DIT WIL JE ÉCHT NIET WETEN

HUIB MODDERKOLK

DIT WIL JE ÉCHT NIET WETEN

OVER DE ONVOORSTELBARE WERELD ACHTER JE SCHERM

Uitgeverij Podium
Amsterdam

‘I think the potential of what the internet is going to do to society, both good and bad, is unimaginable. I think we’re actually on the cusp of something exhilerating and terrifying.’

– David Bowie in gesprek met Jeremy Paxman,
BBC Newsnight, 1999.

Eerste druk maart 2024
Vijfde druk april 2024

Omslagontwerp Stroomberg
Auteursfoto Frank Ruiter
Redactie Willemijn Lindhout

ISBN 9789463812160
NUR 320

www.uitgeverijpodium.nl

Inhoud

Proloog

Met een man van middelbare leeftijd zit ik in een café in Den Haag. Hij is al jaren een van mijn belangrijkste bronnen. De man is goed ingevoerd bij de Nederlandse veiligheidsdiensten – om die reden kan ik zijn naam niet prijsgeven.

We praten af en toe bij, veelal op mijn initiatief. Hij is iemand met vertrouwen in de overheid en maakt zich niet snel zorgen over zijn privacy. Hoewel hij zich bezighoudt met geheime informatie, deelt hij zonder schroom zijn laatste sportactiviteiten via de app Strava, plaatst persoonlijke foto's op sociale media – net als zijn exacte verblijfslocatie. 'Ik heb niets te vrezen,' is zijn levenshouding.

Zijn perspectief vind ik, als journalist die vooral schrijft over de schaduwkanten van digitalisering, waardevol. Maar nu, op een dag in 2022, kijken we allebei verbaasd op onze telefoons naar PimEyes: een nieuwe krachtige online zoekmachine voor gezichtsherkenning. Voer een afbeelding van een willekeurig persoon in en de slimme software vertelt je wie het is. Ik had erover gehoord en hem de zoekmachine laten zien.

Uit nieuwsgierigheid besluiten we ter plekke een test te doen. Ongemerkt nemen we een foto van een cafébezoeker die een tafel verderop zit. Dan doet PimEyes zijn werk. Terwijl de man doorpraat en géén idee heeft wat zich op onze telefoons afspeelt, scrollen wij door foto's die de software voor ons heeft gevonden. In slechts enkele ogenblikken hebben we een beeld van zijn leven, identiteit en werkzaamheden. 'Ik maak me niet snel zorgen over privacy,' zegt de veiligheidsbron terwijl hij de zoekresultaten bekijkt, 'maar nu wel.'

*

Een paar maanden later tref ik in een Van der Valk-hotel een ander goed contact. Een kalme, aardige onderzoeker die bij een internationaal beveiligingsbedrijf werkt. Hij is een meester in het ontleden van computervirussen en het zoeken daarin naar hints van de daders. Over de hele wereld helpt hij overheden en bedrijven die zijn geraakt door een digitale aanval. Hij komt in presidentiële kantoren in Oost-Europa, bij ministeries in heel Europa en Azië, en bij oliebedrijven in het Midden-Oosten.

Tijdens zijn werk stuit hij geregeld op Iraanse en Russische geheime diensten die in een buitenlands netwerk zitten. Maar steeds vaker, zegt hij, richten die landen hun pijlen daarom op hem. In de hotellobby vertelt hij dat hij met intimidatie te maken heeft. 'Ik ontvang dreigende telefoontjes van Russen.'

Dat baart hem zorgen. Hij heeft kleine kinderen. De man weet bovendien hoe kinderlijk eenvoudig zijn tegenstanders aan informatie over hem en zijn familie kunnen komen. Niet omdat hij daar slordig mee omspringt, maar omdat onze – en dus ook zijn – data bij tientallen en soms zelfs honderden organisaties liggen. Daar zijn ze lang niet altijd veilig, blijkt steeds vaker. Het aantal datalekken blijft toenemen. Na een digitale aanval bij parkeerapp EasyPark[1] liggen zijn persoonsgegevens en mogelijk zelfs parkeerlocaties op straat – net als die van miljoenen anderen.

