2

Inlichtingenvergaring

1 mei 2011. Barack Obama bevindt zich in de overvolle Situation Room van het Witte Huis. Naast de Amerikaanse president zitten vicepresident Joe Biden, minister van Buitenlandse Zaken Hillary Clinton en de andere leden van de Nationale Veiligheidsraad. Vanuit de kelder van de westvleugel kijken ze live mee met Operatie Neptune Spear, de missie waarbij Osama bin Laden gepakt wordt.

Naderhand kwamen er veel details over de operatie naar buiten. We zagen satellietbeelden van Bin Ladens verblijfplaats in Abottabat, en we hoorden dat hij was gevonden via een van zijn koeriers, nadat een telefoontje door de CIA was onderschept. Deze set inlichtingen, uiteraard gecombineerd met het optreden van de Amerikaanse Navy SEALS, zorgde ervoor dat Bin Laden eindelijk gepakt kon worden.

Bovenstaand voorbeeld maakt duidelijk dat informatie uit diverse bronnen als inlichtingen gebruikt kan worden. Diensten zullen indien mogelijk altijd proberen om een analyse op te stellen of actie te ondernemen op basis van meerdere inlichtingen, die idealiter afkomstig zijn uit verschillende soorten bronnen. Oftewel: vaak maken diensten in hun werk gebruik van

verschillende methoden naast elkaar om de puzzel compleet te maken.

In dit hoofdstuk zal ik ingaan op de belangrijkste disciplines van 'inlichtingenvergaring', zoals dat in het vak heet. Op de andere stappen van het inlichtingenproces – de keuze voor de te onderzoeken onderwerpen, de verwerking van de gevonden informatie en de analyse op basis waarvan actie ondernomen kan worden – kom ik later terug. Eerst zal ik de vraag beantwoorden waar je waarschijnlijk het benieuwdst naar bent: hoe komen de diensten aan hun informatie?

De Dikke Van Dale omschrijft een inlichting als een 'mededeling waardoor iemand op de hoogte van iets komt'. Diensten willen zichzelf dus op de hoogte stellen van mogelijke dreigingen voor de democratie en de samenleving.

Wanneer ik een wetenschappelijk artikel schrijf, gebruik ik vaak de volgende definitie van inlichtingen: het gestructureerd verzamelen van specifieke informatie om de uitvoerende macht (diverse overheidsinstanties) te ondersteunen bij de uitvoering van hun taken om de nationale veiligheid en democratische rechtsstaat te beschermen. Doorgaans gaat het hierbij om kennis over de mate waarin tegenstanders (zoals andere staten, extremisten of terroristen) van plan zijn en/of in staat zijn om acties te ontplooien die de democratie en staat schade toebrengen. Niet elk stukje informatie is dus een inlichting. Om van inlichtingen te kunnen spreken moet de informatie worden verzameld en geduid in het licht van de specifieke onderzoeksvraag van de diensten.[1]

In dit hoofdstuk onderscheid ik vijf verschillende typen inlichtingen: inlichtingen uit menselijke bronnen (humint), inlichtingen uit open bronnen (osint), inlichtingen uit foto's en

geografische informatie (geoint), inlichtingen uit signaalonderschepping (sigint) en inlichtingen uit sociale media (socmint). Per type inlichting sta ik ook stil bij de algemene en bijzondere bevoegdheden die de diensten hebben om deze inlichtingen te kunnen vergaren. Zoals je direct ziet aan de namen van de typen inlichtingen, is het een misverstand dat inlichtingen alleen op geheime informatie betrekking zouden hebben. Een groot deel van de informatie waar de diensten zich op baseren is voor iedereen beschikbaar. De toegevoegde waarde van de diensten zit er dan in dat ze weten waar ze naar zoeken, waar ze de informatie kunnen vinden en wat ze ermee doen.

