'Beveiligingsbranche kan te voor forensische biometrie'

Biometrie voor toegangbeheer is niets nieuws. Ook van politieagenten die DNA-sporen verzamelen op een Plaats Delict kijken we niet meer op. Maar forensische biometrie? Didier Meuwly van het Nederlands Forensisch Instituut houdt zich sinds kort ook als bijzonder hoogleraar aan de Universiteit Twente bezig met onderzoek naar deze tak van sport. "Het is een nichemarkt met ingewikkelde issues."

Een inbraak in een bedrijfspand? Dikke kans dat de politie DNA-sporen komt verzamelen en op zoek gaat naar vingerafdrukken. En er is meer mogelijk om daders op te sporen. Een foto van het gezicht, een audio-opname van de stem, een video van de manier van lopen. Het zijn allemaal sporen waarmee de forensische biometrie uit de voeten kan om personen te identificeren. Daarom kan deze vorm van forensisch onderzoek een belangrijke rol spelen in opsporing en vervolging van verdachten, en in het werk van inlichtingen- en opsporingsdiensten.

"Forensische biometrie kent meerdere modaliteiten: de stem, het gezicht en lichaam, de tanden, de tred, het handschrift en natuurlijk vingerafdrukken. Het gaat om een breed spectrum van onderscheidende kenmerken die te maken hebben met het lichaam van een individu", vertelt Didier Meuwly, principal scientist bij het Nederlands Forensisch Instituut (NFI) en bijzonder hoogleraar aan de Universiteit Twente. "De vraag is natuurlijk wat je met dit type sporen kunt doen. Vingerafdrukken worden doorgaans gebruikt voor identiteitsverificatie en vingersporen spelen een grote rol in de opsporingspraktijk. De andere modaliteiten bieden potentieel voor bewijsvoering, opsporing of intelligence. Maar niet alle technologieën om de verschillende typen sporen te verzamelen, bevinden zich in hetzelfde ontwikkelingsstadium."

Bewijsvoering Voor bewijsvoering in rechtszaken is het gebruik van vingersporen volledig geaccepteerd. "Daarentegen worden de audio-opnamen van stemmen en de beelden van camera's met gezichtsherkenning in de rechtszaal niet altijd als bewijsmateriaal toegestaan", vertelt Meuwly. "De technologie op dit terrein is de laatste jaren wel verbeterd, maar levert nog beperkt bruikbare informatie. Bijvoorbeeld: als een stemopname tijdens een autorit is gemaakt met een mobieltje, zijn de sporen van zeer beperkte kwaliteit. En de resolutie van CCTV-beelden is vaak zodanig dat van gezichtsherkenning geen sprake kan zijn."

Als het gaat om opsporing, heeft forensische biometrie ook nog eens te maken met de beperkte beschikbaarheid van databanken met bijvoorbeeld stemopnamen en de vormen van tanden van verdachten. Bovendien behoren het postuur en de manier van lopen tot de zogenoemde soft biometrics. Deze lichaamskenmerken zijn minder onderscheidend dan bijvoorbeeld vingerafdrukken en handschriften. De analyse van de lichaamsomvang en tred van een inbreker biedt dan ook eerder mogelijkheden om verdachten uit te sluiten dan om ze op te sporen. Meuwly benadrukt dat het ook internationaal niet altijd van een leien dakje loopt. "Op internationaal niveau is er nog geen standaard voor de registratie van biometrische gegevens, behalve voor vingersporen en DNA. En er zijn nog geen geformaliseerde processen voor gegevensuitwisseling. Daardoor zijn de verschillende databases lokaal en lastig doorzoekbaar. En zelfs als dat wel zo zou zijn: om databanken die een factor tien of vijftig groter zijn dan de nationale te kunnen doorzoeken, is betere technologie nodig."

Doelen De Universiteit Twente is de enige academische instelling in Nederland die structureel onderzoek doet naar forensische biometrie. Een van de doelen van Meuwly's recente aanstelling als bijzonder hoogleraar is om de automatische interpretatiemethoden voor biometrische sporen te verbeteren. Op dit moment interpreteren deskundigen deze sporen veelal op basis van hun kennis en ervaring. Automatische methoden maken gebruik van algoritmen en van grotere hoeveelheden gegevens. Dit vergroot de objectiviteit van het onderzoek. Net als hij al doet bij het NFI, zal Meuwly aan de Universiteit Twente intensief samenwerken met forensische ketenpartners (zoals de politie en het Openbaar Ministerie), academische kennisinstellingen en hightech-bedrijven.