Zo zijn er meer voorbeelden. De telefoondata met exacte locatiegegevens van ruim 1,5 miljard mensen zijn online te koop.[2] De specialist uit zijn bezorgdheid: 'Ik realiseer me steeds meer hoe kwetsbaar ik ben.' Ziehier de tragiek: de digitaal expert, die alles weet van beveiliging, heeft geen controle over zijn eigen gegevens.

Een poos na onze ontmoeting stuurt hij me een bericht: 'Het gaat niet zo goed.' Ik schrik en bel hem meteen. Hij mag geen details verstrekken maar het is duidelijk dat er maatregelen zijn getroffen hem te beschermen. 'Er hielden zich verdachte personen op in mijn om-

geving.' Het beangstigt hem. Hij woont met zijn gezin op een afgelegen plek. 'We willen verhuizen naar een buurt met meer sociale controle.'

*

Christiaan Beek denkt als een hacker. Dus als de digitaal specialist in 2018 in de Verenigde Staten met zijn vrouw naar het ziekenhuis gaat voor een echo van hun ongeboren kind, kijkt hij mee wat er op het computerscherm gebeurt. De vrouwelijke arts meet eerst de omvang van het hoofd en daarna de buik van de ongeboren baby en klikt op 'opslaan'. Dan merkt Beek iets vreemds op. 'In plaats van de melding "data opgeslagen in bestand", zag ik de melding "data opgeslagen in foto"', vertelt hij telefonisch. En die foto,[3] ontdekt hij bij verder onderzoek thuis, wordt binnen het ziekenhuis via allerlei systemen gedeeld.

Zo'n fotobestand bevat niet alleen een afbeelding van een echo of MRI, maar ook informatie over de patiënt. Soms zelfs de volledige naam, geboortedatum en andere persoonlijke details. Tot zijn schrik ziet Beek dat hij met gemak in de online systemen kan die de medische afbeeldingen bevatten. De foto's met data blijken onbeveiligd. 'Al voor de geboorte was de privacy van onze baby geschonden,' zegt hij.

Terug in Nederland doet Beek in 2023 opnieuw onderzoek naar de beveiliging van de systemen met deze medische foto's, die wereldwijd bij ziekenhuizen en privéklinieken in gebruik zijn. Hij scant het internet en vindt bijna tweeduizend kwetsbare servers vol afbeeldingen. Het probleem is veel groter dan hij vreesde: bij ruim 40 procent hiervan kan hij de medische foto's met patiëntdata ongehinderd opvragen.[4] Beek: 'Ziekenhuizen en fabrikanten van MRI-apparatuur doen er al jarenlang niets aan. Ze voelen de noodzaak niet.' Bij toeval stuitte hij tijdens de echo van zijn kind op iets opmerkelijks. Vijf jaar later blijkt die ontdekking symbool te staan voor de achteloze omgang met medische data.

Het is een wonderlijk mechanisme: iedereen heeft te maken met de keerzijdes van digitalisering en toch is er een constante neiging de gevaren te bagatelliseren. Mensen willen het er liever niet over hebben. 'Het zal allemaal wel.' Zoals het prettig is om net te doen of de klimaatcrisis een probleem is van anderen. Alleen experts of mensen die de gevolgen wel al hebben ervaren, zoals de personen in de voorbeelden hierboven, begrijpen de ernst.

In mijn eerste boek *Het is oorlog maar niemand die het ziet* beschreef ik hoe technologie het werk van inlichtingendiensten fundamenteel veranderde en op grote schaal spionage en beïnvloeding mogelijk maakte. Na verschijning van het boek werd mij met regelmaat gevraagd een lezing te geven. Dan vertelde ik hoe Russische hackers de stroom in Europa uitzetten, hoe Chinezen in elk denkbaar bedrijf kostbare informatie stalen en hoe Britse en Amerikaanse hackers binnendrongen bij telecomproviders, advertentiepartijen en het internationale bankverkeer. Hoe deze spionage en manipulatie van data burgers en overheden kwetsbaar maakt – en daarmee democratische rechtsstaten ondermijnt.