Humint

Eind december 2020 verspreidde de AIVD beelden van twee mannen die buiten op een bankje naast elkaar zitten en een envelop en een usb-stick met elkaar uitwisselen. Op de beelden zag je een medewerker van een Nederlands hightechbedrijf en een Russische inlichtingenofficier. De dienst bracht naar buiten dat twee Russische inlichtingenofficieren het land hadden moeten verlaten omdat ze betrapt waren op spionage. Ze waren bezig om een netwerk op te bouwen in de hoogwaardige technologische industrie van Nederland, om op deze wijze gevoelige informatie te verwerven over kunstmatige intelligentie, halfgeleiders en nanotechnologie. Daartoe benaderden ze mensen die bij dit soort bedrijven werkten of onderzoek deden aan universiteiten. De Russen zetten hen ertoe aan om gevoelige informatie met Rusland te delen.[2]

Het verkrijgen van inlichtingen via menselijke bronnen is de manier van informatievergaring waaraan de meeste mensen als eerste denken bij de geheime diensten. Denk bijvoorbeeld aan een minister die naakt in een bordeel wordt aangetroffen en la-

ter onder druk wordt gezet om gevoelige informatie te delen omdat er foto's van de nacht in kwestie bestaan. In vaktermen wordt het vergaren van inlichtingen uit menselijke bronnen *human intelligence* (humint) genoemd.

Er zijn verschillende soorten menselijke bronnen; dit heeft onder andere te maken met hun verhouding tot de dienst en de mate waarin de diensten deze personen kunnen aansturen. Sommige mensen wordt alleen gevraagd naar hun waarnemingen – denk aan diplomaten of migranten die kennis hebben van een specifiek land. Deze personen worden informanten genoemd. Er zijn ook personen die actief door de diensten worden aangestuurd om informatie te verzamelen. Dat kan bijvoorbeeld door te infiltreren in een staat, een bedrijf, een organisatie of een terroristische cel waarin de dienst interesse heeft. Zij worden agenten genoemd. Informanten en agenten worden vanuit de dienst begeleid door zogenoemde acquisiteurs (vroeger ook wel operateurs genoemd, in het Engels ook wel *case officers*).

Checklist van de BVD

Wanneer een spion een profiel van iemand maakt en/of iemand in de gaten dient te houden, zijn er veel zaken om op te letten. Zo gaf de BVD in 1953 aan medewerkers deze lijst met punten om op te letten mee:

1 Algemene indruk (mannelijk type, atletisch, gevoelig, sensueel, zachtaardig, diplomatiek, artistiek enz.)
2 Kleding (verzorgd, overdreven netjes, bizar, stijlvol enz.)
3 Fysiek (vorm hoofd, kleur ogen, geschatte lengte, gewicht, omvang enz.)

4 Handen (beschrijving handen, verzorgd, hoe houdt hij ze, tikt hij ermee op tafel, in z'n zakken?, karakteristieke bewegingen)
5 Taal (hoe spreekt hij zijn taal, beschaafd, slordig; hoe spreekt hij Nederlands; hoe is zijn stem)
6 Bewegingen (maakt hij karakteristieke bewegingen, door het haar strijken, hoofd in z'n handen e.d.)
7 Wat voor indruk zal hij maken op de meeste mannen/vrouwen
8 Wat is zijn achtergrond (bevolkingsgroep, ras, cultureel, ontwikkeling, opleiding)
9 Welke indruk vestigt hij m.b.t. zijn achtergrond (ontwikkeld, intelligent, begrijpend, temperamentvol, dom enz.)
10 Sociaal gedrag (vriendelijk, punctueel, informeel of formeel, onvoorspelbaar in de omgang e.d.)
11 Rook- en eetgewoonten (sigaretten, sigaren, pijp, filters, zelf sigaretten rollen, merken, wijze van eten, soort voedsel dat zijn voorkeur heeft, kenner van goed eten)
12 Drinkgewoonten (soort drank, hoeveelheden, wijze van consumeren: nippen of in één teug achterover, verandert zijn optreden onder invloed van drank)
13 Rij- en loopgedrag (rijdt hij goed, snel, langzaam, zenuwachtig, geagiteerd, verkeersfouten; loopt hij snel, slenterend, alert, rechtop)

Maar waarom zou je eigenlijk een bron willen zijn? Er kunnen immers best wel wat gevaren kleven aan het delen of actief verzamelen van informatie. Bronnen hebben altijd een motief, al is niet voor elke bron even gemakkelijk door diensten te bepalen wat dat precies is. Dit motief kan gevolgen hebben voor de betrouwbaarheid van een bron.