"Beveiligingsbedrijven kunnen binnen de forensische biometrie een rol spelen op het terrein van de capture (verzameling) van sporen", zegt Meuwly over de mogelijke samenwerking met de particuliere beveiligingsbranche. "Er zijn nu camerabewakingssystemen die goed genoeg zijn om verdachte activiteiten in beeld te brengen, maar de kwaliteit is vaak onvoldoende om gezichten te identificeren. De beveiligingsmarkt kan daarin een verbeteringsslag maken. Bijvoorbeeld door een camera die een grote hoek vangt standaard te combineren met een camera die inzoomt op een gezicht."

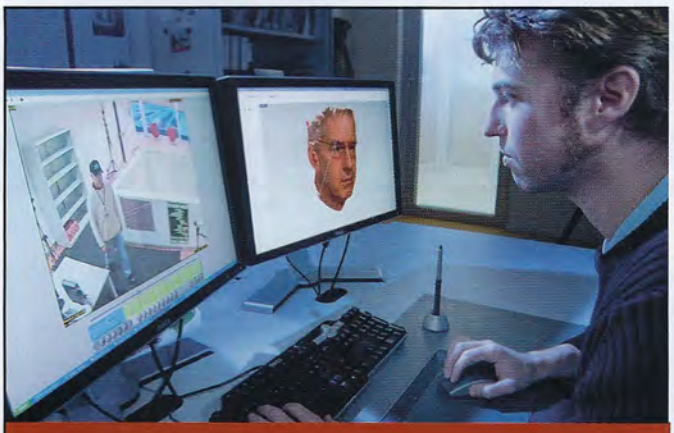
Ook is er binnen het forensisch biometrisch onderzoek behoefte aan technologie die verschillende modaliteiten kan linken. "Een CCTV-camera kan de lengte van een persoon schatten en het gezicht in beeld brengen. De bewijskracht van deze informatie kan sterk omhoog gaan als deze gegevens gecombineerd kunnen worden."

chnologie ontwikkelen

Hobbels Meuwly erkent dat er voor de beveiligingssector wel wat hobbels te nemen zijn. "Voor de forensische biometrie is de opname van informatie die misschien een spoor kan vormen in een delict essentieel. Maar als er in de markt geen trigger of incentive (prikkel) is, of een eis van verzekeraars, om een hightech-systeem te installeren, zal het er - vanwege de kosten voor de klant - niet zo snel komen."

Er liggen wel andere kansen voor de beveiligingssector, denkt Meuwly. "De tools die de forensische biometrie gebruikt zijn vaak spin-offs van techniek die is gemaakt voor toegangscontrole. De beveiligingsbranche kan dus algoritmen die oorspronkelijk voor access control zijn ontwikkeld later binnen het veld van forensische biometrie aanbieden. Bijvoorbeeld: voor 3D-gezichtsvergelijking heeft de Universiteit Twente tegenwoordig de beste algoritmen in huis. Er is zeker ruimte voor bedrijven om dit soort technologie ook te bieden."

Tegelijkertijd krijgt de markt wel te maken met de nodige uitdagingen. "Ik denk niet dat er een grote rol ligt voor de private beveiligingsbranche als het gaat om de uitvoering van forensische biometrie. Het is een nichemarkt met ingewikkelde issues. Een van de uitdagingen is dat je doorgaans werkt met informatie van slechte kwaliteit, die je vervolgens moet gebruiken in uiteenlopende processen, waarvoor je verschillende databanken nodig hebt. En dan krijg je ook nog eens te maken met de spelregels voor bewijsvoering van rechtbanken. Als je je als beveiligingsbedrijf in de markt van forensisch onderzoek wilt begeven, is dat dus heel moeilijk. De marktkansen liggen naar mijn idee eerder in de ontwikkeling van kerntechnologie, zoals algoritmen, en van softwareproducten en -oplossingen." Het beperkte aantal bedrijven dat zich - ook internationaal - bezighoudt met forensische biometrie is dan ook veelzeggend. "Wereldwijd is de markt in handen van overheidsinstanties. Er is wel een Spaans bedrijf dat oplossingen levert voor stemherkenningsystemen in ▸