Mensen reageerden enthousiast op het boek en de verhalen, maar ik merkte aan hun reacties ook: dit gaat niet over mij. Die Modderkolk beschrijft een wereld die eng en gevaarlijk is, maar die buiten mijzelf staat. Het is mijn probleem niet.

Daarop besloot ik mijn verhaal aan te passen. Vanaf dat moment liet ik stap voor stap de risico's van technologie zien. Hoe de ontzaglijke hoeveelheden persoonlijke data steeds meer tegen mensen en samenlevingen worden gebruikt. Hoe overheden, bedrijven en even onschuldige als onwetende burgers erdoor in grote problemen raken.

Bij een uitgebreide lunch in Fort Altena in het Brabantse Werkendam luisterden in 2022 een kleine honderd man uit de chemische industrie naar mijn verhaal. Halverwege voelde ik de interesse wegvloeien en bij het hoofdgerecht – er stond wild op het menu – zei een directeur die werkte met systemen voor de machinebouw: 'Ik

zal je eerlijk zeggen: ik wil het eigenlijk niet weten.' Even was ik sprakeloos.

Maar hoe meer ik in de weken daarna over zijn opmerking nadacht, hoe beter ik die kon plaatsen. De ontwikkelingen gaan zo snel dat het amper bij te houden is. Sinds de introductie van de smartphone in 2007, de toenemende rekenkracht van computers en het online koppelen van allerlei apparaten, is de digitale revolutie in een stroomversnelling geraakt – en daar komt kunstmatige intelligentie nog eens bij.

Niet alleen inlichtingendiensten weten hoe ze technologie voor eigen gewin kunnen inzetten. Ook techreuzen, overheden, criminelen en eenlingen gebruiken de groeiende databergen om te controleren, te stelen en te manipuleren. Het probleem is daarmee fundamenteler. 'Iedereen krijgt te maken met de gevolgen van een datalek,' waarschuwde de Nederlandse Autoriteit Persoonsgegevens in 2023.[5] Alleen: de consequenties daarvan voelen niet ernstig, laat staan bedreigend, omdat ze zo moeilijk tastbaar te maken zijn. En dan is het verleidelijk om de ogen ervoor te sluiten. Of nog makkelijker: te doen alsof het gevaar niet bestaat.

Net als bij het klimaatprobleem is het simpel om de digitale crisis weg te wuiven. Om ieder symptoom ervan – 'helft kinderen telefoonverslaafd,'[6] 'anoniem protesteren niet meer mogelijk,'[7] 'medische instellingen in Nederland gehackt door China,'[8] 'democratieën onder druk door repressieve technologie'[9] – af te doen als een op zichzelf staand incident.

Je gaat de bredere, zorgelijke ontwikkeling pas scherp zien als de wereld áchter de nieuwsberichten begrijpelijk wordt. Daarom wilde ik dit boek schrijven. Dat een ongewoon postpakketje in 2020 de directe aanleiding zou vormen, kon ik toen nog niet voorzien.

1

Het aparte pakketje

Is het dom om een pakketje van een geheime dienst open te maken? Met die vraag loop ik nu een aantal dagen rond.

Het pakje ligt op de redactie van *de Volkskrant* en is opgestuurd na een merkwaardig mailcontact. Begin december 2019 verschijnt een Engelstalig bericht in mijn postvak. Dat begint met 'Mijnheer, Modderkolk. Ik heb belangrijke informatie voor u.' Een formidabele openingszin om de interesse van een onderzoeksjournalist te wekken.

De mail bevat brisante informatie. 'Een agent van de Mossad is al jaren in Nederland actief als undercover.' Snel pel ik de informatie af. De Mossad is de beruchte buitenlandse veiligheidsdienst van Israël. 'Zijn dekmantel is een reisbureau,' legt de afzender uit. Daarna volgt allerlei informatie over de Mossad-agent, opgeschreven in korte, feitelijke Engelse zinnen. 'Hij ontvangt inkomen van een Israëlisch bedrijf. Dit bedrijf bestaat niet.'