De motieven van bronnen laten zich samenvatten in het acroniem MICE: *Money* (geld), *Ideology* (ideologie), *Coercion* (afpersing of dwang) en *Ego* (ego). Veel bronnen zijn financieel gemotiveerd om informatie te delen, soms simpelweg om er rijker van te worden, maar mogelijk ook uit pure noodzaak, bijvoorbeeld om medische rekeningen of het schoolgeld van de kinderen te kunnen betalen. Anderen zijn ideologisch gemotiveerd (denk aan religieuze of politieke overtuigingen) en willen vanuit die overtuiging samenwerken met diensten of regimes (zie hieronder het voorbeeld van het communisme en de Cambridge Five). En ook het ego van een bron kan een rol spelen: iemand kan erop kicken om belangrijk te worden gevonden en informatie te kunnen delen.

Rusland en China staan erom bekend dat ze chantage, afpersing en seksuele uitlokking gebruiken om informatie te verzamelen. Niet voor niets zie je in veel films de zogenoemde *honeytraps*: mooie vrouwen die mannen verleiden, zodat ze in de hotelkamer helemaal 'leeglopen' en alle geheimen prijsgeven. Of er worden foto's gemaakt van hun seksuele escapades waarmee ze later onder druk kunnen worden gezet. Veel andere landen doen dit juist niet – uit ethische overwegingen, maar ook omdat bronnen die vrijwillig meewerken over het algemeen betrouwbaarder zijn.

Cambridge Five

Een klassiek voorbeeld van spionage uit de Koude Oorlog is dat van de Cambridge Five. In de jaren dertig vormden Britse universiteiten een vruchtbare voedingsbodem voor kritiek op de Britse maatschappij. Een deel van de studenten voelde zich aangetrokken tot het communisme en het antifascisme.

De Sovjet-Unie zag dat ook en startte met de werving van spionnen op bepaalde universiteiten, waaronder de universiteit van Cambridge.

De Cambridge Five waren vijf studenten die geloofden dat het marxisme het beste politieke systeem was en de beste manier vormde om het fascisme buiten de deur te houden. Dat maakte hen tot gewillige bronnen voor de Sovjet-Unie. Waarschijnlijk zijn zij al tijdens hun studie gerekruteerd door de Sovjet-Unie, maar pas later konden zij relevante informatie leveren. Dit laat ook goed zien dat een humint-relatie een langetermijninvestering kan zijn. Na hun studie kwamen de mannen terecht op invloedrijke posities in het Verenigd Koninkrijk, in het bijzonder bij MI5 (de binnenlandse geheime dienst), MI6 (de buitenlandse geheime dienst) en het ministerie van Buitenlandse Zaken.

Jarenlang hebben deze mannen schade toegebracht aan de Britse veiligheidsbelangen. Zo brachten ze de Sovjet-Unie op de hoogte van het feit dat de Verenigde Staten en het Verenigd Koninkrijk bezig waren een atoombom te maken. Ze ontmoetten een contactpersoon in het park en verstrekten uitgebreide informatie over de werkwijze, de doelen en de medewerkers, zoals onderstaande omschrijving van een collega:

> MR NICHOLAS ELLIOT. *24, 5 ft 9 in. Brown hair, prominent lips, black glasses, ugly and rather pig-like to look at. Good brain, good sense of humor. Likes a drink but was recently very ill and now, as a consequence, drinks little. He is in charge of Holland.*[3]

Deze omschrijving lijkt misschien wat cartoonesk, maar was wel doeltreffend. In de tijd dat mensen nog niet makkelijk online te vinden waren, was een uitgebreide omschrijving van het uiterlijk op zijn plaats. Maar het gaat natuurlijk vooral om de mogelijke kwetsbaarheden. Als je over een persoon weet dat hij of zij graag drinkt of een echte flirt is, kun je daarop inspelen wanneer je diegene wilt benaderen of onder druk wilt zetten.

Een opvallend detail in dit verhaal is dat geen van deze vijf spionnen voor spionage is vervolgd. Drie van hen vluchtten naar de Sovjet-Unie, eentje vertrok naar Zuid-Europa en de laatste kon, na het afleggen van een verklaring in ruil voor immuniteit, in het Verenigd Koninkrijk blijven, waar hij in 1983 overleed.

Een van de grote voordelen van menselijke bronnen is dat zij vaak de enige zijn die de ware bedoelingen van groepen en individuen kunnen duiden. Zeker als het gaat om terroristische organisaties of andere groepen die in cellen opereren en snel van samenstelling of werkwijze veranderen, kunnen menselijke bronnen het verschil maken. Over het algemeen geldt dat hoe kleiner de groep is of hoe hoger het veiligheidsbewustzijn (de mate waarin iemand zich bewust is van de risico's die horen bij bepaalde gedragingen en de wijze waarop de persoon hierop reageert) van de groep of persoon is, hoe belangrijker humint kan zijn.

