdrukken kunnen worden onderscheiden in 'live' en 'latent'. Live vingerafdrukken zijn vingerafdrukken die live zijn afgenomen van een persoon, door middel van inkt en papier of elektronisch. In NAVO-jargon heet dit *enrollment*. Daarnaast wordt gesproken van *latent prints* bij vingerafdrukken die als sporen worden aangetroffen op goederen. Vingerafdrukken hebben als grote voordeel dat ze achterblijven op door een tegenstander gebruikte middelen. Daarmee kunnen deze middelen en de incidenten die ermee veroorzaakt zijn worden gelinkt aan mensen. Ook kan worden vastgesteld dat meerdere personen aan elkaar te linken zijn als er vingerafdrukken van meerdere personen zijn. Hiermee kan een netwerkanalyse beginnen. Niet elke latente vingerafdruk is (automatisch) te verwerken: de kwaliteit moet daarvoor wel voldoende zijn.

- De irisscan wordt veel gebruikt voor toegang tot bijvoorbeeld een compound. Het voordeel is dat het zeer snel werkt en met grote zekerheid. Maar omdat een iris evident geen sporen achterlaat, is de toepassing enigszins beperkt.

- Gezichtsherkenning heeft als groot voordeel dat toepassing van grotere afstand mogelijk is, zonder dat de geregistreerde persoon zich hiervan bewust is. In de praktijk is het niet altijd goed toepasbaar vanwege verandering in gezichtsbeharing en bewuste afdekking van het gezicht.

- Stemherkenning kan worden toegepast bij onderschepping van communicatie van de tegenstander. Hierbij kunnen niet alleen verschillende personen aan elkaar gelinkt worden, maar ook de communicatiemiddelen. Maakt een persoon gebruik van meerdere middelen, of andersom, meerdere personen van één telefoon of een ander apparaat, dan kan dit op zichzelf interessante informatie zijn.

- DNA heeft, net als (latente) vingerafdrukken, het grote voordeel dat de tegenstander dit kan achterlaten als spoor. Het kan gaan om een haar, een stukje huid of bloed. Daarnaast kan met DNA een hoge mate van betrouwbaarheid worden verkregen in het vaststellen bij welke persoon een DNA-spoor hoort (of juist niet).

Multimodale biometrie is de combinatie van twee of meer modaliteiten. Dit is beter voor zowel de bruikbaarheid als de betrouwbaarheid. Als bij het enrollen bijvoorbeeld vingerafdruk, iris, aangezicht en stem worden vastgelegd en in een document opgeslagen, kan het systeem op meerdere modaliteiten een match vinden. Mocht een latente vingerafdruk matchen met een liveregistratie (volledige enrollment), dan kan de aangezichtsfoto meteen worden gebruikt in briefings of een targetinglijst.

Figuren 1 en 2 De veranderende operationele omgeving

individu zich beweegt wordt tevens belangrijker. Acties van een individu kunnen immers strategische en politieke gevolgen hebben.

Veiligheid eigen troepen

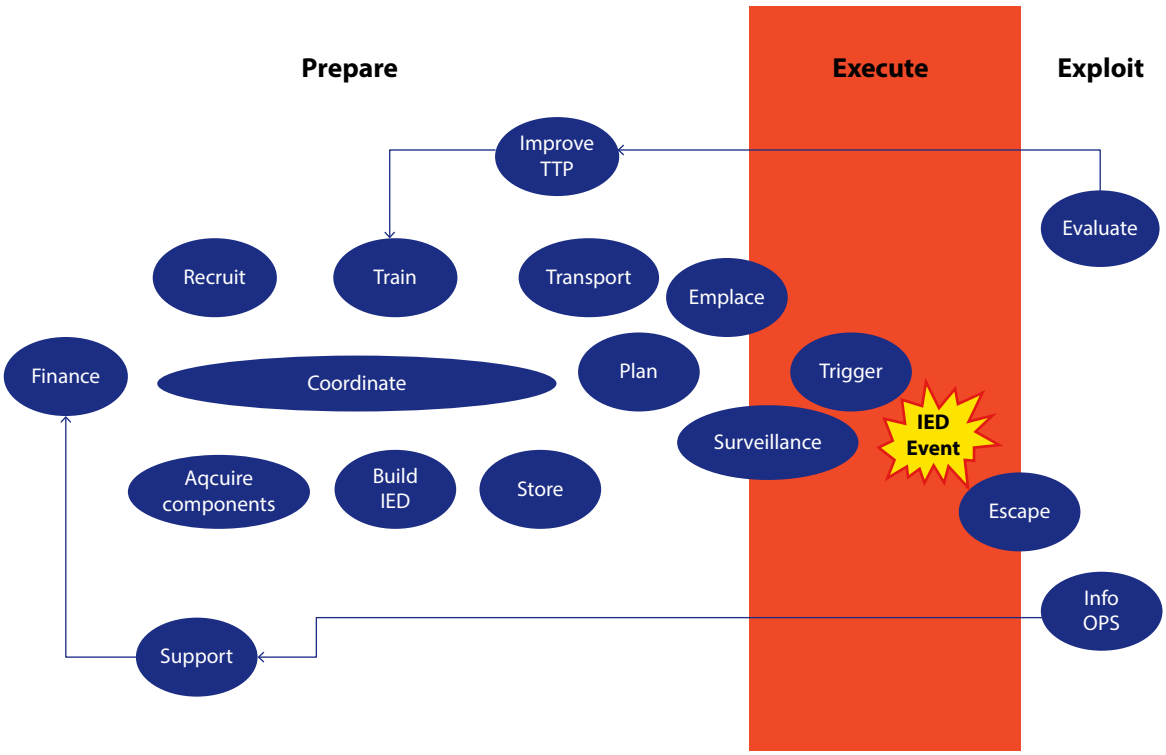
Het concept van biometrie is bij Defensie als aandachtspunt voortgekomen uit de Counter IED als onderdeel van Attack the Network, één van de drie pijlers van de C-IED doctrine,[2] naast Prepare the Force en Defeat the Device. De eerste reactie tegen IED-dreiging was fysieke bescherming door middel van bepantsering. Daarnaast speelde in deze fase het vergroten van de bewustwording een grote rol. Daarna is Defensie zich gaan richten op het *jammen* van signalen die IED's doen afgaan. Een derde pijler onder het concept is het principe van Attack the Network: proberen zicht te krijgen op het netwerk achter de bommenlegger en proberen zoveel mogelijk *left of the boom* (de benodigde activiteiten voordat een aanslag kan worden gepleegd, zie figuur 3) te komen, door zich te richten op de planning, productie en financiering van een IED-netwerk.[3]