Ik lees de mail een paar keer om alle details goed in me op te nemen. De Israëlische spion, zo blijkt, is recentelijk ontmaskerd door iemand die hij probeerde te rekruteren. Ook is de computer van zijn vrouw gehackt. 'Bent u geïnteresseerd?' eindigt de mail.

Een aantal dingen valt me direct op. De tipgever spreekt soms in de ik-vorm en soms in de wij-vorm. 'Wij hebben de pc van zijn vrouw gehackt en hebben bewijs gevonden.' Hij heeft voor zijn communicatie met mij een speciaal Gmail-adres aangemaakt. Hij beheerst het jargon van geheime diensten. Zo noemt hij de Israëlische agent een non-official cover, kortweg NOC. Een NOC is een spion die niet bij een ambassade of consulaat werkt en daardoor geen diplomatieke onschendbaarheid geniet. Ook wel een 'slapende agent', iemand die opgaat in een samenleving en lang aan

een alternatieve identiteit werkt. Geduldig wacht hij tot zijn opdrachtgever hem een klus toebedeelt. De afzender gebruikt het alias Nasir.[1] Een veelgebruikte jongensnaam in Iran, leert een snelle zoekvraag via Google.

Verder valt op dat deze Nasir weinig loslaat over wie hij is en wat zijn motieven zijn. Terwijl de informatie die hij stuurt uitgebreid en gedetailleerd is. De tipgever vermeldt bijvoorbeeld de volledige naam van de Israëlische agent. Dat zet me aan het denken. Waarom zou iemand die zulke specifieke informatie deelt dat doen via een standaardmailprogramma en zijn eigen achtergrond weglaten? Of is dat onderdeel van zijn strategie? Mij nieuwsgierig maken met opzienbarende informatie zodat ik zeker op zijn mail zal antwoorden? En wat ik me tijdens het lezen ook afvraag: waarom deelt hij de informatie over een Israëlische spion uitgerekend met mij? In de mail staat geen verklaring. 'Ik kan u meer informatie sturen,' eindigt hij zijn bericht.

*

De mail komt binnen tijdens een hectische periode in mijn leven. Na publicatie van het boek *Het is oorlog maar niemand die het ziet*, twee maanden vóór de mail, volgden talloze aanvragen voor gesprekken en lezingen. Ik ontving tips voor nieuwe verhalen en uitnodigingen om bij organisaties te komen die eerder ontoegankelijk bleken. Nog lang niet alles bleek bekend over de onzichtbare strijd die zich afspeelt op onze computers en smartphones.

Eén specifieke casus kwam steeds weer ter sprake: een verhaal dat ik samen met de Amerikaanse journalist Kim Zetter maakte. Het beschreef de actie van een Nederlandse agent die binnendrong in een nucleair complex in Iran en daar een digitaal wapen lanceerde.[2]

Buitenlandse journalisten wilden er meer over weten, studenten stelden er vragen over, scenarioschrijvers zagen er een film in. De lancering van dat digitale wapen markeerde het begin van de on-

zichtbare oorlog. Stuxnet, zoals het ingezette computervirus werd genoemd, veranderde de wereld. Het liet de ongekende potentie van cyberwapens zien: in stilte konden die fysieke schade veroorzaken op een plek ver van het eigen grondgebied. Maar ook werden de gevaren zichtbaar. Stuxnet verspreidde zich over honderdduizenden computers, raakte op drift en de aanvallers verloren de controle. Andere landen zagen de offensieve kracht van het wapen en begonnen hun eigen cyberwapens te ontwikkelen. Juridische kaders waren er niet. Als Stuxnet geoorloofd was, leek alles geoorloofd. Stuxnet zette een beweging in gang die niet meer te stoppen was.

Door de interesse van de buitenwereld begon ik weer meer over het onderwerp te denken. Zeker toen er na een praatje bij een beveiligingsbedrijf in Rotterdam een man naar mij toe kwam. Hij zei op fluistertoon dat Nederland een veel grotere rol bij Stuxnet had gespeeld dan bekend was.