Tegelijkertijd is het heel lastig om in sommige groepen te infiltreren. Als de groep erg klein is en de groepsleden elkaar al lange tijd kennen, valt het erg op als je daartussen probeert te komen. Het is dan vaak een betere optie om te proberen contact

te leggen met een van de leden van een groep en deze te 'draaien', oftewel over te halen om voor jou te werken. Maar ook hier zijn risico's aan verbonden: je weet nooit helemaal zeker waar uiteindelijk de loyaliteit van deze persoon ligt. Het kan immers ook een dubbelspion blijken.

Een voorbeeld van iemand die 'gedraaid' leek maar uiteindelijk een dubbelspion bleek te zijn, was de dokter Humam Khalil Abu-Mulala al-Balawi. Overdag was al-Balawi een arts in een Palestijns vluchtelingenkamp in Jordanië; 's nachts was hij een jihadistische blogger met het alias Abu Dujuna. Met hulp van de Amerikanen kwam de Jordaanse dienst achter zijn identiteit. Hij werd opgepakt, verhoord en vervolgens vrijgelaten. Later werd hij gerekruteerd door de Jordaanse dienst, omdat hij mogelijk zou kunnen helpen bij de jacht op de tweede man van Al Qaida, al-Zawahiri. De Jordaanse dienst werkte in dit geval samen met de CIA, en al snel werd voor al-Balawi een reis georganiseerd naar Pakistan. En inderdaad: de arts leek snel het vertrouwen van Al Qaida te winnen; hij zou zelfs de arts van al-Zawahiri zijn geworden. Daarop werd door de diensten besloten dat ze al-Balawi snel moesten ontmoeten om hem te equiperen om inderdaad informatie te kunnen doorgeven. Hij zou vanuit Pakistan naar de Amerikaanse basis in Khost, Afghanistan, komen.

Op 30 december 2009 bezocht hij inderdaad deze militaire basis. In plaats van getraind te worden, blies hij zichzelf echter op; hij doodde met deze aanslag zeven medewerkers van de CIA en een Jordaanse militair, een neef van de Jordaanse koning Abdullah II. Achteraf bleek dat vanaf het moment dat de arts in Pakistan was aangekomen, hij in contact was gekomen met de leiding van Al Qaida en met hen ging samenwerken. Daarom leek hij voor de Amerikanen en Jordaniërs een goede bron die

snel relevante informatie kon leveren.[4] Later vertelde zijn vrouw in een interview dat zijn loyaliteit nooit bij de Jordaniërs of de Amerikanen had gelegen. Zelf deelde hij in een afscheidsfilmpje dat na de aanslag naar buiten kwam mede dat hij deze aanslag pleegde als vergelding voor een aanslag op een Pakistaanse Talibanleider.

Er zitten zowel voor- als nadelen aan het gebruik van menselijke bronnen. Een van de voordelen is dat menselijke bronnen cruciale inlichtingen opleveren die niet via andere wegen te verkrijgen zijn. Dit maakt humint in sommige gevallen de meest waardevolle bron voor inlichtingenvergaring. Daarnaast is humint relatief goedkoop: je hoeft er immers geen dure apparatuur voor aan te schaffen, zoals je die bijvoorbeeld wel nodig hebt voor signaalonderschepping. Bovendien is het vaak mogelijk om menselijke bronnen gedurende het onderzoek bij te sturen, zodat je preciezer kunt zoeken naar de informatie die je nog mist.

Een van de nadelen van deze manier van vergaring is dat je voor het vergaren van humint vaak in de directe nabijheid van de bron moet verkeren. Dit kan tot gevaarlijke situaties leiden voor zowel bronnen als medewerkers van diensten (zoals hierboven in het voorbeeld over de aanslag in Camp Khost). Hierbij kun je denken aan langdurig verblijf in oorlogsgebied, maar ook bijvoorbeeld infiltratie in een terroristische organisatie is niet zonder risico's. En hoe kleiner de groep is waarvan een spion deel uit probeert te maken, hoe groter het risico is dat die wordt ontdekt.