Vanuit deze ontwikkeling is de behoefte aan het gebruik van biometrie binnen de krijgsmacht voortgekomen: onder meer door analyse van sporen en gebruikte technieken van bommenmakers wordt geprobeerd een netwerk in kaart te brengen (zie verder paragraaf 4). Door steeds eerder in het proces van een dreigingsnetwerk te kunnen storen, ontstaat de kans verder left of the boom te komen en initiatief (over) te nemen. Hierdoor kunnen aanslagen in missiegebieden worden voorkomen. Naast het vergroten van de veiligheid voor eigen troepen zal dit ook bijdragen aan een verbeterd veiligheidsgevoel van de lokale bevolking, een van de oogmerken van de commandant.

Voor het doorlichten van lokaal veiligheidspersoneel kan biometrie worden ingezet. Men kan nagaan of vingerafdrukken of DNA van dit personeel in verband te brengen is met acties tegen eigen troepen of die van de *host nation.* Hiermee kan de dreiging van *insider threat* worden teruggebracht. Ook kunnen deze resultaten worden ingevoerd in een database van vergelijkbare gegevens van coalitiepartners, waaruit kan blijken dat een persoon niet zou moeten worden toegelaten tot een nationale veiligheidsdienst.

Heel concreet is biometrie ook bruikbaar voor toegangscontrole op een basis. Parallel aan het voorbeeld hierboven kunnen mensen die toegang willen krijgen op een basis worden gecontroleerd op 'biometrische antecedenten'. Toegang kan vervolgens worden verkregen op basis van een irisscan. Ook is zo heel eenvoudig vast te stellen of een persoon veel moeite doet om op een basis te komen werken. Het kan

2 *Allied Joint Doctrine For Countering – Improvised Explosive Devices* - AJP- 3.15(C).
3 Idem.



Figuur 3 Attack the Network betekent zicht krijgen op het netwerk van een aanslagpleger

bijvoorbeeld zijn dat een persoon op meerdere, ver uit elkaar liggende locaties gepoogd heeft aan het werk te gaan, wat vragen oproept.

Operationeel effect

Een bekende uitspraak van Von Clausewitz is dat, in een gewapend conflict, veel inlichtingenrapporten in tegenspraak met elkaar zijn, dat er nog meer onjuist zijn en dat de meerderheid onbetrouwbaar is.[4] Maar de mogelijkheden om betrouwbaarheid van informatie of intelligence te toetsen nemen steeds meer toe. En hoe beter de informatiepositie ten opzichte van een

FOTO MCD, E. KLIJN

Het trainen van politieagenten in Afghanistan: door het verzamelen van sporen op aangetroffen goederen kunnen onweerlegbare verbanden worden gelegd tussen personen, personen en incidenten of personen en wapens

4 Carl von Clausewitz, *On War* (Princeton, Princeton University Press, 1989) 117.

tegenstander is, hoe effectiever de commandant zijn middelen kan inzetten. Biometrie kan een onweerlegbaar verband leggen tussen personen onderling, personen en incidenten, personen en wapens, en verschillende aangetroffen goederen als hier vergelijkbare sporen op zijn gevonden.