PERSONALIA

Didier Meuwly

Didier Meuwly (46) werkt sinds 2004 bij het Nederlands Forensisch Instituut. Recent werd Meuwly benoemd tot bijzonder hoogleraar forensische biometrie aan de Universiteit van Twente. In deze positie richt hij zich op vingerafdrukherkenning en de toepassing van biometrie in forensische zaken. Meuwly volgde de forensische opleiding van de Universiteit van Lausanne. In 2000 promoveerde hij daar op een onderzoek naar automatische sprekerherkenning. Na enkele jaren te hebben gedoceerd aan de Universiteit van Lausanne, werkte Meuwly als onderzoeker bij de Engelse Forensic Science Service. Inmiddels behoort hij tot een van de vier principal scientists bij het Nederlands Forensisch Instituut, en tot een van de zes bijzonder hoogleraren die vanuit het instituut parttime zijn verbonden aan Nederlandse universiteiten.

bewijsvoering, opsporing en intelligence. Verder zijn er vooral erg kleine forensische instellingen actief, die zich meer met de uitvoering dan met research & development bezighouden."

Indirecte toegang Meuwly vertelt over de visie van de Europese Unie over data privacy en open data, die technisch wordt uitgewerkt in bijvoorbeeld het project Biometrics Evaluation and Testing. "Het idee is dat bedrijven de mogelijkheid krijgen om in databases van de overheid te werken zonder over de data te kunnen beschikken. Biometrische en forensische data zijn natuurlijk gevoelig om vrij te geven. Er wordt daarom technologie ontwikkeld om indirecte toegang te bieden aan private beveiligingsbedrijven en universiteiten om de door hen ontwikkelde algoritmen te toetsen met behulp van echte data in plaats van data die zijn gesimuleerd in een laboratorium. Dan kan het gebruik van de technologie beter worden geëvalueerd."
Meuwly denkt al na over een vervolg op het Biometrics Evaluation and Testing project en ziet daarin ook een rol voor de Nederlandse beveiligingssector. "Tot nu toe is het niet mogelijk gebleken om een interactief platform met forensische data en scenario's te creëren voor bedrijven en universiteiten die biometrische technologieën en oplossingen kunnen bieden. Deze ontwikkeling biedt kansen voor de particuliere beveiliging om zich te profileren. Want in Nederland zijn het op dit moment vooral universiteiten die zich ermee bezighouden."

■ dr. Lynsey Dubbeld

Column

Bedrijfsbelangen

'Langer doorgaan met uithollen van uw beveiliging kan u duur komen te staan!'

Stel, u heeft de afgelopen jaren sterk ingeteerd op uw beveiligingsbudget. Doordat er gelukkig niets is gebeurd in deze periode heeft u flink geld bespaard. Geld dat nodig was om de moeilijke economische tijd te overbruggen. Dan heeft u het goed gedaan volgens sommigen! Maar wat indien het fout was gegaan? Had dat de ondergang van uw bedrijf betekent of niet?

Wie nuchter kijkt naar de huidige wereld kan niet anders dan constateren dat er momenteel veel conflicten gaande zijn die hun weerslag op Europa en Nederland kunnen hebben. Worden Israëlische objecten een verhoogd risico, vormen de terugkerende Syriëgangers een probleem, worden Amerikaanse bedrijven wellicht een doelwit voor IS aanhangers, wordt de samenstelling van een buurt een probleem omdat de bewoners elkaar niet langer verdragen, wat zijn de gevolgen van de Russische tegenmaatregelen naar aanleiding van sancties door de VS en de EU, of wordt u het slachtoffer van cybercrime? Wie het weet mag het zeggen.

Jarenlang is er bezuinigd op uitgaven voor de security, maar wat als deze in één keer door genoemde ontwikkelingen weer een boost krijgt? Dan is de vraag naar vakbekwaam personeel groot en de spoeling dun, omdat men binnen deze bedrijven de opleidingen sterk heeft teruggedraaid. Zet uw bedrijfsbelangen eens af tegen de risico's die u neemt met betrekking tot deze belangen. Wellicht is het dan wijs om net als de Nederlandse overheid, die jarenlang heeft bezuinigd op Defensie en nu tot een ommekeer komt, na te denken wanneer u ook weer eens 'om' gaat. Kijk kritisch naar een evenwichtige afweging van risico's en kies voor een mix van technopreventieve maatregelen en manbewaking indien zulks nodig is. Langer doorgaan met uithollen van uw beveiliging kan u duur komen te staan!

Gerard Bongers RSE Security Consultant

Opinie@beveiliging.nl