Daarnaast moet er bij humint veel gebeuren voordat je informatie krijgt van een bron – stappen die veel tijd in beslag kunnen nemen. Allereerst moet je weten wie jou van de juiste informatie kan voorzien, nu of in de toekomst. Daarna moet

je met deze persoon in contact komen en een band opbouwen. Je gaat mensen vragen iets te doen wat ze waarschijnlijk nooit voor mogelijk hadden gehouden. Je moet deze persoon dus weten te overtuigen en mogelijk een beloning overeenkomen. Pas daarna krijg je van diegene mogelijk relevante informatie. Deze verschillende stappen kunnen bij elkaar opgeteld soms wel jaren duren. Dit is ook een van de redenen waarom diensten altijd goed vooraf moeten bedenken op welke plekken en waarover ze in de toekomst mogelijk informatie willen verzamelen. Als je op het moment dat Rusland Oekraïne binnenvalt nog moet beginnen een netwerk op te bouwen, ben je te laat.

De 'Braziliaanse' stagiair

Een goed voorbeeld van een langetermijninvestering is de casus van de 'Braziliaanse' stagiair bij het Internationale Strafhof in Den Haag. Op 16 juni 2022 brengt de AIVD het bericht naar buiten dat in april 2022 is voorkomen dat een Russische spion Nederland binnenkwam en als stagiair voor het Internationale Strafhof in Den Haag gaat werken. Het Hof heeft op dat moment meerdere onderzoeken naar Rusland lopen. Victor Muller Ferreira blijkt de dekmantel te zijn van de Rus Sergej Vladimirovitsj Tsjerkasov. Al jaren was Sergej bezig een fictief leven op te bouwen, zodat hij op een gegeven moment door Rusland zou kunnen worden ingezet om inlichtingen te verzamelen. Dit soort personen wordt ook wel *illegals* (illegalen) genoemd. Illegals zijn personen die jarenlang onder de radar opereren om bij wijze van dekmantel een heel eigen leven te fingeren, onder een andere naam, met een volledig ander bestaan.

Toen de AIVD het bericht over de gepakte inlichtingenme-

dewerker naar buiten bracht, liet die ook de zogenoemde 'legende' van deze persoon zien. In een document van vier pagina's, waarin sommige namen en details waren zwartgemaakt, werd de levensweg van 'Victor' uit de doeken gedaan. Zijn opa aan moederskant zou zijn overleden aan een hartaanval en zijn oma aan kanker; hij zou speciale jeugdherinneringen hebben aan bepaalde plekken in Brazilië; hij beschrijft gedetailleerd hoe het huis waarin hij opgroeide eruitzag en hoe zijn basisschool vanbuiten oogde enzovoort. Al deze details waren van belang, omdat ze hem een cover gaven: hij kon op deze manier veinzen dat hij al een heel leven deze persoon was.

Het doorvoeren van dit leven gaat heel ver. Victor had een uitgebreide online aanwezigheid: hij was te vinden op Facebook en op een Amerikaanse banenwebsite, hij had een actief Twitter-account en hij was in 2017 een blog gestart over geopolitiek. Hoewel hij op Facebook niet zo actief was, had hij daar wel veel vrienden uit Brazilië (waar hij zou zijn opgegroeid) en ook uit Dublin en de Verenigde Staten (waar hij zou hebben gestudeerd).

Deze variant van humint vraagt heel veel van de spionnen. Vanaf het moment dat je undercover opereert, is er geen weg terug. Je kunt niet in het weekend op bezoek bij je oma, je kunt geen contact hebben met vrienden van vroeger en je bouwt een heel nieuw leven op waarin je nooit de waarheid kunt spreken over je echte identiteit.

Sergej werd teruggestuurd naar Brazilië, waar hij werd veroordeeld voor fraude in geschrifte. In november 2022 bleek Rusland een verzoek tot uitlevering te hebben ingediend. Zij zeiden dat Sergej geen spion was, maar werd gezocht voor

handel in heroïne. Deze truc (spionnen terughalen omdat ze in eigen land vervolgd zouden moeten worden voor een crimineel delict) wordt wel vaker geprobeerd – voor zover ik weet meestal met weinig succes. Tot op heden is Brazilië niet op het verzoek ingegaan.[5]

Humint gaat overigens niet alleen over undercoveroperaties en in het geheim informatie verzamelen. De diensten gaan daarnaast openlijk met mensen in gesprek, op zoek naar informatie. Zo proberen ze in contact te komen met mensen die om radicale individuen heen staan. Het is bijvoorbeeld voorstelbaar dat ouders zich zorgen maken en graag met een dienst spreken als dat hun kind in hun ogen uiteindelijk kan helpen.