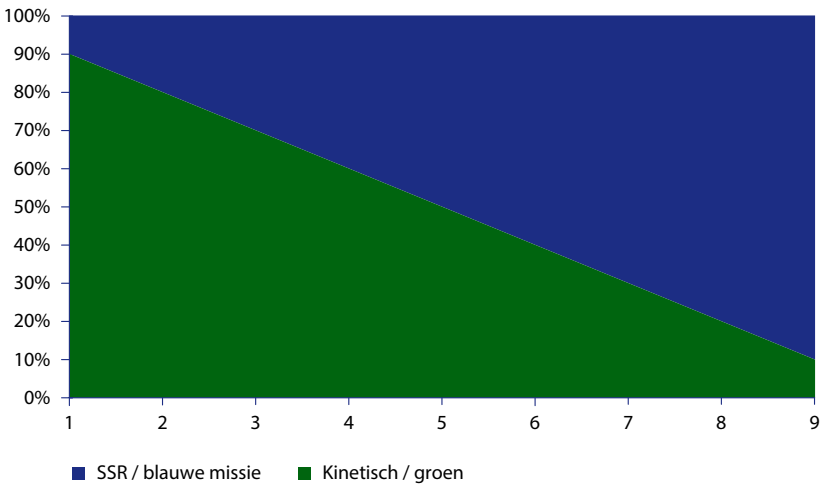
Met wetenschappelijke nauwkeurigheid kunnen uitspraken worden gedaan over de identiteit van personen. Een groot voordeel is dus het verminderen van *collateral damage* als gevolg van misidentificatie tijdens het *targeting* proces.[5] Door het verminderen van collateral damage en het verwijderen van 'stoorzenders' binnen een operatiegebied, zal het gebied overzichtelijker worden en wordt tevens het draagvlak bij de lokale bevolking verstevigd.

Bij contact met een individu (dit kan zijn bij een checkpoint, tijdens een huiszoeking, of personeel van Defensie wordt zelf benaderd) kan er reden zijn deze persoon te registeren. De tijd tussen het eerste contact en het vaststellen/ registeren van de identiteit is zeer kort doordat de verwerking van data geautomatiseerd is. De militair die de identiteit vaststelt krijgt (near) real-time een response van het identificatie/ registratiesysteem wat de status van de persoon is, zoals: bekende dreiging/geen dreiging/ onbekend. Deze real-time feedback biedt de kans om meteen een actie aan een nieuw feit te koppelen, bijvoorbeeld iemand meteen meenemen voor nader onderzoek.

Biometrie maakt het identificatieproces niet alleen betrouwbaarder, maar ook een stuk sneller door automatisering. Hierdoor kunnen acties elkaar sneller opvolgen. Ter illustratie: op basis van informatie wordt iemand aangehouden en onderzocht. De biometrische informatie die dit oplevert (deze persoon blijkt biometrisch te linken aan andere personen), eventueel gecombineerd met informatie uit telefoon, USB, wapens, of andere zaken, kan heel snel leiden tot een volgende zoekactie, en de informatie die hieruit voortkomt meteen weer tot een volgende. Zo kunnen militairen het initiatief houden dan wel overnemen en het verrassingseffect maximaal uitbuiten, want de tegenstander heeft steeds minder tijd om zich te verschuilen.

Ook voor het vaststellen van de identiteit overledenen kan biometrie worden gebruikt. Zo kan biometrie voor eigen personeel ingezet worden om vast te stellen of iemand daadwerkelijk is aangetroffen (mogelijk aan de hand van vingerafdrukken, anders aan de hand van DNA). Daarnaast is biometrie bruikbaar bij het beoordelen van het resultaat van een actie (*battle damage assessment).* Wanneer met zekerheid kan worden vastgesteld dat een belangrijk doelwit is uitgeschakeld, kan dat van de lijst worden verwijderd.

5 *Targeting* is het cyclische proces van het selecteren en prioriteren van doelen en deze koppelen aan passende oplossingen, rekening houdend met de operationele behoefte en eigen mogelijkheden. Een *target* is een gebied, object, persoon, organisatie, gedachtegoed, denkproces, houding of een gedragspatroon, te beïnvloeden door het inzetten van capaciteit. *Targeting* verbindt daarmee het inlichtingenproces met operaties (Doctrine Publicatie 3.2: Landoperaties).