Over de Nederlandse inbreng bij Stuxnet was nog veel onduidelijk. Wie was bijvoorbeeld de man die de gevaarlijke missie ondernam? Hoe was het met deze persoon afgelopen? Maar ook: wie had in Nederland toestemming gegeven voor de inzet van dit digitale wapen? Welke afweging was er in het kabinet gemaakt?

Als ik de mail van de Iraanse Nasir nog eens lees, blijft mijn blik hangen bij de eerste zin. 'Ik heb recentelijk uw boek gelezen.'

*

Een man met een Iraanse naam die zegt dat hij een Nederlands boek heeft gelezen en die een tip stuurt over een Israëlische spion. Door de combinatie van die drie landen moet ik ogenblikkelijk aan Stuxnet denken, al begrijp ik de relatie niet direct. En hoe kan het dat hij een Nederlands boek leest dat nog niet is vertaald?

Dat iemand uit Iran weet heeft van het boek is niet zo gek. Toen de Nederlandse rol bij de sabotage van het Iraanse nucleaire programma twee maanden eerder bekend werd, was er toevallig net een

Nederlandse diplomatieke delegatie in Teheran. Die werd door Iran ontboden en haar werd om opheldering gevraagd. Iran nam de zaak hoog op.[3]

Maar in de mail staat geen woord over Stuxnet. Nieuwsgierig geworden, vraag ik Nasir de volgende ochtend om meer informatie. Over de Israëlische spion die in een slaperig dorp in Nederland zou wonen en over hemzelf. Ik schrijf terug dat ik het gevonden 'bewijs' uit de hack niet wil ontvangen. Hacken is strafbaar. Voor de zekerheid wijs ik hem op de mogelijkheid een veiliger kanaal dan Gmail te gebruiken. Mails van Gmail zijn dan wel goed versleuteld waardoor ze niet te lezen zijn als ze ergens worden onderschept, maar Google heeft de sleutels en zal bij een informatieverzoek van een overheid de communicatie overhandigen.

Nog geen twee uur later volgt het antwoord.

'Dank voor uw snelle reactie. Ik werk op een Iraanse ambassade in Europa.' In korte zinnen die allemaal op een nieuwe regel beginnen geeft Nasir een heleboel extra informatie. Zijn Engels is behoorlijk. Hij zegt dat 'onze' inlichtingeneenheid de Israëlische spion heeft ontmaskerd. Iran is erachter gekomen dat de agent al decennialang actief is. Eerst in het Israëlische leger waar hij Arabieren rekruteerde, daarna vanaf eind jaren negentig voor de Israëlische veiligheidsdienst Mossad in Nederland. De agent doet alsof hij werkzaam is bij een reisbureau in Nederland. En op missie, als hij Iraniërs wil overtuigen voor hem te werken, speelt hij een Duitse of Zuid-Afrikaanse zakenman. Arabieren en Iraniërs laten zich niet zo makkelijk rekruteren door een Israëliër; een Duitse of Zuid-Afrikaanse zakenman is een stuk minder bedreigend.

Dan volgen twee zinnen die me op scherp zetten. 'We hebben nu ook verklaringen van een Iraanse wetenschapper die door hem in het verleden is gerekruteerd.' En: 'De commandant van de Iraanse Revolutionaire Garde, generaal Qasem Soleimani, heeft opdracht gegeven hem gevangen te nemen of hem publiekelijk te ontmaskeren.'

De verwijzing naar de Iraanse wetenschapper doet me ogenblikkelijk weer aan Stuxnet denken. Israël probeert voortdurend bij Iraanse wetenschappers te komen die iets weten van, of betrokken zijn bij, het geheime nucleaire programma van Iran. Zou het kunnen dat de Israëlische spion in Nederland ook heeft meegedaan aan de Stuxnet-operatie?

Dat de tipgever over generaal Soleimani spreekt, is opzienbarend. Soleimani is een machtig man in Iran en verantwoordelijk voor de meest geheime militaire operaties van het land. Hij wordt gezien als de op één na belangrijkste persoon in het streng islamitische land, na de hoogste leider Ali Hosseini Khamenei.[4] Wat wil Nasir hiermee zeggen? Loopt de Mossad-man, zoals ik hem ben gaan noemen, in Nederland gevaar? En waarom vertelt hij dat aan mij?