Wanneer de diensten openlijk in gesprek gaan, is het doel niet altijd om inlichtingen te vergaren. Een gesprek kan ook een afschrikkende werking hebben. Een recent voorbeeld hiervan heeft betrekking op voormalig CDA-senator René van der Linden. Uit artikelen in *de Volkskrant* en NRC blijkt dat Van der Linden jarenlang zeer intensieve contacten met Rusland onderhield.[6] Nadat hij in juli 2019 op kosten van de Russen een conferentie in Moskou heeft bezocht, voert de AIVD een gesprek met hem. Van der Linden vertelt zelf dat zijn contact na dit 'waarschuwende' gesprek is afgebroken.[7] Door de dienst 'gezien' of gewaarschuwd worden kan ertoe leiden dat bronnen hun acties opnieuw overwegen of dat tegenstanders het contact met de niet langer geheime bron verbreken.

Wat vaak onvermeld blijft, maar wat wel een belangrijke stap is wanneer er met menselijke bronnen wordt gewerkt, is het 'afbouwen' van een bron. De meeste bronnen zullen niet hun hele leven interessante informatie voor diensten kunnen blijven leve-

ren. Dat kan zijn doordat de bron, bijvoorbeeld door een carrièreswitch, geen toegang meer heeft tot de gewenste informatie, of doordat de informatie die de bron kan geven niet meer relevant is voor de dienst, zoals na de afronding van een militaire missie.

Afbouwen kan een lastige fase zijn, zeker wanneer de bron inmiddels afhankelijk is van de dienst, financieel of op een andere manier. Ook kan de bron, in het geval van een heimelijk contact van de dienst, denken dat er sprake is van een jarenlange vriendschappelijke relatie; die kan over het algemeen ook niet van de ene op de andere dag worden afgebroken. Een andere reden om de samenwerking met een bepaalde bron stop te zetten is dat deze is 'aangebrand', oftewel dat bekend is geworden dat deze persoon een bron van de dienst is. Mogelijk vereist de situatie dan ook dat de diensten hun bron in bescherming nemen. De hoofden van de diensten hebben een wettelijke zorgplicht als het gaat om het beschermen van hun bronnen.[8]

Afbouwen van contacten is een belangrijk aandachtspunt, want wanneer dit niet met zorg gebeurt, kan een bron besluiten om informatie aan een tegenstander te geven of op een andere manier de dienst dwars te zitten. In het verleden hebben bronnen die het gevoel hadden niet goed behandeld te zijn door een van de diensten ook de media opgezocht.

De diensten kunnen wettelijk gezien verschillende bevoegdheden inzetten als het gaat om het verzamelen van humint. Ze kunnen altijd op basis van vrijwilligheid gesprekken met personen voeren om informatie op te halen. Dit wordt het raadplegen van informanten genoemd en is een algemene bevoegdheid van de diensten. Ook kunnen diensten mensen volgen, agenten inzetten of een bedrijf of rechtspersoon opzetten (denk aan Project Mongool). Dit zijn allemaal bijzondere bevoegdheden. Op

het verschil tussen algemene en bijzondere bevoegdheden kom ik in het volgende hoofdstuk nog terug.

Informanten raadplegen betekent niets meer dan dat diensten aan iedereen vragen mogen stellen. Diensten kunnen onder deze bevoegdheid niemand dwingen om met hen te praten en ze mogen niemand onder het mom van 'praten met informanten' aanzetten tot acties; het gaat echt alleen om met iemand in gesprek gaan om informatie te krijgen. Te denken valt aan praten met een medewerker van een buurtcentrum om een idee te krijgen wie er allemaal bijeenkomen in het gebouw, in gesprek gaan met de ouders van een kind dat mogelijk radicaliseert, of praten met een hoogleraar over de afscherming van gevoelig onderzoek. De kern van deze bevoegdheid is dat de diensten met bijna iedereen mogen praten (met politiemensen mag dat alleen na toestemming van een leidinggevende), en dat iedereen mag weigeren in gesprek te gaan.