Figuur 4 In de loop van een missie is er steeds meer behoefte aan fijnkorrelige (en onder meer biometrische) informatie. Het percentage vormt een kunstmatige verdeling tussen de 'groene' en 'blauwe' inspanningen tijdens een missie

Ten slotte zal, naarmate een operatie in tijd vordert, de informatiebehoefte wijzigen. Het is aannemelijk dat de doelen in de beginfase meer gegroepeerd en geconcentreerd zijn dan na verloop van tijd. Tegenstanders zullen hoofdkwartieren kwijtraken en groepen zullen splitsen in kleinere groepen en willen opgaan in de lokale bevolking. Met het concept van vinden-binden-slaan in gedachten zal het vinden van de vijand in een beginfase nog relatief eenvoudig zijn ten opzichte van binden en slaan. Als grotere doelen, zoals wapenopslagplaatsen en hoofdkwartieren, eenmaal zijn uitgeschakeld, zal het vervolgens relatief veel inspanning kosten om de enkele man of zijn netwerk te vinden. Eenmaal gevonden zullen de stappen binden en slaan relatief weinig inspanning of vuurkracht vereisen. Het zwaartepunt van de inspanning gaat daarmee na verloop van tijd van slaan naar vinden. Daardoor zal de operatie en daarmee de informatiebehoefte steeds meer verschuiven van 'groen' naar 'blauw' en op personen en netwerken gericht zijn, inclusief criminele samenwerkingsverbanden (zie figuur 4).

Interne/externe veiligheidsnexus (nationale veiligheid)

Ook in het kader van nationale veiligheid heeft biometrie meerdere toepassingsmogelijkheden. Biometrie kan als een satéprikker door verschillende domeinen (militair, rechtshandhaving, grensbewaking) gestoken worden om erachter te komen of individuen in meerdere databases voorkomen. Het zou bijvoorbeeld interessant zijn om van bepaalde reizigers of asielzoekers in het grensproces, dan wel in een IND-proces, na te gaan of ze voorkomen in een militaire database met biometrische gegevens. Dit hoeft niet geautomatiseerd te zijn, maar kan op basis van bepaalde indicatoren worden besloten. Of het kan voor de commandant ter plaatse interessant zijn te weten welke mensen uit Europese landen naar zijn missiegebied zijn gereisd. Deze kunnen op een *watch list* worden geplaatst en met biometrie is vast te stellen of de gezochte inderdaad degene is die is aangehouden, dan wel overleden in het missiegebied. Als laatste voorbeeld kan gedacht worden aan sporen op explosieven die worden *gematcht* met biometrische gegevens uit missiegebieden. Hieruit kan een beeld van een netwerk ontstaan dat de politiekorpsen inzicht geeft in wie er mogelijk bij betrokken zijn en mogelijk kunnen worden aangehouden voordat dit netwerk een volgende aanslag pleegt (zie figuur 5).

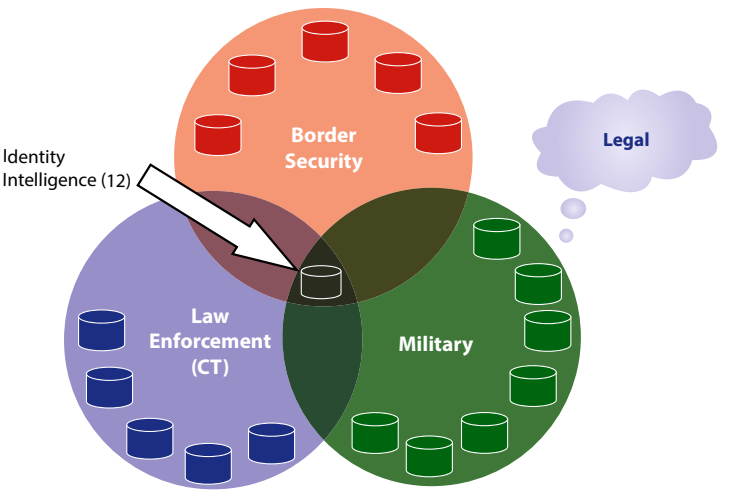
Een belangrijk aspect is wel dat dit binnen de juridische randvoorwaarden gebeurt en

momenteel zijn die niet zodanig dat dit tot de mogelijkheden behoort. De wet- en regelgeving die hierin een rol speelt is voornamelijk artikel 8 van het Europees Verdrag van de Rechten van de Mens (EVRM) en de Wet Bescherming Persoonsgegevens, waarmee het recht op privacy wordt gewaarborgd. Er kunnen uitzonderingen worden gemaakt in geval van bedreiging van de staatsveiligheid en dan moet per geval worden afgewogen wat zwaarder weegt: de privacy van een individu of een (mogelijke) dreiging tegen de (staats)veiligheid. Hierbij zijn noodzakelijkheid, proportionaliteit en subsidiariteit de kernbegrippen.

In een scriptie over deze problematiek van Dayna de Boer, in opdracht van het Defensie Expertisecentrum C-IED (DEC C-IED), is dit nader onderzocht. De hoofdconclusie luidde: 'Uit het onderzoek is gebleken dat de verwerking van persoonsgegevens zowel nationaal als internationaal is gebonden aan strikte regelgeving. Daarnaast dient bij afwijking sprake te zijn van voldoende motivering, met name op het gebied van doelbinding. Dit heeft geleid tot de conclusie dat het delen van biometrische gegevens in het kader van terrorismebestrijding wel mogelijk is, echter dat het doel van de maatregel goed gemotiveerd dient te worden. Toetsing door het EHRM of de nationale rechters is hierbij onvermijdelijk.'[6]

Aan de hand van de onderzoeksresultaten zijn aanbevelingen gedaan aan het DEC C-IED. Eén aanbeveling is het onderzoeken van mogelijkheden om een samenwerkingsverband te ontwikkelen met de inlichtingendiensten. Daarnaast dient er een voorstel te komen dat het verwerken van reeds verzamelde (of nog te verzamelen) persoonsgegevens toelaat.