Soleimani wordt vier weken later bij een Amerikaanse droneaanval gedood. De aanslag op de generaal, die door de VS wordt gezien als een belangrijke terrorist vanwege de samenwerking met organisaties als Hamas en Hezbollah, zet de verhoudingen tussen de VS en Iran op scherp. Iran zweert na de liquidatie wraak en valt Amerikaanse legerbases in de regio aan.[5]

Nasir sluit af met: 'Als we verder communiceren, zullen we andere middelen gebruiken zoals een anoniem e-mailaccount en wegwerptelefoons.' Bij de mail zit ook een bijlage. Ik twijfel of ik die moet openen. Zou het een val zijn? Zo op het oog is het een foto. Ik laat hem nog even ongeopend staan.

Alle nieuwe informatie maakt het niet overzichtelijker. Als het klopt wat Nasir zegt, is hij iemand met een hoge functie binnen de Iraanse overheid, die ook nog eens toegang heeft tot informatie van de Iraanse inlichtingendienst. Waarom gaat zo iemand mailen met een Nederlandse journalist? Dat voelt onlogisch. Ook het soort informatie dat hij deelt, is vreemd. Niet eerder heb ik van een bron zomaar staatsgeheime informatie gekregen via de mail. Het maakt het mysterie des te groter. Wat is hier aan de hand?

'Wat is je motivatie om dit met mij te delen? En hoe kan ik veri-

fiëren of de informatie klopt?' zijn enkele van de vragen die ik nog diezelfde dag terugstuur. En ook: 'Is er een relatie met Natanz?' Natanz is het nucleaire complex waar de Nederlandse agent Stuxnet naar binnen bracht. Het blijft in me opkomen dat de bemoeienis van deze Iraanse afzender niet op toeval berust, dus het lijkt me goed het maar gewoon op de man af te vragen. Het antwoord, de volgende ochtend, laat me schrikken.

*

De man, die zijn mails consequent blijft afsluiten met 'Nasir' zonder verdere groet, zegt dat hij niet langer in Iran kan leven. Hij wil asiel aanvragen in Europa. Door de informatie over de Israëlische spion met een journalist te delen hoopt hij meer kans te maken op asiel. 'Zoals u zult begrijpen, zet ik mijn leven op het spel door u te benaderen.' Ook het leven van de Mossad-man is in gevaar nu hij bekend is bij de Iraanse veiligheidsdienst. 'Door de informatie over hem te publiceren, kunt u zijn leven redden,' schrijft Nasir, wederom in kernachtige zinnen. Als publiekelijk bekend is dat er een Israëlische spion in Nederland gevaar loopt, laten de Iraniërs het wel uit hun hoofd om actie tegen hem te ondernemen, is zijn redenatie.

Vol verbazing kijk ik naar de mail. Met elke nieuwe zin wordt het belang van de zaak verder opgeschroefd. Had Nasir het in zijn eerste berichten nog over iemand die was ontdekt, nu is het een kwestie van leven en dood. Een Israëlische spion die in een Nederlands dorp woont zou in levensgevaar zijn. Tegelijkertijd blijf ik me afvragen waarom hij mij hierin betrekt. Zijn redenering is flinterdun. Als Nasir werkelijk is wie hij claimt te zijn, een hoge Iraanse overheidsmedewerker met toegang tot inlichtingeninformatie, staan alle Europese diensten met open armen te wachten om hem te ontvangen en naar hem te luisteren. Daar heeft hij geen journalist van een Nederlandse krant voor nodig.

Nasir schrijft verder dat de AIVD, de Nederlandse inlichtingendienst, op de hoogte is van de 'verdachte activiteiten' van de Mossadman in Nederland. 'De AIVD heeft, voor zover wij weten, vorig jaar de spion ondervraagd.' Het zou betekenen dat de Iraanse veiligheidsdienst goed op de hoogte is van het handelen van de AIVD in Nederland. Nasir schrijft ook dat hij ervan uitgaat dat de AIVD mijn e-mail onderschept en mijn telefoon afluistert. Daarom zal hij, voordat we elkaar fysiek kunnen ontmoeten, 'de juiste maatregelen nemen' om te voorkomen dat de geheime dienst hem identificeert.