Zodra de diensten iemand willen aansturen, gaat het niet meer om het raadplegen van informanten, maar wordt iemand tot agent gemaakt. Deze bijzondere bevoegdheid is in een apart artikel in de Wiv opgenomen. Dat dit een bijzondere bevoegdheid is, heeft er onder andere mee te maken dat agenten betrokken kunnen raken bij strafbare feiten. Hierbij is het zogenoemde Tallon-criterium van toepassing. Dit houdt in dat agenten van de diensten anderen nooit mogen aanzetten tot beraming of pleging van strafbare feiten, voor zover deze persoon dat nog niet van plan was. Vaak wordt hierover vooraf met de Landelijk Officier van Justitie (LOVJ) gesproken en wordt ook in de instructie voor de agent opgenomen (voor zover dat van tevoren kan worden voorzien) aan welke strafbare handelingen de agent medewerking mag verlenen.[9]

In de Wiv staat ook dat de diensten bevoegd zijn om mensen

of zaken te observeren en te volgen, bijvoorbeeld door bepaalde personen te volgen of apparatuur in hun huizen of auto's aan te brengen. Op deze manier kunnen de diensten inzicht krijgen in de intenties van deze personen. Ook kunnen ze in de gaten houden met wie zij in contact staan, wat ze doen en hoe ze zich gedragen.

Osint

De diensten hebben lang niet altijd bijzondere bevoegdheden nodig om aan informatie te komen. Ik vermelde al eerder dat er weleens gezegd wordt dat 80 procent van de inlichtingen tegenwoordig afkomstig is uit open bronnen. Of dat percentage nu klopt of niet, open bronnen (*open-source intelligence*, afgekort tot osint) vormen een omvangrijke bron van informatie. Veel informatie is gewoon te vinden in kranten, op radio en televisie, in archieven, op websites en internetfora en in databases zoals het Kadaster.

Osint is niet nieuw, maar heeft door internet wel een vlucht genomen.[10] Veel meer informatie dan ooit tevoren is voor iedereen ontsloten. De Verenigde Staten hadden echter al tijdens de Tweede Wereldoorlog een inlichtingenonderdeel dat zich volledig richtte op open bronnen.[11] Uit honderden dag- en weekbladen verzamelden de medewerkers informatie die inzicht gaf in het doen en laten van de tegenstander. Of het nu ging om foto's van oorlogsmaterieel, beelden van ontploffingen en gebouwen die in puin lagen of om overlijdensadvertenties waaruit bleek welke nazi's overleden waren, alles werd nauwlettend in de gaten gehouden en bewaard.

In artikel 25 van de Wiv 2017 staat dat de dienst gegevens uit voor iedereen toegankelijke bronnen mag verzamelen, ook als daarvoor betaald zou moeten worden – denk aan uittreksels van

de Kamer van Koophandel of een abonnement op een krant. Indien de diensten stelselmatig gegevens in open bronnen willen verzamelen, bijvoorbeeld door structureel bij te houden wat iemand doet op sociale media, is daar toestemming voor nodig van dienstmedewerkers die door het hoofd van de dienst hiertoe zijn aangewezen.

Voordelen van het gebruik van osint zijn dat er veel informatie beschikbaar is en dat je daar snel aan kunt komen. Bij humint moet je gericht te werk gaan, maar bij osint kun je een breed net uitwerpen. Ook is het relatief goedkoop om informatie uit open bronnen te verzamelen, al kost continue monitoring natuurlijk wel tijd en geld. Een laatste voordeel, bijvoorbeeld ten opzichte van humint, is dat osint vaak op afstand beschikbaar is: je hoeft meestal niet dicht in de buurt van je tegenstander te komen om de informatie te verkrijgen.

Dat er meestal geen bijzondere bevoegdheden nodig zijn om osint te verzamelen, wordt ook gezien als een groot voordeel. Diensten moeten namelijk altijd eerst het lichtste middel inzetten om hun informatie te verzamelen, oftewel de manier die het minst inbreuk maakt op de privacy van de onderzochte personen. Over het algemeen begint dus ook elk onderzoek met een openbronnenonderzoek. Pas als daarna blijkt dat er nog aanvullende informatie nodig is, zullen diensten zwaardere middelen inzetten.

De inlichtingen afkomstig uit osint zijn vaak snel te verspreiden, zowel binnen als buiten de organisatie. Veel inlichtingenproducten zijn namelijk 'gerubriceerd', oftewel: ze zijn als meer of minder geheim bestempeld. Dat betekent in praktische zin dat je de inlichtingen alleen mag delen met geselecteerde personen of organisatieonderdelen. Dat is ook logisch, want het is meestal niet wenselijk de naam van een bron bekend te ma-