Wellicht is het noodzakelijk om bij missieplanning in het kader van doelbinding al rekening te houden met tijdens de missie gegenereerde (persoons)informatie. Als we constateren dat interne- en externe veiligheid steeds meer vervlochten zijn, zou het logisch zijn de inspanningen en de daarvoor benodigde informatie ook te verweven.



Figuur 5 Biometrie als een satéprikker door informatie in verschillende domeinen gestoken

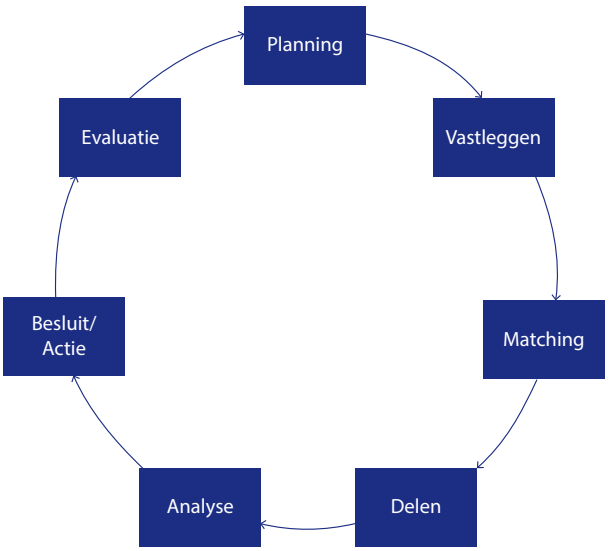
Het biometrisch proces

Bovenstaande maakt duidelijk dat het belangrijk is om te kunnen identificeren wie zich – en met welke bedoelingen – ophouden in het missiegebied of specifiek de Area of Responsibility (AOR). Steeds meer NAVO-landen merken biometrie daarom aan als belangrijke capaciteit. De NAVO-definitie van biometrie is: *the automated recognition of individuals based on their behavioural and biological characteristics*. Biometrie is een inlichtingeninstument, specifiek inzetbaar ten behoeve van Identity Intelligence. In deze paragraaf wordt nader ingegaan op het biometrieproces, een beknopte versie van het proces beschreven in de eerder genoemde AINTP-15.

Planning

Allereerst moet bepaald worden wat de informatiebehoefte is. Vervolgens kan worden vastgesteld welke biometrische informatie moet worden verzameld. Er kan bijvoorbeeld worden gekozen voor multimodale biometrie, dat wil zeggen een combinatie van modaliteiten

6 Dayna de Boer, *Samen spelen, samen delen. Een onderzoek naar de juridische mogelijkheden voor het delen van biometrische gegevens ter identificatie van vermeende terroristen* (op verzoek bij auteur verkrijgbaar).



Figuur 6 De stappen in het biometrisch proces, zoals ook beschreven in Allied Intelligence Publication-15

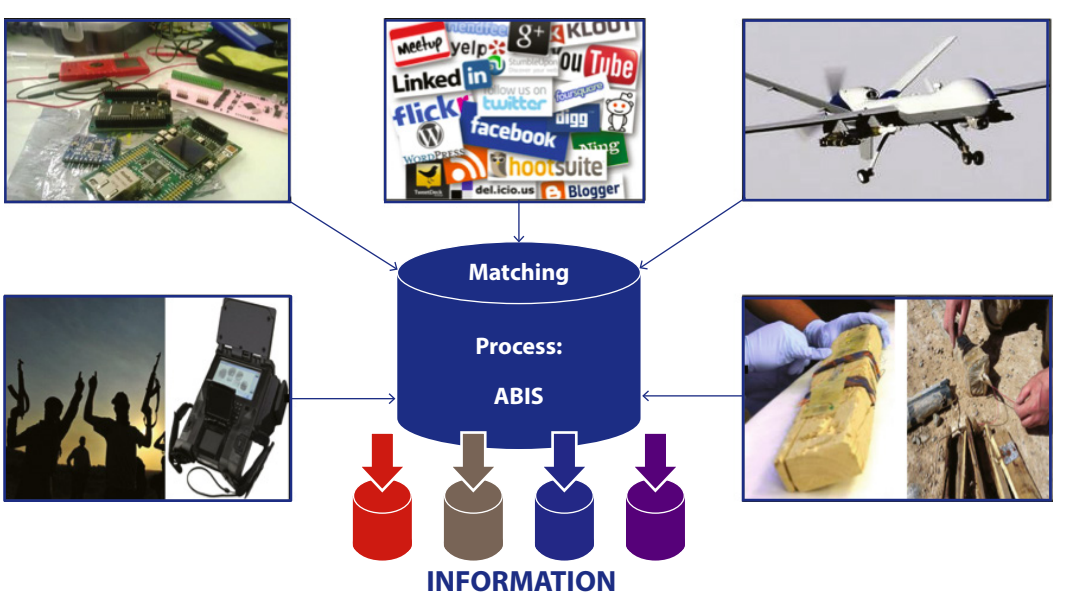
zoals vingerafdrukken met gezicht. Daarnaast moet dan bepaald worden met welke sensoren de informatie wordt verzameld. Ook zullen eventuele juridische beperkingen (omschreven in de Rules of Engagement), alsmede culturele aspecten van de lokale bevolking, in ogenschouw moeten worden genomen.