Dan volgt een zin die bij mij argwaan oproept. 'We zullen wegwerptelefoons, Tor en versleutelde communicatie gebruiken.' Die woorden zijn letterlijk afkomstig uit een eerdere mail van mij. Toen had ik gewezen op het belang van veilige communicatie en, vrij willekeurig, drie mogelijkheden genoemd. Met simpele wegwerptelefoons maak je de kans op afluisteren kleiner. Zeker als je ze niet in de buurt van je eigen telefoon gebruikt en geregeld wisselt van simkaart. Online netwerk Tor maakt anoniem communiceren mogelijk via een browser die het IP-adres verhult. Versleutelde communicatie kan bijvoorbeeld via de chatapp Signal. Uiteraard is het ook mogelijk – en aan te bevelen – een combinatie van deze drie te gebruiken. Nasir herhaalt echter alleen deze zin en stelt niets concreets voor. Hij eindigt met: 'Als we elkaar ontmoeten, zal ik bewijs overhandigen van mijn identiteit en werkgever.' Mijn vraag over Natanz blijft onbeantwoord.

*

Het duizelt me. Door het mailcontact met Nasir dreig ik deelgenoot te worden van een inlichtingenspel op leven en dood. De informatie die hij geeft is spectaculair, misschien wel te mooi om waar te zijn. De tipgever onderscheidt zich in zijn mails duidelijk van andere personen die mailen door de details die hij verstrekt. Ogenschijnlijk is hij goed ingevoerd. En het curieuze is dat elke volgende mail van

hem spectaculairder is dan de voorgaande. Bij veruit de meeste tipgevers werkt het andersom: die verstrekken eerst de belangrijkste informatie, na doorvragen volgen meestal nuanceringen ('nou, ik heb het via via gehoord en ik weet niet of het nog steeds gaande is') en mogelijke obstakels ('ik heb geen documenten meer, maar persoon X wil die misschien wel geven').

Tegelijkertijd ben ik op mijn hoede. Dit is duidelijk iemand die bekend is met het werk van geheime diensten. De Iraanse Revolutionaire Garde staat niet bekend om haar zachtzinnigheid. Is de man eerlijk over zijn intenties? En is het verstandig hem te ontmoeten?

Om beter te begrijpen wat er aan de hand is, bel ik met twee bronnen van de AIVD. Meer dan tien jaar schrijf ik nu over het werk van de Nederlandse geheime dienst. In dat decennium heb ik stap voor stap een netwerk opgebouwd van mensen die bij de AIVD werken of hebben gewerkt en die ik af en toe raadpleeg. Met sommige bronnen is het contact zo goed dat ze hun kennis delen. Ik kan ze op elk moment van de dag bellen. Ik weet dat deze twee personen bij de AIVD onderzoek hebben gedaan naar Iran en in hun werk te maken hebben gekregen met agenten van de Iraanse dienst. Als de eerste bron hoort waarover het gaat, stelt hij direct voor om zo snel mogelijk ergens af te spreken.

Bij een biertje in een Amsterdams café nemen we de mails door. Mijn telefoon heb ik thuisgelaten. 'Hij moet voor een geheime dienst werken,' zegt de bron, die het taalgebruik van de Iraniër illustratief vindt. 'Als ik dit lees is het alsof ik zelf weer in een operatie zit.' Wat de tipgever precies wil, is hem niet duidelijk. 'Dat hij iets bij jou zoekt, lijkt me helder.' Hoewel de bron het contact zou voortzetten om te zien waar het naartoe gaat, en hij zeker niet uitsluit dat de tipgever zelf in gevaar is, is hij ook voorzichtig. 'Let de komende weken goed op. Je weet nooit waar dit soort diensten toe in staat zijn.' Als we afscheid nemen in het donker, merk ik dat ik extra alert ben op de omgeving. Als de bron wegrijdt, check ik haast automatisch of er iemand achter hem gaat rijden.