Vastleggen

In de doctrine is de definitie van vastleggen: '[Biometric] Capture: collecting or attempting to collect a signal(s) from a biometric characteristic(s), or a representation of a biometric characteristic(s), and converting the signal(s) to a captured biometric sample set. (ISO/IEC JTC1/SC 37).'

Aan de hand van de figuur 7 worden vijf verschillende manieren besproken om biometrische kenmerken vast te leggen. Uiteraard sluiten deze elkaar niet uit, maar vullen ze elkaar aan. Als een bepaalde persoon of groep het waard is, kunnen meerdere sensoren worden ingezet waarvan de resultaten elkaar zullen versterken.

Linksonder in de figuur is een *capture device* afgebeeld, een apparaat om een persoon biometrisch te registreren. Hiermee kan de militair van een individu het gezicht, vingerafdruk, iris, en stem vastleggen, plus relevante contextuele (locatie, aanleiding, andere bijzonderheden) en biografische informatie (naam, geboortedatum, en andere gegevens). Ook kunnen foto's worden opgeslagen van mogelijk interessante items en documenten. Het registreren van personen kan als indringend



Figuur 7 Vastleggen, matchen en verwerken van biometrische informatie

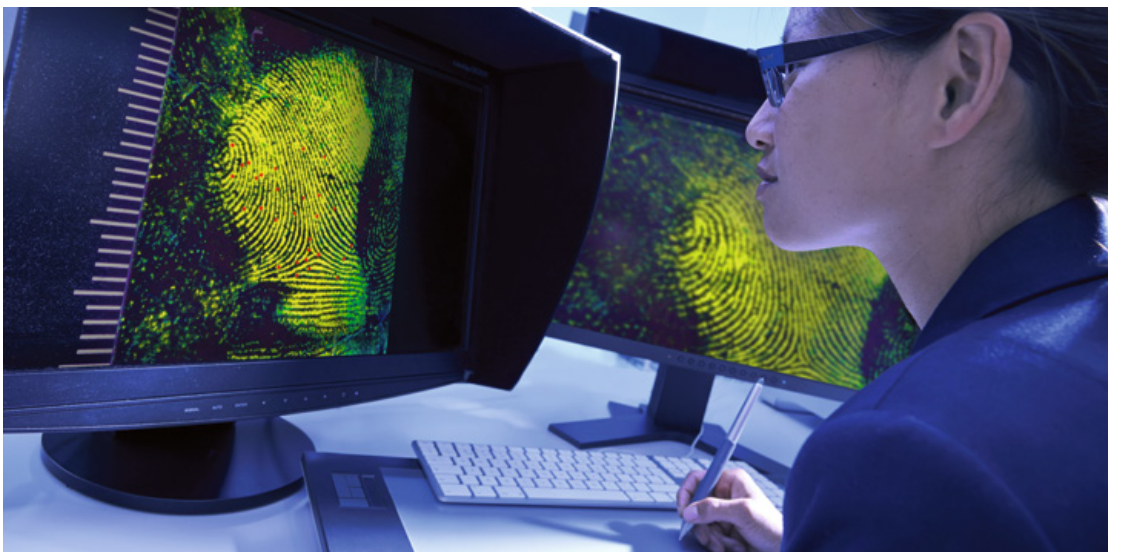


FOTO NEDERLANDS FORENSISCH INSTITUUT

Vingerafdrukken vormen een biometrisch spoor dat via gerichte acties tegen personen of groepen gevolgd kan worden

en onaangenaam worden ervaren en daarom dient zeer precies te worden bepaald welke informatiebehoefte het afnemen van biometrie vervult en hoe kan worden voorkomen dat onnodig veel weerstand ontstaat.

Een tweede mogelijkheid is het gebruik van Document and Media Exploitation (DOMEX). Dit houdt onderzoek in van aangetroffen of buitgemaakte telefoons, computers, USB-sticks of cd-roms, waarbij specifiek wordt gelet op foto's en video's met gezichten, eventueel in combinatie met stemherkenning (bij video's). Bruikbaar materiaal kan vervolgens met vergelijkingssoftware worden vergeleken met bestaande biometrische data.

Een derde manier om informatie te verzamelen is via Open Source. Dit werkt vergelijkbaar met DOMEX: het is mogelijk om gezichten en stemfragmenten te verzamelen van bijvoorbeeld propagandavideo's die zijn verspreid door de tegenstander. Bruikbare biometrische informatie wordt geëxtraheerd, gerangschikt en gematcht met bestaande biometrische data.

Stand-off vastlegging is een vierde mogelijkheid. Dit is het gericht verzamelen van biometrische informatie van een bepaald individu, maar van een grotere afstand en over het algemeen zonder dat betrokkene zich hiervan bewust is. Het eenvoudigste voorbeeld zijn foto of filmbeelden, waarbij met name het gezicht gebruikt wordt ter vergelijking. Maar ook de *gait*, de manier van lopen van een persoon, (trekkend, mank, of anders) valt onder biometrie. Dit is ook 's nachts waarneembaar. Ook valt bij stand-off te denken aan radioverkeer, waarmee stemmen opgeslagen kunnen worden om vervolgens stemherkenning te doen.

De vijfde categorie is enigszins afwijkend van de vier voorgaande en draait om het veiligstellen van biometrische sporen, nog zonder dat deze te koppelen zijn aan een persoon. Hierbij kan het gaan om zowel vingerafdrukken als DNA. Voor de hand liggende interessante items waar dit materiaal op kan zitten zijn (hand)wapens, IED's, documenten, pakketten drugs en geld. Ook is het mogelijk om bij een gerichte actie tegen een persoon of groep deze te volgen en actief te kijken waar ze sporen achterlaten (waterflesjes of sigarettenpeuken). Zodoende is belangrijk identificerend materiaal met zekerheid aan personen te koppelen. Uiteraard dient dit met de juiste waarborgen omgeven te worden. Ook dient het betrokken personeel over de juiste forensische vaardigheden te beschikken om een spoor identificerend en bruikbaar te houden. De sporen kunnen vervolgens worden opgewerkt in

een daartoe ingericht lab zoals het JDEAL, het *Joint Deployable Exploitation & Analysis Laboratory*, momenteel onder Nederlandse leiding en gevestigd in Soesterberg.

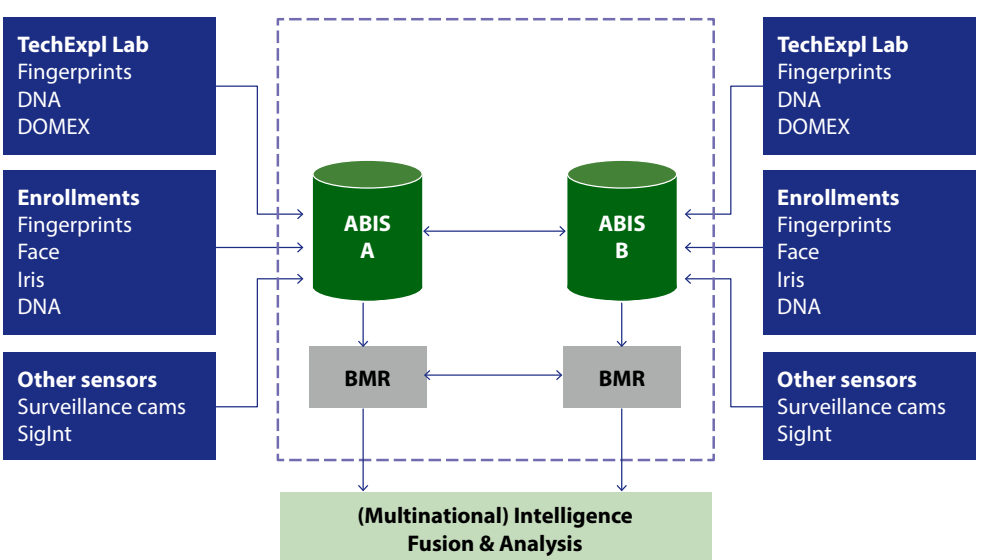
Matching

Voor de matching van biometrische gegevens wordt de zogeheten ABIS ingezet, het Automated Biometric Identification System. De output van de ABIS is een rapport waarin de resultaten van de match worden weergegeven. Centraal in figuur 7 staat de ABIS afgebeeld. Dit is het centrale punt waar de biometrische informatie wordt opgeslagen, geanalyseerd en gerapporteerd.
In gevallen waarbij een match wordt gerapporteerd op basis van iris, is het met aan zekerheid grenzende waarschijnlijkheid vast te stellen dat het hier inderdaad om dezelfde persoon gaat. De irisscan geeft een zeer hoge betrouwbaarheid. Maar wanneer een match wordt gevonden op basis van latente vingersporen, zal een nadere analyse van een dactyloscopist nodig zijn omdat automatische vergelijking van kwalitatief soms slecht 'leesbare' sporen onvoldoende uitsluitsel biedt.

Delen

De effectiviteit van het gebruik van biometrie is grotendeels afhankelijk van het delen van de data. Er moet een bepaalde kritische massa aan biometrische informatie zijn waardoor de mogelijkheid gaat ontstaan op matches. Een kleine referentiedatabase zal minder snel leiden tot resultaat. Als verschillende deelnemende landen in een missiegebied overeen kunnen komen dat ze hun biometrische informatie met elkaar delen, of centraal beheren op een hoofdkwartier, zal niet alleen de kans op een match of hit toenemen, maar draagt dit meteen bij aan een *Common Operational Picture* van wie zich ophouden in het missiegebied. Zo wordt de tegenstander de kans ontnomen om, door veelvuldig te reizen tussen AOR's, uit beeld te blijven.

Figuur 8 figuur geeft een mogelijke architectuur weer om biometrische informatie uit te wisselen. Dit is tevens de basis waarop NAVO-landen de uitwisseling testen. In de linker- en rechterkolommen staan de modaliteiten waarvan landen de keuze kunnen maken ze te delen. Allereerst zal de informatie in de eigen ABIS worden opgeslagen. De keuze kan zijn bepaalde informatie rechtstreeks te delen met andere landen, maar andere informatie alleen onder bepaalde voorwaarden of na nadere analyse. Een willekeurig voorbeeld wordt weergegeven in schema 1.



Figuur 8 Schematische weergave van het delen van biometrische gegevens

In dit voorbeeld deelt land A met elk land in het missiegebied de latente vingersporen en biometrische informatie verkregen uit OSINT. Gezichtsvergelijking wordt alleen automatisch met land B gedeeld.

Vanzelfsprekend dient de informatie met de juiste veiligheidseisen te zijn omgeven, met name omdat het hier veelal – zo niet uitsluitend – gaat om geautomatiseerde verwerking van tot een persoon herleidbare gegevens. Daarnaast zijn er mogelijkheden om de gegevens te encrypten.

Modaliteit / Land	B	C	D	Z
Latente vingersporen	X	X	X	X
Gezichtsvergelijking	X	-	-	-
Irisscan	X	X	-	X
DNA	-	-	X	-
OSINT	X	X	X	X

Schema 1 Uitwisselingsregels voor land A

Analyse
In de analysestap wordt nader bekeken welke waardevolle *links* het systeem heeft gelegd voor de informatiepositie van de commandant. Na de analysestap van een of meerdere subjecten moeten vragen kunnen worden beantwoord als: wie is het, gebruikt hij een alias, waar is hij de afgelopen tijd geweest, wat weten we over (vroegere) activiteiten en welk dreigingsniveau zit aan betrokkene vast. De analyse kan duidelijk maken tot welk(e) netwerk(en) een persoon behoort, en of netwerken aan elkaar kunnen worden gekoppeld. Deze uitkomsten voeden vervolgens de *intelligenceketen,* waar ze worden samengevoegd met andere intel. Daardoor kan een alomvattend beeld ontstaan van de omgeving waarin de operatie wordt uitgevoerd, inclusief de mensen en netwerken die hierbinnen actief zijn.

Besluit/actie
Gebaseerd op bovenstaande analyse kunnen besluiten worden genomen om bijvoorbeeld de status of het dreigingsniveau van betrokkenen aan te passen. Ook kunnen op basis hiervan nieuwe acties worden uitgezet om biometrie te verzamelen.

Evaluatie
De laatste stap, de evaluatie, maakt de cirkel compleet. In deze fase wordt met name het proces geëvalueerd: hebben de inspanningen tot het verwachte resultaat geleid of moet de manier waarop we biometrische gegevens verzamelen worden aangepast? Dit moet ook worden gerelateerd aan de fase waarin een operatie zich bevindt: in de beginfase kan het nodig zijn assertief te verzamelen, in latere fases meer op basis van consensus, of uitvoering door de *host nation*.

Conclusie

In dit artikel is uiteengezet welke voordelen en kansen het gebruik van biometrie biedt. Daarnaast is beschreven wat het concept van het gebruik van biometrie in missiegebieden is, zoals beschreven in de NAVO doctrinepublicatie AINTP-15. Biometrie kan zeer veel en grote voordelen bieden, maar het is belangrijk goed na te denken over de inzet ervan.

Biometrie kan ook risico's met zich meebrengen voor het eigen personeel. Defensiemedewerkers moeten zich bewust zijn van biometrische sporen die zij kunnen achterlaten voor een tegenstander en zij dienen zich te realiseren dat een tegenstander actief bezig kan zijn biometrische gegevens te verzamelen. Daarnaast zal de tegenstander nadenken hoe hij het systeem kan misleiden, zodat er geen of verkeerde informatie in systemen belandt. Dit zijn onderwerpen die nadere aandacht verdienen.

Ten slotte is er nog een juridische horde te nemen om verbindingen te kunnen leggen tussen binnenlandse en buitenlandse incidenten en personen. Maar deze zaken zouden niet in de weg moeten staan van een verdere implementatie van biometrie in de krijgsmacht. ■